UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE RUSSAS

CURSO DE GRADUAÇÃO EM ENGENHARIA DA SOFTWARE

LUIS ANTONIO VIANA FRANKLIN

SISTEMA DE GESTÃO DE ACESSO USANDO RECONHECIMENTO FACIAL E MICROCOMPUTADOR.

RUSSAS

2023

LUIS ANTONIO VIANA FRANKLIN

SISTEMA DE GESTÃO DE ACESSO USANDO RECONHECIMENTO FACIAL E MICROCOMPUTADOR.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Software.

Orientador: Prof. Dr. Alexandre Matos Arruda.

RUSSAS

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

F915s Franklin, Luis.
Sistema de Gestão de Acesso usando Reconhecimento Facial e microcomputador / Luis Franklin. – 2023.
47 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas, Curso de Engenharia de Software, Russas, 2023.
Orientação: Prof. Dr. Alexandre Matos Arruda.

1. visão. 2. computacional. 3. reconhecimento. 4. facial. 5. microcomputador. I. Título.
CDD 005.1

LUIS ANTONIO VIANA FRANKLIN

SISTEMA DE GESTÃO DE ACESSO USANDO RECONHECIMENTO FACIAL E MICROCOMPUTADOR.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Software.

Aprovada em: 13/12/2023.

BANCA EXAMINADORA

Prof. Dr. Alexandre Matos Arruda (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Reuber Regis de Melo
Universidade Federal do Ceará (UFC)

Prof. Dr. Bonfim Amaro Júnior
Universidade do Estado do Ceará (UECE)

À minha família, por todo apoio e confiança que tiveram em mim. Mãe, seu amor e carinho foi que deram, em alguns momentos, a esperança para seguir firme nesse desafio. Pai, por ser minha maior inspiração, seu apoio mostrou que não estou sozinho nessa caminhada.

AGRADECIMENTOS

A Deus, primeiramente, que em toda minha trajetória esteve ao meu lado e colocou as melhores pessoas na minha vida.

Aos meus pais, Dr. Carlos Castilho Batalha Franklin e Alice Viana Franklin, por todo tempo, amor e carinho investidos em mim, vocês foram e são o pilar da minha vida.

À minha futura esposa, Anne Mikaelly, por todo amor e compreensão durante essa fase da minha vida, por estar comigo em todos os momentos bons e ruins, por todas as noites sem dormir ao meu lado em busca dessa tão incrível conquista.

Ao Prof. Dr. Alexandre Matos Arruda, pela excelente orientação, conselhos, reflexões, críticas e apoio acadêmico durante minha graduação, sem o Sr. não teria capacidade de trilhar tantos caminhos.

Aos professores participantes da banca examinadora Prof. Dr. Bonfim Amaro Junior e Prof. Dr. Reuber Regis de Melo, pelo tempo e pelas valiosas colaborações e sugestões.

Ao professor entrevistado, Prof. Dr. Dmontier Pinheiro Aragão Junior, pelo tempo concedido nas entrevistas.

A todos os colegas que me ajudaram participando desse experimento, sem a ajuda de vocês esse trabalho nunca teria saído do papel.

A todos os colegas do Laboratório de Tecnologias Inovadoras (LTI), desenvolvemos projetos incríveis de tamanha importância para o crescimento tecnológico da Universidade Federal do Ceará (UFC), vocês foram mais que amigos nessa trajetória, estar ao lado de vocês com certeza fez toda a diferença na minha formação.

Ao Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat), pela oportunidade e confiança depositadas pela Profa. Dra. Rossana Maria de Castro Andrade no meu trabalho como Cientista de Dados para o projeto BigData Fortaleza, onde pude me desenvolver na área.

Aos colegas da graduação, alcançamos muitas coisas juntos e o apoio de vocês foi inevitável.

RESUMO

A tecnologia tem avançado a passos largos, permeando cada vez mais o cotidiano das pessoas e facilitando a vida humana através da automação de processos. Um exemplo notável é o uso do reconhecimento facial para controle de acesso, aumentando a segurança em diversas áreas. No entanto, apesar dos avanços significativos, ainda existem desafios a serem superados. Variações de iluminação, expressões faciais e oclusões são alguns dos obstáculos que ainda precisam ser superados para melhorar a eficácia e a precisão desses sistemas, portanto, é crucial aprofundar o estudo desses desafios e das técnicas utilizadas. Atualmente, a gestão de acesso no Laboratório de Laboratório de Tecnologias Inovadoras (LTI) apresenta oportunidades de melhoria. O registro manual do nome e do horário de retirada e devolução da chave é um processo que pode ser otimizado. Nesse sentido, o desenvolvimento de um sistema automatizado de reconhecimento facial pode tornar esse processo mais eficiente e seguro. Com base nisso, este trabalho propõe o desenvolvimento de um sistema de gestão de acesso para os laboratórios da Universidade Federal do Ceará - Campus Russas, utilizando Microcomputador e Visão Computacional. Espera-se que este sistema torne a gestão de acesso mais eficiente, facilitando o acesso dos alunos e a gestão dos professores coordenadores. Este é um passo importante na direção de uma gestão de laboratório mais moderna e eficiente.

Palavras-chave: visão; computacional; reconhecimento; facial; microcomputador.

ABSTRACT

Technology has been advancing rapidly, increasingly permeating people's daily lives and facilitating human life through process automation. A notable example is the use of facial recognition for access control, increasing security in various areas. However, despite significant advances, there are still challenges to be overcome. Variations in lighting, facial expressions, and occlusions are some of the obstacles that still need to be overcome to improve the effectiveness and accuracy of these systems. Therefore, it is crucial to deepen the study of these challenges and the techniques used in facial recognition. Currently, access management at the Innovative Technologies Laboratory (LTI) presents opportunities for improvement. The manual registration of the name and the time of withdrawal and return of the key is a process that can be optimized. In this sense, the development of an automated facial recognition system can make this process more efficient and secure. Based on this, this work proposes the development of an access management system for the laboratories of the Federal University of Ceará - Russas Campus, using Microcomputer and Computer Vision for facial recognition. It is expected that this system will make access management more efficient, facilitating student access and teacher management. This is an important step towards more modern and efficient laboratory management.

Keywords: computer; vision; facial; recognition; microcomputer.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

EAR	*Eye Aspect Ratio*
GREat	Grupo de Redes de Computadores, Engenharia de Software e Sistemas
HOG	*Histogram of Oriented Gradient*
LBPH	Local Binary Patterns Histograms
LTI	Laboratório de Tecnologias Inovadoras
OpenCV	Open Source Computer Vision Library
UFC	Universidade Federal do Ceará
XML	eXtensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

A detecção e o reconhecimento de faces são tarefas naturais para os seres humanos, mas descrever objetos a partir de imagens é um desafio complexo para os computadores, pois é necessário entender o funcionamento da visão humana em relação vários fatores como iluminação e percepção de cores (SZELISKI, 2011). No entanto, com o avanço das pesquisas em visão computacional, houve um progresso significativo no desenvolvimento de máquinas que podem sentir o seu ambiente de visão, compreender e tomar decisões apropriadas mediante de programas computacionais (BESL P. J., 1985). Essa área tem sido aplicada com sucesso em questões de segurança, aumentando a precisão dos sistemas.

O avanço da miniaturização tem possibilitado a integração de câmeras em uma variedade crescente de sistemas e dispositivos embarcados. Esse desenvolvimento tem simplificado a vida cotidiana das pessoas e, ao mesmo tempo, fortalecido a segurança em diversas áreas, especialmente no controle de acesso a locais por meio do reconhecimento facial.

Vários países já estão utilizando o reconhecimento facial para identificar criminosos e pessoas desaparecidas, como Estados Unidos da América e China. No Brasil, essa tecnologia também está sendo implementada em diferentes estados, por exemplo, em São Paulo, onde a SP Trans bloqueou mais de 300 mil cartões de Bilhete Único por uso indevido de terceiros (SANTINO, 2019). Os ônibus da capital paulista possuem câmeras logo acima da máquina onde o passageiro registra o bilhete, a fim de verificar a identidade do usuário (SANTINO, 2019).

1.1 Motivação

A motivação deste trabalho reside na importância do reconhecimento facial como ferramenta de segurança e automação em diversas áreas. O avanço da tecnologia e a crescente disponibilidade de recursos computacionais possibilitaram a utilização do reconhecimento facial em uma variedade de aplicações, como controle de acesso a locais restritos, sistemas de vigilância, autenticação biométrica, entre outros.

No entanto, apesar dos avanços, ainda existem desafios a serem superados, como a robustez em relação a variações de iluminação, expressões faciais e oclusões (SZELISKI, 2011). Portanto, é necessário aprofundar o estudo desses desafios e das técnicas utilizadas no reconhecimento facial, a fim de melhorar a eficácia e a precisão desses sistemas.

Além disso, a gestão de acesso atualmente utilizada no Laboratório de Tecnologias

Inovadoras (LTI) apresenta oportunidades de melhoria, visto que hoje o processo funciona da seguinte forma: Durante o início do semestre letivo, os professores responsáveis por cada laboratório compilam informações dos alunos, incluindo nome, curso e matrícula, formando uma lista enviada para a portaria do campus. A portaria é então encarregada da administração das chaves dos laboratórios. Assim, o desenvolvimento de um sistema automatizado de reconhecimento facial pode otimizar esse processo, tornando-o mais eficiente e seguro.

1.2 Objetivo Geral

Pensando nisso, o objetivo geral deste trabalho é desenvolver um sistema automatizado de gestão de acesso, utilizando um microcomputador e Visão Computacional explorando técnicas de detecção facial como *Haar Cascade* e *Histogram of Oriented Gradient* e algoritmos utilizados nessa área, como *Local Binary Patterns Histograms*, *Fisherfaches* e *Eigenfaces*.

1.3 Objetivos Específicos

- Avaliar os algoritmos *Local Binary Patterns Histograms*, *Fisherfaches* e *Eigenfaces*, e selecionar o mais adequado com base na avaliação realizada;
- Desenvolver um modelo eficiente com base no algoritmo selecionado que possa detectar e classificar alunos cadastrados por meio de vídeo;
- Construir uma base de dados com imagens de alunos do LTI;
- Desenvolver um protótipo utilizando o microcomputador *Raspberry Pi 4 Model B*.

1.4 Estrutura do Trabalho

Este trabalho está dividido em seis capítulos: (1) Introdução; (2) Fundamentação Teórica; (3) Trabalhos Relacionados;(4) Metodologia; (5) Resultados e (6) Conclusão.

No capítulo dois, apresenta-se a fundamentação teórica, com uma breve descrição dos principais assuntos abordados neste trabalho. Ele está dividido em uma introdução ao *software*, seguida por uma explicação sobre o *hardware* e finalizando com uma discussão sobre ética e legislação. No capítulo três, são abordados os trabalhos relacionados. O capítulo quatro descreve a metodologia utilizada neste projeto. No capítulo cinco, são apresentados os resultados obtidos. Por fim, no capítulo seis, encontra-se a conclusão do trabalho, juntamente com as considerações finais e sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Visão Computacional

A Visão Computacional é um campo que se dedica a extrair informações e realizar transformações em dados, como imagens digitais e vídeos, visando compreender e descrever o mundo ao nosso redor (SZELISKI, 2011). Esse processo envolve o uso de algoritmos e técnicas que permitem identificar padrões, reconhecer objetos e reconstruir propriedades visuais, como forma, iluminação e cores (GARCIA, 2015).

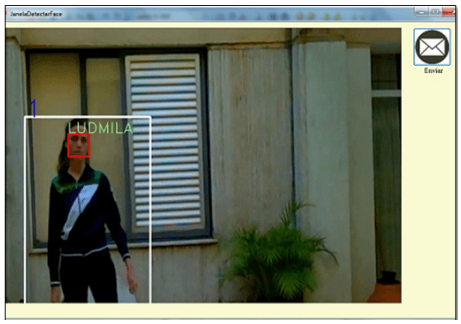
Do ponto de vista da engenharia, a Visão Computacional busca automatizar tarefas realizadas pelo sistema visual humano. Assim como um médico pode identificar um tumor em uma tomografia ou uma pessoa pode reconhecer seu próprio rosto em uma fotografia, sistemas de Visão Computacional têm o potencial de realizar essas mesmas tarefas (SZELISKI, 2011).

Algumas aplicações práticas da Visão Computacional incluem o reconhecimento ótico de caracteres, como a leitura de códigos postais escritos à mão, e o reconhecimento automático de placas veiculares em tempo real por meio de monitoramento de tráfego. Também é possível utilizar a Visão Computacional para inspecionar peças industriais, garantindo sua qualidade por meio de técnicas como visão estéreo e iluminação especializada. Outra aplicação importante é a modelagem 3D, que permite a construção de modelos tridimensionais a partir de fotografias aéreas utilizando a técnica de fotogrametria.

A Visão Computacional também desempenha um papel importante no desenvolvimento de áreas como veículos autônomos, permitindo que eles obtenham informações sobre o ambiente, como localização e detecção de obstáculos, para uma navegação segura. Embora a tecnologia de veículos autônomos ainda esteja em desenvolvimento, várias montadoras já demonstraram protótipos funcionais. Além disso, a exploração espacial também se beneficia da Visão Computacional, utilizando-a em veículos autônomos como o *Mars Exploration Rover* da *NASA* (NASA, 2018).

Outro exemplo de aplicação da Visão Computacional é o reconhecimento de movimentos e gestos humanos, como no sistema *Microsoft Kinect* para o videogame *Xbox*.

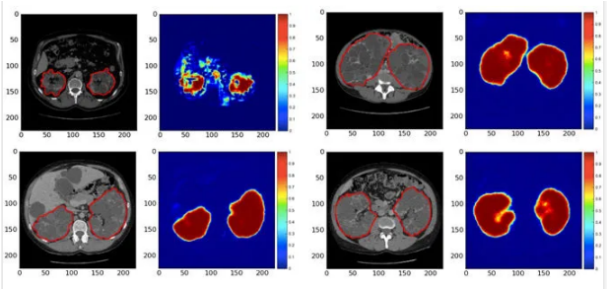
Figura 1 – Exemplo de Deteção de Movimento



Fonte: (DIGITAL, 2015).

No campo médico, a Visão Computacional é utilizada para processar imagens de diferentes modalidades, como microscopia, radiografia e ressonância magnética, auxiliando no diagnóstico e tratamento de pacientes Figura 2.

Figura 2 – Exemplo do uso da Visão Computacional no auxílio à identificação de doenças.

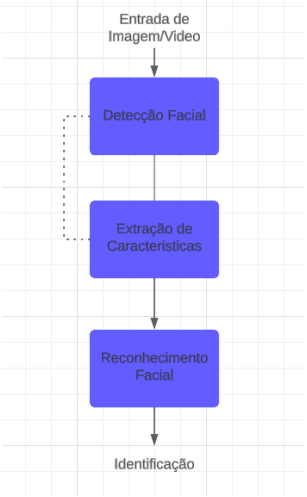


Fonte: (ACADEMY, 2022).

2.2 Reconhecimento Facial

Atualmente, há inúmeros algoritmos, que permitem o reconhecimento facial, em que é necessário seguir, pelo menos, três passos, como mostra a Figura 3: a detecção facial, a extração das características (*features*) e, então, a identificação dos rostos, ou seja, o reconhecimento facial propriamente dito.

Figura 3 – Fases do Reconhecimento Facial



Fonte: Tradução de (ZHAO, 2003).

Para a extração das características (*features*) de cada face, existem 3 principais abordagens: *holistic approach*, *feature-based approach*, e *hybrid approach*. A primeira utiliza a face como um todo para retirar as características faciais individuais, enquanto a segunda utiliza as partes específicas da face e a relação geométrica entre elas. Já a terceira é uma mesclagem entre a primeira e a segunda abordagens (BAKSHI, 2014).

Para cada um desses passos, várias são as técnicas disponíveis; o grande desafio está em escolher a mais adequada a cada aplicação, visto que cada uma apresenta diferentes formar de extração e perfomam melhor dependendo do tipo de uso desejado.

2.3 Algoritmos de Detecção

Os algoritmos de detecção mais populares atualmente são o *Haar feature-based cascade* e o *Histogram of Oriented Gradient (HOG)*. O primeiro foi apresentado por Paul Viola e Michael Jones no artigo *"Rapid Object Detection using a Boosted Cascade of Simple Features"* (em 2001) e o segundo proposto foi por Navneet Dalal e Bill Triggs no artigo *"Histograms of Oriented Gradients for Human Detection"* (em 2005)

2.3.1 Haar feature-based cascade

O algoritmo *Haar Cascade* é amplamente empregado na detecção de objetos em imagens ou vídeos em tempo real. Embora seja comumente usado para identificar faces (S., 2020), ele não se limita a essa aplicação, sendo também eficiente na identificação de objetos,

carros e placas. Neste projeto, o foco será a utilização do *Haar Cascade* para o reconhecimento de rostos.

A aplicação do *Haar Cascade* na detecção de faces requer um conjunto significativo de imagens, categorizadas como positivas e negativas (JONES, 2001). As imagens positivas contêm rostos de várias pessoas, o que permite a identificação de características comuns, como olhos, boca e nariz, presentes em todas as faces não afetadas por deficiências ou outros problemas. Por outro lado, as imagens negativas compreendem quaisquer outras imagens que não contenham os elementos a serem identificados. É crucial que essas imagens não apresentem faces, conforme ilustrado na Figura 4.

Figura 4 – Faces Positivas e Negativas.

Fonte: (OPENCV, 2022).

As imagens positivas e negativas necessárias para a detecção de faces podem ser adquiridas a partir de modelos já existentes, disponíveis em formato *eXtensible Markup Language (XML)*, um padrão comumente usado para arquivos codificados. Esses dados podem ser facilmente encontrados na internet e integrados ao *Open Source Computer Vision Library (OpenCV)*, uma biblioteca de visão computacional compatível com a linguagem de programação *Python*. O *OpenCV* suporta vários algoritmos de reconhecimento facial, incluindo o *Haar Cascades*, que estamos discutindo, e o *Histogram of Oriented Gradient (HOG)*.

O algoritmo *Haar Cascade* emprega classificadores para identificar as faces detectadas e posiciona-os sobre as características distintivas do rosto, como a boca, o nariz e os olhos, conforme mostrado na Figura 5. Esses classificadores são baseados em *features*, que são valores numéricos derivados da intensidade dos píxeis. O cálculo dessas *features* é feito com base no conceito de imagem integral, o que melhora significativamente o desempenho do processamento.

Figura 5 – Classificadores posicionados sobre as partes caracterizadoras do rosto.

Fonte: (OPENCV, 2022).

As *features* de borda (a) são utilizadas para identificar elementos faciais horizontais ou verticais, com base nos valores de referência dos píxeis 0 e 1, em uma determinada margem de valores e diferenças.

As *features* de linha (b) são aplicadas em áreas onde a diferença entre píxeis brancos e pretos segue a sequência 0, 1 e 0 novamente, como na região da boca de uma pessoa, onde os píxeis são mais claros acima e abaixo do lábio.

Por fim, as *features* de "quatro-retângulos"(c) são projetadas para identificar linhas diagonais, como as linhas externas do rosto. Essas características são fundamentais para o processo de reconhecimento facial, pois permitem que o sistema distinga detalhes sutis e complexos na estrutura do rosto, resultando em uma identificação mais precisa e confiável.

2.3.2 Histogram of Oriented Gradient (HOG)

O *Histogram of Oriented Gradient (HOG)*s, também conhecido como HOG, é um descritor de características que simplifica a representação de imagens ao se concentrar nas informações essenciais e ignorar detalhes irrelevantes. Ele identifica a direção das linhas nos píxeis (TYAGI, 2021). O HOG calcula o número de ocorrências (histogramas) dos gradientes de orientação em pequenas partes da imagem. Em combinação com o *Haar Cascade*, este descritor desempenha um papel fundamental no reconhecimento facial, permitindo não apenas a detecção, mas também a diferenciação entre as faces registradas. A Figura 6 mostra o histograma completo de gradientes orientados (à direita), realizado a partir da imagem de entrada (à esquerda).

Figura 6 – Histograma de gradientes orientados completo.

Fonte: (YE, 2022).

Para alcançar o resultado exibido à direita na Figura 6, é necessário calcular o vetor gradiente da imagem. Este vetor indica a variação dos níveis de cinza e sua direção. O cálculo do vetor gradiente leva em consideração as posições x e y da imagem (em relação à sua altura e largura em píxels) e é obtido através da seguinte equação (SANTOS M., 2020):

$$\nabla f(x,y) = \frac{\partial f(x,y)}{\partial x}\mathbf{i} + \frac{\partial f(x,y)}{\partial y}\mathbf{j} \tag{2.1}$$

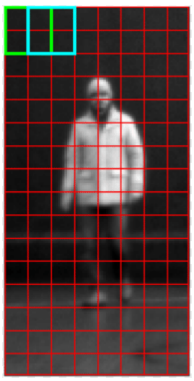
Para simplificar a notação, a primeira parte da Equação 2.1 será referida como Gx e a segunda parte da Equação 2.1 será referida como Gy. Aqui, Gx e Gy representam o gradiente da imagem nas direções x e y, respectivamente. A Equação 2.2 apresenta o cálculo da magnitude do operador gradiente, enquanto a Equação 2.3 mostra o cálculo da orientação do vetor gradiente.

$$\text{Mag}(Vf) = \sqrt{Gx^2 + Gy^2} \tag{2.2}$$

$$\theta(Vf) = \arctan\left(\frac{Gy}{Gx}\right) \tag{2.3}$$

A Figura 7 demonstra o processo de cálculo realizado em pequenas partes da imagem, conhecidas como células. Para cada célula, um histograma é calculado com base nos gradientes de orientação presentes. A combinação desses histogramas individuais resulta no histograma de gradientes orientados, representado na Figura 6. Este procedimento é crucial para capturar a silhueta detalhada das faces que serão posteriormente reconhecidas.

Figura 7 – Células demonstradas na imagem (quadriculados), onde serão calculadas.



Fonte: (GARZON, 2013).

2.4 Tecnicas de Detecção Facial

2.4.1 Local Binary Patterns Histograms (LBPH)

O algoritmo *Local Binary Patterns Histograms (LBPH)*, que se baseia no algoritmo de Padrões Binários Locais, é uma técnica de análise de texturas que visa resumir a estrutura de uma imagem através da comparação dos píxel s com seus vizinhos (OJALA, 1996).

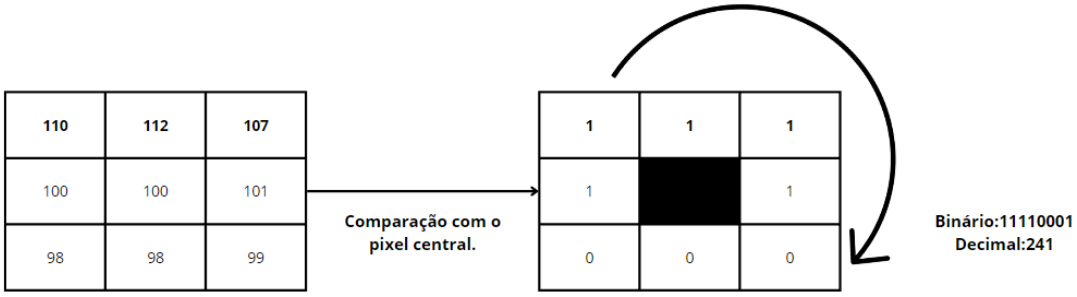
A partir de um raio que define a vizinhança de um píxel central, e sendo P o número de vizinhos nesse limite, o valor da intensidade I de um píxel , denotado por x_{ij} (onde i e j são as coordenadas do píxel na imagem), é comparado com o de seus P vizinhos. Os vizinhos com intensidade maior ou igual à do píxel central recebem o valor 1, enquanto os demais recebem o valor 0. Em seguida, realiza-se uma multiplicação do valor dos vizinhos (0 ou 1) pela potência de 2 da posição que ocupam em relação ao píxel central. Finalmente, os valores são somados e o valor do píxel central é definido. Este processo é exemplificado na Figura 8. A função é descrita da seguinte maneira:

$$LBP(X_{ij}) = \sum_{p=0}^{P-1} 2^p S(I_p - I_x) \tag{2.4}$$

sendo,

$$S(x) = \begin{cases} 1, & \text{se } x \geq 0 \\ 0, & \text{se } x < 0 \end{cases} \tag{2.5}$$

Figura 8 – Operador *LBPH*.



Fonte: Feito pelo Autor.

A imagem produzida pelo operador *LBPH* Figura 9 (b) é dividida em m regiões locais. Em seguida, o histograma de cada região é extraído. Estes histogramas são então concatenados para formar um único histograma de características espacialmente aprimorado, que representa eficientemente a imagem do rosto (AHONEN, 2004).

Figura 9 – Rosto original e rosto gerado através do operador *LBPH*.

(a) Rosto original

(b) Rosto processado com o operador *LBPH*

Fonte: Feito pelo Autor.

Por fim, as características resultantes desse histograma de Padrões Binários Locais, ou *Local Binary Patterns Histograms*, são usadas como descritores da imagem e, consequentemente, nas comparações para determinar a classe da imagem que mais se assemelha à imagem

apresentada pelo RF.

2.4.2 Eigenfaces

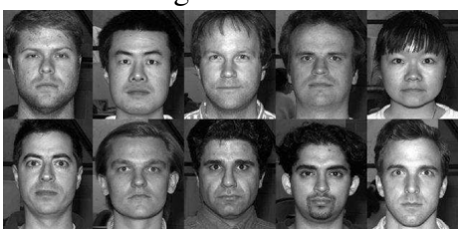
O método *Eigenfaces* é uma técnica que busca identificar características faciais independentemente das formas geométricas, como olhos, nariz, orelhas e boca, utilizando todas as informações disponíveis na representação facial (BAKSHI, 2014). Este método utiliza uma matriz de covariância para calcular autovetores e autovalores.

É importante ressaltar que a iluminação tem um papel crucial no *Eigenfaces*. Ela influência a criação dos autovetores, que são baseados tanto nas variações das faces quanto nas variações de luminosidade. Se existirem várias imagens da mesma pessoa com variações faciais significativas, o resultado obtido pelo método será mais preciso. No entanto, se houver variações significativas de iluminação para cada face, essas variações serão usadas para determinar as *Eigenfaces*, para não comprometer a precisão do algoritmo.

As *Eigenfaces*, baseadas na Teoria da Informação, buscam identificar um número reduzido de características relevantes para diferenciar uma face das outras. Essas características podem ser analisadas apenas considerando a variação nos valores assumidos pelos píxeis em um conjunto de imagens faciais (DINIZ, 2013).

O termo "*Eigenfaces*" refere-se aos autovetores da matriz de covariância das imagens das faces no banco de dados de treinamento, pois eles possuem características das faces. No *Eigenfaces*, o conjunto de imagens de treinamento extrai as componentes mais relevantes da face humana e cria uma face média com base nesses dados. Variando os valores dessas componentes, é possível representar uma ampla variedade de faces, realizando apenas multiplicação escalar com os autovalores. De fato, cada face pode ser representada como uma combinação linear das várias *Eigenfaces*. A Figura 10 mostra exemplos de faces do banco de imagens de *Yale*.

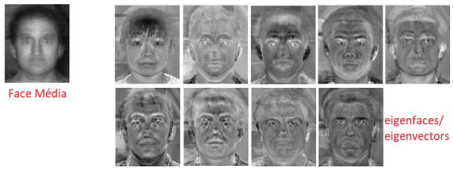
Figura 10 – Exemplos de faces do banco de imagens de *Yale*.



Fonte: (BELITSKAYA, 2018).

A Figura 11 mostra as *Eigenfaces* extraídas das faces presentes no banco de dados de imagens de *Yale*. Além disso, a face média, que será usada como base para a reconstrução das diversas faces, também é apresentada.

Figura 11 – Face Média e *Eigenfaces*.



Fonte: (DAVE, 2010).

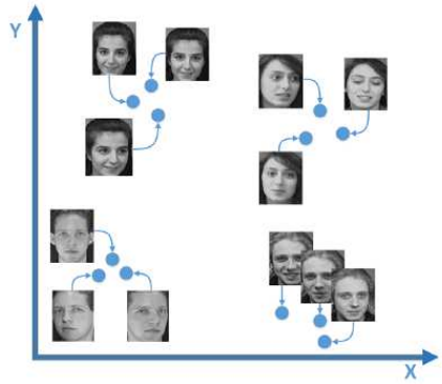
O método *Eigenfaces* permite a classificação de faces ao calcular a distância entre a imagem em análise e a imagem projetada no novo espaço. Se essa distância estiver em um limite predefinido, conhecido como *threshold*, a imagem é considerada uma face; caso contrário, é classificada como não face. Além de permitir a classificação, o método *Eigenfaces* também possibilita a reconstrução e a compactação de imagens faciais.

2.4.3 Fisherfaces

Semelhante ao método *Eigenfaces*, as *Fisherfaces* podem ser visualizadas como imagens de características, onde as características das *Fisherfaces* representam variações de aparência presentes nas imagens de cada indivíduo, como variações de luminosidade, poses e expressões faciais.

Assim como as imagens no espaço de dados possuem um valor para cada atributo, os vetores e características possuem um valor correspondente para cada *Fisherface*. A Figura 12 mostra a projeção das faces em relação às *Fisherfaces*.

Figura 12 – Espaço de Faces Fisherfaces.



Fonte: Adaptado de (SILVA, 2016).

Quanto mais distintas forem as pessoas, mais distantes estarão suas projeções no espaço de *Fisherfaces*. Por outro lado, quanto mais semelhantes forem as imagens de uma pessoa, mais próximas estarão suas projeções.

O algoritmo *Fisherfaces* é composto por 8 etapas:

1. **Cálculo da Face Média por Classe:** A face média por classe é obtida somando píxel a píxel todas as imagens de uma mesma classe no conjunto de treinamento e dividindo pelo total de imagens da classe.

2. **Cálculo da Face Média Geral:** A face média é calculada somando píxel a píxel todas as imagens do conjunto de treinamento e dividindo pelo total de imagens.

3. **Transformação das Imagens em Vetores:** Cada imagem é transformada em um vetor, concatenando as linhas da imagem e formando um vetor.

4. **Construção da Matriz de Dispersão Intra-Classe:** Esta matriz calcula o quão dispersos estão os dados dentro da mesma classe, ou seja, o quanto as imagens de um mesmo indivíduo diferem entre si.

5. **Construção da Matriz de Dispersão Inter-Classe:** Esta matriz calcula o quão dispersos estão os dados entre as diferentes classes, ou seja, o quanto as imagens de indivíduos distintos diferem umas das outras.

6. **Cálculo das *Fisherfaces*:** As *Fisherfaces* e seus valores associados são obtidos como autovetores e autovalores da matriz de dispersão intra-classe e inter-classe.

7. **Cálculo dos Vetores de Características:** Cada imagem de face é representada pela soma ponderada das *Fisherfaces*. Os pesos dessa combinação são os vetores de características das imagens de face.

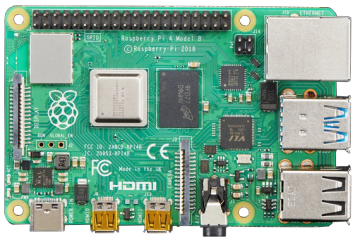
8. **Cálculo da Similaridade:** O reconhecimento pode ser realizado através de

um classificador ou de uma métrica de similaridade. Uma das métricas comuns é a distância euclidiana, onde a similaridade entre duas faces é medida pela distância entre seus vetores de características.

2.5 Microcomputador *Raspberry*

As placas *Raspberry Pi* são unidades de processamento de baixo custo comumente utilizados em projeto de sistemas embarcados devido às funcionalidades que oferecem, como o suporte a diversos protocolos de comunicação, à documentação open source e ao compartilhamento de informações pela comunidade. Um modelo se destaca para esse trabalho: o *Raspberry Pi 4 model B*.

Figura 13 – R*aspberry Pi 4 Model B*



Fonte: Raspberry Pi Foundation.

O *Raspberry Pi 4 Model B* representa uma evolução significativa na linha de microcomputadores *Raspberry Pi*. Equipado com um processador *quad-core* de 64 bits, o *Raspberry Pi 4* oferece um desempenho notável em comparação com seus predecessores. Seu sistema operacional baseado em Linux proporciona uma plataforma flexível e poderosa para uma variedade de aplicações. Ao contrário da abordagem mais compacta dos modelos *Zero W* e *Pico*, o *Raspberry Pi 4 Model B* é concebido para atender a demandas mais robustas, com portas USB, HDMI e conectividade de *Ethernet*, oferecendo maior versatilidade para projetos que exigem conectividade mais extensa. Além disso, o *Raspberry Pi 4 Model B* suporta os protocolos de comunicação padrão, como USB, SPI, I2C, entre outros, proporcionando uma gama ampla de opções para a interação com dispositivos externos e circuitos integrados.

2.6 Lei Geral de Proteção de Dados

O reconhecimento facial é uma tecnologia que permite a identificação e autenticação de indivíduos com base em características faciais únicas. Essa tecnologia tem sido amplamente utilizada em diversas áreas, como segurança, autenticação biométrica e organização de fotos digitais. No entanto, juntamente com os benefícios trazidos por esse avanço tecnológico, surgem desafios relacionados à proteção da privacidade e segurança dos dados sensíveis dos usuários.

Conforme o (GRYFO, 2023), a Lei Geral de Proteção de Dados (LGPD) reconhece os dados biométricos de rostos humanos tratados no contexto de reconhecimento facial como dados pessoais sensíveis. Esses dados são capazes de revelar informações como emoções, gênero, origem racial ou étnica, direcionamento do olhar e idade aproximada. Nesse sentido, é importante considerar os riscos associados ao uso desses dados sensíveis.

Um desses riscos é a possibilidade de discriminação com base nas informações de gênero ou raça obtidas por meio do reconhecimento facial. Conforme mencionado no texto, fornecedores podem classificar clientes com base nesses perfis, atribuindo vantagens a um grupo em detrimento do outro. Esse tipo de discriminação levanta preocupações éticas e sociais, destacando a necessidade de regulamentações que garantam a igualdade e a não discriminação.

Outro risco significativo é o vazamento de imagens que originam os dados biométricos. Esses vazamentos podem expor os usuários a diversas ameaças, como fraude ou exposições públicas indesejadas. Com uma captura de tela dos dados biométricos, é possível explorar outros dados pessoais do usuário. Portanto, é essencial adotar medidas de segurança robustas para proteger essas informações sensíveis e garantir a privacidade dos indivíduos.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais desempenha um papel fundamental na garantia da segurança dos dados sensíveis no contexto do reconhecimento facial. A lei estabelece que empresas, microempreendedores digitais e o governo só podem tratar esses dados com o consentimento explícito da pessoa e para um fim definido. Além disso, existem situações específicas em que o tratamento dos dados sensíveis é permitido, como em casos de obrigação legal, direito, contrato ou processo, prevenção de fraudes, estudos de órgãos de pesquisa e políticas públicas.

3 TRABALHOS RELACIONADOS

Neste capítulo, é apresentado uma comparação entre o trabalho abordado nesta tese e estudos relacionados, focando na representação do conteúdo presente em materiais educacionais. A elaboração deste capítulo envolveu uma pesquisa no site "Google Acadêmico"utilizando os seguintes termos e frases-chave: Visão Computacional, Reconhecimento Facial, Sistema de Reconhecimento Facial e Sistema de Reconhecimento Facial utilizando Arduino.

3.1 Aplicativo para Controle de Fluxo de Trânsito usando Arduino e Câmera com *OpenCV*

No trabalho apresentado por (LOPES, 2016), foi proposta a construção de um aplicativo de controle de fluxo de trânsito utilizando Arduino e visão computacional. O objetivo era utilizar técnicas de visão computacional, com o auxílio da biblioteca *OpenCV*, para resolver problemas de fluxo de trânsito em ambientes urbanos.

O trabalho mencionado utilizou uma *webcam* USB conectada a um computador programado com um *script python* para capturar imagens e implementar as funcionalidades de visão computacional. O Arduino Uno foi utilizado para controlar fisicamente o fluxo de trânsito por meio de LEDs, recebendo as informações geradas pelas imagens processadas pela visão computacional.

A análise realizada pelo sistema contava a quantidade de fluxo de trânsito e enviava sinais lógicos ao Arduino para controlar os semáforos. A comunicação entre o computador e o Arduino era realizada por meio de uma conexão *Wi-Fi*, utilizando o Arduino Uno conectado a um servidor *Wi-Fi*.

Embora o trabalho apresentado por (LOPES, 2016) tenha semelhanças com a proposta do autor deste, existem algumas diferenças a serem destacadas. A proposta do autor deste trabalho visa resolver o problema da gestão de acesso, utilizando a placa *Rasbperry Pi 4 Model B*, que possui módulo de câmera da mesma fabricante, sendo mais acessível. Além disso, o *Rasbperry Pi 4 Model B* tem processamento próprio, não sendo necessário um servidor *Wi-Fi* intermediário para tomada de decisões. Isso permite uma resposta mais rápida e evita problemas de conectividade em condições adversas.

Portanto, a proposta apresentada neste texto se destaca por oferecer uma solução mais robusta em termos de conectividade e resposta em comparação ao trabalho anteriormente citado.

Este trabalho foi escolhido pelo autor para comparar como a arquitetura de comunicação dos componentes, proposta por (LOPES, 2016), funcionaria em um sistema de reconhecimento facial.

3.2 Protótipo de fechadura eletrônica com Reconhecimento Facial

No trabalho apresentado por (NOGUEIRA, 2019), o objetivo é desenvolver um protótipo de fechadura eletrônica com reconhecimento facial. O autor realizou uma pesquisa bibliográfica para embasar e facilitar a execução do trabalho, reduzindo o tempo necessário para sua realização. Após a pesquisa, a biblioteca *OpenCV* foi escolhida devido ao seu suporte oferecido e seus algoritmos de visão computacional, como *Eigenface, Fisherfaces* e *LBPH*, que foram utilizados para o processo de detecção, treinamento e reconhecimento facial. Além disso, o autor optou pelo uso do microprocessador *Raspberry Pi* para a automação do sistema, aproveitando seu sistema operacional e linguagens de comunicação de dispositivos.

O funcionamento do sistema desenvolvido pelo autor ocorre da seguinte maneira: um computador externo, conectado à mesma rede do *Raspberry Pi*, permite o cadastro de usuários e a configuração de autorizações de acesso. O sistema realiza o reconhecimento facial em tempo real, comparando as imagens capturadas com os rostos cadastrados. Caso a pessoa seja reconhecida e autorizada, o *Raspberry Pi* aciona a fechadura eletrônica por um determinado tempo. Caso contrário, a porta permanecerá fechada. O autor também captura uma foto do indivíduo durante o acesso, salvando-a em um banco de dados juntamente com a data e horário do acesso.

Os resultados obtidos pelo autor foram positivos, com uma taxa de precisão considerável nos algoritmos de reconhecimento facial. Surpreendentemente, o algoritmo *LBPH* obteve a maior taxa de precisão, contrariando as expectativas baseadas em pesquisas anteriores que apontavam o *Fisherface* como o mais adequado para o ambiente em questão. O autor concluiu que o desempenho dos algoritmos pode variar conforme as condições do ambiente e luminosidade.

Comparando o trabalho do autor deste com o trabalho apresentado por (NOGUEIRA, 2019), é possível observar que ambos possuem o objetivo de solucionar o mesmo problema, que é o controle de acesso utilizando técnicas de baixo custo em conjunto com a visão computacional e utilizam placas da fabricante *Rasbperry*, porém o autor utiliza *Rasbperry Pi 4 Model B*, o trabalho apresentado por (NOGUEIRA, 2019) não especifica o modelo da placa utilizada. Além disso, o trabalho do autor deste texto busca evitar fraudes no reconhecimento facial por meio da

detecção de piscadas e microexpressões faciais, proporcionando maior segurança e autenticidade ao sistema de acesso.

Este trabalho foi escolhido pelo autor para comparar como as técnicas de reconhecimento facial utilizadas por (NOGUEIRA, 2019) foram implementadas, visto que o objetivo dos trabalhos é o mesmo.

3.3 Sistema para Controle de Acesso e Automação em Prédios Inteligentes

No trabalho apresentado por (MACIEL, 2018), o objetivo é desenvolver um sistema integrado para controle de acesso e automação em prédios inteligentes. O autor propõe a utilização de tecnologias como reconhecimento facial e *RFID* para garantir a segurança e facilitar o acesso aos ambientes restritos. Além disso, o sistema também visa controlar dispositivos de automação, como iluminação e climatização, conforme a presença e necessidades dos usuários.

O sistema proposto por (MACIEL, 2018) utiliza o reconhecimento facial como uma das formas de autenticação de acesso. Para isso, são aplicados algoritmos de visão computacional, como *Eigenfaces* e *Haar Cascade*, para detectar e reconhecer os rostos dos usuários. Além disso, a tecnologia *RFID* é utilizada para permitir o acesso por meio de cartões ou tags de identificação.

A integração entre o sistema de controle de acesso e os dispositivos de automação é realizada por meio de uma plataforma central, que recebe as informações de autenticação e controle de acesso e aciona os dispositivos conforme as configurações estabelecidas. Dessa forma, é possível adaptar a iluminação e a climatização dos ambientes conforme a presença e necessidades dos usuários, proporcionando um maior conforto e eficiência energética.

O autor destaca a importância de uma infraestrutura de rede adequada para garantir a comunicação entre os dispositivos e a plataforma central. Além disso, são abordados aspectos de segurança, como a proteção dos dados de identificação dos usuários e a prevenção de fraudes no reconhecimento facial.

Comparando o trabalho do autor deste com o trabalho apresentado por (MACIEL, 2018), é possível observar que ambos possuem o objetivo de desenvolver sistemas para controle de acesso. Ambos utilizam tecnologias como reconhecimento facial para autenticação de acesso. No entanto, existem diferenças em relação à forma como essas tecnologias são aplicadas e integradas ao sistema.

Enquanto o trabalho apresentado por (MACIEL, 2018) destaca o uso de algoritmos de visão computacional, como *Eigenfaces* e *Haar Cascade*, para o reconhecimento facial, o

autor deste propõe o uso de técnicas como detecção de micro expressões faciais e contagem de piscadas para evitar fraudes. Essa abordagem adiciona uma camada adicional de segurança e autenticidade ao sistema de acesso.

Além disso, o trabalho apresentado por (MACIEL, 2018) enfatiza a integração do sistema de controle de acesso com dispositivos de automação, como iluminação e climatização, visando melhorar o conforto e a eficiência energética dos ambientes. Essa integração é realizada por meio de uma plataforma central, que recebe as informações de autenticação e controle de acesso.

Ambas as abordagens são relevantes e podem ser aplicadas em diferentes contextos, considerando as necessidades e recursos disponíveis para implementação de sistemas de controle de acesso e automação em prédios inteligentes.

Este trabalho foi escolhido pelo autor para comparar como as técnicas de reconhecimento facial utilizadas por (MACIEL, 2018) foram implementadas, visto que o objetivo dos trabalhos é o mesmo.

3.4 Fechadura Baseada em Reconhecimento Facial Via Dispositivos Móveis *Android*

No trabalho apresentando por (GUSMAO, 2016), foi desenvolvida uma fechadura eletrônica baseada em reconhecimento facial, utilizando dispositivos móveis *Android*. O objetivo desse sistema é fornecer uma solução prática e segura para o controle de acesso, substituindo as chaves tradicionais por reconhecimento facial.

A fechadura eletrônica proposta por (GUSMAO, 2016) utiliza a câmera frontal de um dispositivo móvel *Android* para capturar as imagens faciais dos usuários. O algoritmo de reconhecimento facial é implementado no próprio dispositivo, permitindo que a verificação seja realizada localmente, sem a necessidade de conexão com a nuvem.

O sistema utiliza a biblioteca *OpenCV* para o processamento das imagens faciais. As etapas envolvem a detecção e extração de características faciais, como olhos, nariz e boca, e a comparação dessas características com os dados cadastrados no sistema. O reconhecimento facial é realizado em tempo real, proporcionando uma resposta rápida ao usuário.

A aplicação móvel desenvolvida permite o cadastro dos usuários e o gerenciamento das permissões de acesso. Os usuários podem registrar suas faces no sistema, que armazena as informações necessárias para o reconhecimento facial. Durante o processo de autenticação, o sistema compara a imagem capturada pela câmera com os dados cadastrados e, se houver

correspondência, a fechadura é desbloqueada.

Os resultados obtidos com a implementação do sistema mostraram a eficácia do reconhecimento facial para o controle de acesso. A taxa de precisão na identificação dos usuários foi considerada satisfatória, demonstrando a viabilidade dessa abordagem. No entanto, é importante considerar que o desempenho do sistema pode ser influenciado por fatores como a qualidade da câmera do dispositivo móvel e as condições de iluminação.

A abordagem descrita no trabalho (GUSMAO, 2016) possui semelhanças com o projeto do autor deste, que também utiliza o reconhecimento facial para controle de acesso. Ambas as metodologias envolvem a captura de imagens faciais por meio de câmeras e a utilização de algoritmos de reconhecimento facial para autenticação dos usuários. No entanto, a principal diferença está na plataforma utilizada, sendo o trabalho (GUSMAO, 2016) focado em dispositivos móveis *Android*, enquanto o trabalho anterior adota a plataforma Arduino. Cada uma dessas abordagens tem suas próprias vantagens e pode ser adequada para diferentes contextos de aplicação.

Este trabalho foi escolhido pelo autor para comparar como a arquitetura *mobile*, proposta por (GUSMAO, 2016), funcionaria em um sistema de reconhecimento facial.

3.5 Sistema Autônomo e Inteligente de Reconhecimento Facial para Autorização de Entrada de Pessoal em Ambientes Restritos

Com base no trabalho apresentado por (SILVA, 2022), foi desenvolvido um sistema autônomo e inteligente de reconhecimento facial para autorização de entrada de pessoal em ambientes restritos. O objetivo desse sistema é utilizar técnicas avançadas de reconhecimento facial para garantir a segurança e o controle de acesso em locais específicos.

O sistema proposto por (SILVA, 2022) utiliza uma combinação de *hardware* e *software* para realizar o reconhecimento facial de forma autônoma. O *hardware* é composto por uma câmera de alta resolução e um dispositivo embarcado capaz de processar as imagens capturadas. O *software* implementa algoritmos de detecção e reconhecimento facial, executados no dispositivo embarcado.

A metodologia adotada por (SILVA, 2022) envolve o treinamento de um modelo de reconhecimento facial utilizando uma abundância de imagens de pessoas autorizadas. O modelo é treinado para identificar características específicas de cada pessoa e, assim, realizar o reconhecimento facial com alta precisão. Além disso, o sistema é capaz de detectar e rejeitar

tentativas de fraude, como o uso de máscaras ou fotos.

Os resultados obtidos com a implementação do sistema demonstraram a eficácia do reconhecimento facial para a autorização de entrada em ambientes restritos. O sistema foi capaz de identificar corretamente as pessoas autorizadas e rejeitar as tentativas de acesso não autorizadas. Além disso, o sistema apresentou um tempo de resposta rápido e uma taxa de precisão satisfatória.

Em resumo, o trabalho apresenta um sistema autônomo e inteligente de reconhecimento facial para autorização de entrada de pessoal em ambientes restritos. A abordagem adotada combina *hardware* e *software* para realizar o reconhecimento facial de forma eficiente e precisa. Os resultados obtidos indicam que o sistema é capaz de garantir a segurança e o controle de acesso de forma eficaz.

O projeto descrito por (SILVA, 2022) apresenta semelhanças com o projeto do autor deste, que também visa ao controle de acesso por meio do reconhecimento facial. Ambos os projetos utilizam técnicas avançadas de reconhecimento facial e adotam abordagens autônomas para garantir a segurança e o controle de acesso em ambientes restritos. No entanto, cada projeto possui suas particularidades e aspectos específicos de implementação, como o hardware utilizado e os algoritmos empregados. Essas diferenças podem influenciar no desempenho e nas funcionalidades dos sistemas propostos.

Este trabalho foi escolhido pelo autor para comparar como as técnicas de reconhecimento facial utilizadas por (SILVA, 2022) foram implementadas, visto que o objetivo dos trabalhos é o mesmo.

3.6 Tabela Comparativa

Na tabela 1, é realizada uma análise concisa das características distintivas entre diversos trabalhos relacionados ao controle de acesso por meio do reconhecimento facial. Cada trabalho é identificado por sua referência, com uma coluna adicional dedicada ao trabalho do autor. A tabela destaca aspectos como "Funcionamento *Offline*", "Detecção de Microexpressões Faciais", "Uso de *Display* para *Feedback* do Usuário"e "Armazenamento do Histórico de Acesso", proporcionando uma visão abrangente das diferentes abordagens implementadas em cada contexto. Essas características são essenciais para compreender as distintas funcionalidades e abordagens de cada sistema apresentado.

Tabela 1 – Tabela comparativa dos trabalhos relacionados com o trabalho do autor.

Funções	(LOPES, 2016)	(NOGUEIRA, 2019)	(MACIEL, 2018)	(GUSMAO, 2016)	(SILVA, 2022)	Trabalho do Autor
Sistema *Offline*	Não Presente	Presente	Não Presente	Presente	Não Presente	Presente
Detecção de Micro-expressões Faciais	Não Presente	Presente	Presente	Presente	Presente	Presente
Uso de *Display* para *Feed-back* do Usuário.	Não Presente	Não Presente	Não Presente	Não Presente	Não Presente	Presente
Armazendo do Histórico de Acesso	Não Presente	Não Presente	Presente	Presente	Não Presente	Presente

Fonte: Feito pelo Autor.

4 METODOLOGIA

4.1 Escolha do Algoritmo de Detecção

A escolha do algoritmo de detecção facial foi feita a partir de uma análise comparativa entre os três algoritmos citados na fundamentação Téorica: o Local Binary Patterns Histograms (LBPH), O *Eigenfaces* e o *Fisherfaces*.

A base de dados empregada neste estudo foi a de Yale (BELITSKAYA, 2018), composta por 165 imagens, das quais 30 foram reservadas para teste e 135 para treinamento, as imagens de teste foram as mesmas para todos os algoritmos. O treinamento foi conduzido utilizando todos os algoritmos mencionados anteriormente, resultando nos seguintes dados. A métrica de desempenho adotada foi o percentual de acerto, calculado pela fórmula:

$$\text{percentual\_de\_acerto} = \left(\frac{\text{total\_de\_acertos}}{30} \right) \times 100 \tag{4.1}$$

Com base na fórmula mencionada, foi elaborada uma tabela comparativa entre os algoritmos citados. O *Eigenfaces* apresentou um percentual de acertos de 73%, o *Fisherfaces* obteve 80% de acertos, e o *LBPH* registrou 66% de acertos.

Tabela 2 – Tabela comparativa de Acertos.

Algoritimos	Acertos
Eigenfaces	73%
Fisherfaces	80%
LBPH	66%

Fonte: Feito pelo Autor.

Com base na fórmula mencionada e análise da Tabela 2, foi viável determinar o algoritmo mais eficaz para este estudo. Nesse contexto, optou-se pelo algoritmo *Fisherfaces*.

4.2 Montagem do *Dataset*

A constituição do *dataset* seguiu o seguinte procedimento: Foi selecionado um grupo composto por 5 estudantes da Universidade Federal do Ceará, sendo 4 membros do LTI . Antes de iniciar o contrução do *dataset*, foi enviado para um dos participantes um formulário pedindo a autorização do uso de imagem para esse trabalho e para construção do modelo. Foram capturadas

120 imagens de cada participante em 6 posições diferentes: olhando para a câmera, com o rosto inclinado para a direita, com o rosto inclinado para a esquerda, com o rosto inclinado para cima, com o rosto inclinado para baixo e sorrindo. Cabe ressaltar que, neste estudo, não foi solicitada a remoção de acessórios, como óculos e bonés, com o intuito de avaliar a eficácia dos algoritmos mesmo na presença desses objetos.

Figura 14 – Exemplo de Captura de Face.

Fonte: Feito pelo Autor.

O *script* de captura foi desenvolvido em *Python*, utilizando a biblioteca *OpenCV*. O usuário insere seu nome e, em seguida, a câmera do *notebook* é ativada. O usuário posiciona seu rosto diante da câmera e pressiona a tecla "C". Após essa ação, o script captura 20 fotos na posição especificada. O usuário repete esse processo até concluir a sessão de captura.

4.3 Treinamento do Modelo

No processo de treinamento do reconhecedor *Fisherface*, as imagens do conjunto de treinamento são essenciais para o desenvolvimento de um modelo capaz de reconhecer rostos de maneira eficaz. Cada imagem passa por um pré-processamento, sendo convertida para tons de cinza e redimensionada para um formato padronizado. Além disso, cada pessoa é associada a um identificador único, estabelecendo uma correspondência entre os rostos e seus respectivos IDs.

Figura 15 – Exemplo de Imagens Utilizadas no Treinamento.

Fonte: Feito pelo Autor.

O reconhecedor *Fisherface* é então configurado para aprender padrões discriminativos presentes nas imagens de treinamento. Durante o treinamento, o modelo ajusta seus parâmetros para melhor representar as características distintivas de cada rosto. Esse conhecimento é encapsulado no modelo final, salvo para uso futuro.

Ao longo desse processo, a ênfase recai sobre a capacidade do *Fisherface* em discernir variações subtis nas características faciais, contribuindo para uma representação mais robusta e discriminativa. O resultado é um modelo treinado capaz de identificar indivíduos com base em padrões específicos, proporcionando uma base sólida para a aplicação prática do reconhecimento facial.

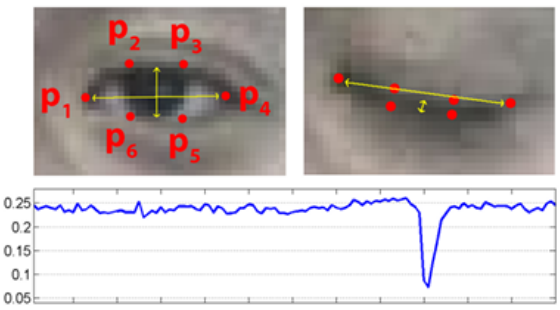
4.4 Detecção de Piscadas

A detecção de piscadas foi implementadautilizando a equação de medição da piscada descrita por (CEHOVIN ROK MANDELJC, 2016) em *"Real-Time Eye Blink Detection using Facial Landmarks"*. Essa equação permite calcular o EAR (*Eye Aspect Ratio*), que reflete a relação entre os pontos faciais envolvidos na medição da piscada. A fórmula para o cálculo do EAR é a seguinte:

$$EAR = \frac{|P_2 - P_6| + |P_3 - P_5|}{2\,|P_1 - P_4|} \tag{4.2}$$

Essa equação é aplicada para medir a taxa de piscadas e detectar possíveis fraudes por meio do uso de fotos.

Figura 16 – Olhos abertos e fechados com pontos de referência spi detectados automaticamente por *Eye Aspect Ratio*



Fonte: (CEHOVIN ROK MANDELJC, 2016).

4.5 Montagem do Protótipo

Foram montados dois protótipos, um seguindo o modelo apresentado na metodologia e outro projetado para instalação no Laboratório de Tecnologias Inovadoras (LTI). No entanto, neste subcapítulo, será abordado o modelo implementado no LTI.

Devido à impossibilidade de realizar alterações na estrutura da universidade, o protótipo a ser implementado no LTI foi concebido com a intenção de proporcionar ao usuário uma usabilidade focada na resposta do sistema. Nesse contexto, optou-se por não utilizar o módulo de relé, adotando apenas o módulo semáforo.

Para aprimorar a interação com o usuário, foi desenvolvido um sistema de feedback com quatro cores e três frases. Durante a fase de verificação, Figura 17 (a), a *"bounding box"* fica na cor azul e o LED do semáforo fica na cor laranja, e o texto exibido é "Verificando Entrada". Quando o usuário é aprovado, Figura 17 (b), a *"bounding box"* e o LED do semáforo mudam para verde, com a mensagem "Entrada Aprovada"e exibição do nome do usuário. Se o usuário não for aprovado, Figura 17 (c), a *"bounding box"* e o LED do semáforo ficam vermelhos, e a mensagem "Entrada Não Aprovada"é exibida, com a indicação "Not Identified"para o usuário.

Figura 17 – Protótipo implementado no Laboratório de Tecnologias Inovadoras

(a) Verificando Entrada **(b) Entrada Aprovada** **(c) Entrada não Aprovada**

Fonte: Feito pelo Autor.

Além disso, o sensor capacitivo tem a funcionalidade de abrir a porta pelo lado de dentro, operando da mesma forma e alterando a cor do LED do semáforo para verde.

4.6 Materiais Utilizados

Para a implementação do sistema, os seguintes materiais foram utilizados

- Microcomputador *Raspberry Pi 4 Model B*.
- *Raspberry Pi Camera* Rev 1.3.

- *Display* LCD TFT Touch 3.5.
- Módulo relé 5V.
- Botão de toque capacitivo TTP223.
- Módulo semáforo.
- Caixas Impressas em 3D para proteção dos componentes.

4.7 Instalação do Protótipo

O protótipo foi implementado na mesa central do Laboratório de Tecnologias Inovadoras, onde os usuários participantes desta pesquisa simularam o uso do sistema ao entrar e sair do laboratório.

Figura 18 – Protótipo implementado no Laboratório de Tecnologias Inovadoras

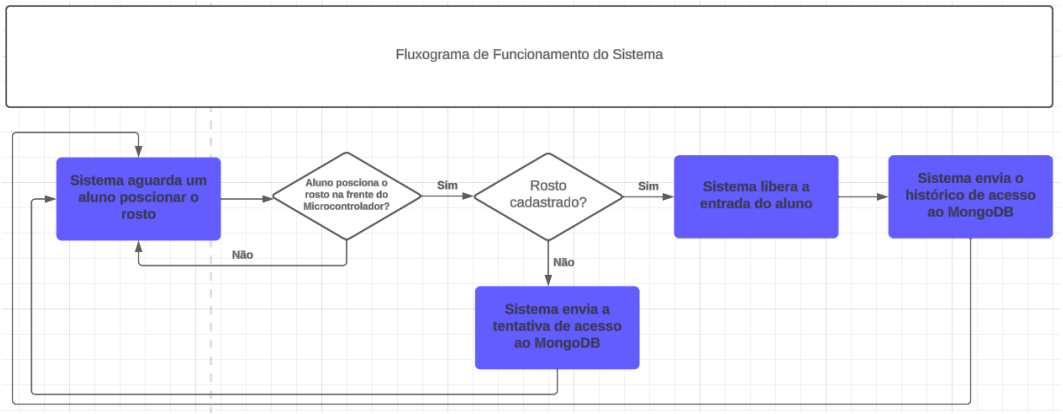
Fonte: Feito pelo Autor.

4.8 Funcionamento do Sistema

O sistema desenvolvido funciona da seguinte maneira:

1. Um aluno posiciona seu rosto em frente ao módulo *Raspberry Pi*. O microcomputador por sua vez inicia a verificação.
2. O código de reconhecimento facial verifica primeiramente se o rosto posicionado está cadastrado e logo em seguida começa a verificação de piscadas
3. Caso o aluno seja identificado e as verificações aprovados, o sistema liga o relé que abre a porta.
4. Após aberturá da porta, o sistema registra em um banco de dados *MongoDB* a data, horário e usuário que acessou para fins de registro.

Figura 19 – Fluxograma de Funcionamento do Sistema



Fonte: Feito pelo Autor.

5 RESULTADOS

Este capítulo apresenta os resultados obtidos a partir da análise dos dados coletados por meio de um formulário enviado aos participantes. A pesquisa teve como objetivo avaliar a aceitação e experiência dos usuários em relação ao sistema de Reconhecimento Facial implementado.

5.1 Perfil dos Participantes

Os participantes da pesquisa foram recrutados entre os estudantes do curso de Ciência da Computação e Engenharia de Software da Universidade Federal do Ceará - Campus Russas, que concordaram em participar voluntariamente. Um total de 5 estudantes participaram da pesquisa.

5.2 Respostas à Pesquisa

5.2.1 Concordância com o Termo de Consentimento

Todos os participantes declararam concordar em participar da pesquisa, indicando um alto nível de aceitação em relação à utilização do sistema de Reconhecimento Facial.

5.2.2 Participação em Laboratórios

80% dos participantes informaram fazer parte de algum laboratório da Universidade Federal do Ceará - Campus Russas. Destes, 4 mencionaram o Laboratório de Tecnologia da Informação (LTI).

5.2.3 Experiência Geral de Utilização

A maioria dos participantes descreveu a experiência ao utilizar o sistema como "Fácil". Essa avaliação reflete uma recepção positiva em relação à usabilidade do sistema pelos usuários.

Com base nas respostas coletadas, pode-se resumir a experiência dos participantes ao utilizar o sistema de Reconhecimento Facial da seguinte forma:

– Fácil

- Interessante, apesar de algumas ocasiões de lentidão
- Tecnologia incrível, transmitindo confiança em relação à segurança de acessos a locais restritos. Além disso, destaca-se a capacidade de controlar o fluxo de entrada e saída em determinados locais. Altamente interessante!
- Ótima
- Inovadora

5.2.4 Avaliação dos Aspectos do Sistema

Quando perguntados sobre o que mais apreciaram no sistema, os usuários destacaram vários aspectos. A simplicidade do sistema foi unanimemente apreciada por todos. Além disso, a maneira como o sistema foi montado e os componentes utilizados também foram mencionados. A gestão de acessos foi outro ponto positivo, assim como a facilidade de uso. A velocidade de identificação do rosto também foi um aspecto que agradou aos usuários. No entanto, é importante notar que o design do sistema e a qualidade da câmera não agradaram dois participantes.

5.2.5 Dificuldades e Sugestões de Melhoria

Nenhum dos participantes relatou dificuldades na utilização do sistema. Dentre as sugestões de melhoria, dois participantes destacaram a estética do sistema como sugestão de melhoria e um participantes destacou a qualidade da câmera, indicando uma taxa geral baixa de problemas enfrentados.

5.2.6 Confiança no uso do Sistema

Todos os participantes declararam confiar na utilização do sistema no seu dia a dia, indicando um alto nível de aceitação em relação à utilização do sistema de Reconhecimento Facial.

5.3 Considerações

Os resultados desta pesquisa indicam uma aceitação geral positiva dos participantes em relação ao sistema de Reconhecimento Facial implementado. As sugestões de melhoria fornecidas pelos participantes serão consideradas na fase de aprimoramento contínuo do sistema, visando proporcionar uma experiência ainda mais satisfatória.

6 CONCLUSÃO

6.1 Considerações Finais

Esta monografia apresentou um sistema de gestão de acesso via Reconhecimento Facial. Inicialmente, foi selecionado um grupo restrito de usuários para o teste do sistema, sendo 80% membros do Laboratório de Tecnologias Inovadoras (LTI). Para a escolha do algoritmo de detecção, foi utilizada a base de Yale (BELITSKAYA, 2018), onde se concluiu que o algoritmo *Fisherfaces* tinha melhor desempenho. Para o treinamento do classificador, foram utilizadas fotos capturadas dos membros da pesquisa.

Com os resultados obtidos neste trabalho, pode-se concluir que o sistema implementado, utilizando o algoritmo *Fisherfaces*, foi capaz de classificar satisfatoriamente os membros da pesquisa. Além disso, os resultados obtidos pelos feedbacks dos membros da pesquisa, mostram que o sistema é fácil de usar e eficiente.

6.2 Desafios

O principal objetivo descrito no Trabalho de Conclusão I era desenvolver um sistema de reconhecimento facial utilizando o *hardware* do microcontrolador *ESP-32-CAM*. No entanto, uma série de desafios fez com que o objetivo principal fosse alterado na reta final do projeto.

Foi proposto utilizar um computador externo para executar o código de visão computacional em conjunto com o microcontrolador, que atuaria como coletor de imagens e controlaria os atuadores, utilizando comunicação serial. Esta abordagem teve sucesso, mas o ESP-32-CAM não conseguiu lidar com a extração das imagens, inicialmente travando e posteriormente quase pegando fogo devido à alta temperatura atingida por ele, o que inviabilizou o andamento do projeto.

Além disso, após a implementação do sistema no *Raspberry Pi*, enfrentou-se dificuldade com o reconhecimento de usuários que utilizavam acessórios, como óculos e bonés. Para resolver esse problema, foi realizada a captura e treinamento tanto com os acessórios quanto sem eles.

6.3 Trabalhos Futuros

A construção de uma aplicação web para o cadastro de novos usuários e o acompanhamento do histórico de acesso, além de ao invés de utilizar modelos clássicos, utilizar redes neurais convolucionais e utilizar validação cruzada na etapa de validação, são ideais de trabalhos futuros. Com o intuito de facilitar o trabalho do gestor do laboratório ao adicionar um novo membro ao laboratório.

REFERÊNCIAS

ACADEMY, D. S. **Segmentação de Imagens Médicas com Deep Learning**. 2022. Disponível em: https://blog.dsacademy.com.br/segmentacao-de-imagens-medicas-com-deep-learning/. Acesso em: 20 jun. 2023.

AHONEN, T. **Face Recognition with Local Binary Patterns.** [*S. l.*]: European Conference on Computer Vision, 2004. 469–481 p.

BAKSHI, M. R. S. U. A survey on face detection methods and feature extraction techniques of face recognition. **Journal of Emerging Trends Technology in Computer Science (IJETTCS)**, IJETTCS, p. 233–237, 2014.

BELITSKAYA, O. **Yale Face Database**. 2018. Disponível em: https://www.kaggle.com/datasets/olgabelitskaya/yale-face-database. Acesso em: 04 nov. 2023.

BESL P. J., . J. R. **FThree-dimensional object recognition. Computing Surveys.** [*S. l.*]: ACM Comput. Surv., 1985. 145 p.

CEHOVIN ROK MANDELJC, V. S. L. Real-time eye blink detection using facial landmarks. **Computer Vision Winter Workshop**, IJETTCS, p. 1–4, 2016.

DAVE, G. Face recognition in mobile phones. **Department of Electrical Engineering Stanford University**, 2010.

DIGITAL, D. **Um computador capaz de identificar um assalto e chamar a polícia? Uma das habilidades da visão computacional. Conheça!** 2015. Disponível em: https://www.dtidigital.com.br/blog/deteccao-de-movimentos-suspeitos-por-visao-computacional. Acesso em: 20 jun. 2023.

DINIZ, F. Um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces. **Revista Brasileira de Computação Aplicada**, 2013.

GARCIA, G. B. **Learning Image Processing with OpenCV.** [*S. l.*]: PACKT, 2015. 19–23 p.

GARZON, M. Human detection from a mobile robot using fusion of laser and vision information. **PubMed**, 2013.

GRYFO. **Reconhecimento facial para proteção de acesso a dados sensíveis**. 2023. Disponível em: https://gryfo.com.br/blog/2023/02/07/protecao-acesso-dados-sensiveis/#:~:text=Segundo%20a%20Lei%20Geral%20de,reconhecimento%20facial%20s%C3%A3o%20dados%20sens%C3%ADveis. Acesso em: 20 jun. 2023.

GUSMAO, A. L. d. S. C. e. R. d. F. Z. Arthur Trindade Abreu de. Fechadura baseada em reconhecimento facial via dispositivos móveis android. **XXXIV Simpósio Brasileiro de Telecomunicações**, 2016.

JONES, P. V. M. Rapid object detection using a boosted cascade of simple features. **Conference on Computer Vision and Pattern Recognition**, 2001.

LOPES, M. T. L. F. B. Proposta de aplicativo para controle de fluxo de trânsito usando arduino e câmera com opencv. **Departamento de Pós-graduação - Faculdade Cidade Verde (FCV)**, 2016.

MACIEL, A. L. A. H. S. Sistema para controle de acesso e automação em prédios inteligentes. **Reunião Anual da Sociedade Brasileira para o Progresso da Ciência**, 2018.

NASA. **MARS Exploration Rovers**. 2018. Disponível em: https://mars.nasa.gov/mer/. Acesso em: 04 nov. 2023.

NOGUEIRA, F. G. d. S. G. R. G. Desenvolvimento de protótipo de fechadura eletrônica com reconhecimento facial. **Instituto de Educação, Ciência e Tecnologia do Piauí (IFPI)**, 2019.

OJALA, T. **A comparative study of texture measures with classification based on featured distributions.** [*S. l.*]: Pattern recognition, 1996. 51–59 p.

OPENCV. **Cascade Classifier**. 2022. Disponível em: https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html. Acesso em: 04 nov. 2023.

S., B. G. **Face Detection with Haar Cascade**. 2020. Disponível em: https://towardsdatascience.com/face-detection-with-haar-cascade-727f68dafd08. Acesso em: 04 nov. 2023.

SANTINO. **Como a tecnologia de reconhecimento facial é usada mundo afora**. 2019. Disponível em: https://olhardigital.com.br/2019/06/21/videos/como-a-tecnologia-de-reconhecimento-facial-e-usada-mundo-afora/. Acesso em: 13 jun. 2023.

SANTOS M., C. M. Detecção de padrões em imagens através de histogramas de gradientes orientados e classificadores lineares do tipo svm. **Universidade Federal de Uberlândia**, 2020.

SILVA, A.

Redução de Características para Classificação de Imagens de Faces, 2016.

SILVA, F. S. O. Leonardo Claudio de Paula e. Sistema autônomo e inteligente de reconhecimento facial para autorização de entrada de pessoal em ambientes restritos. **Mostra Nacional de Robótica (MNR)**, 2022.

SZELISKI, R. **Computer Vision: Algorithms and Applications.** [*S. l.*]: Springer, 2011. 14 p.

TYAGI, M. **HOG (Histogram of Oriented Gradients): An Overview**. 2021. Disponível em: https://towardsdatascience.com/hog-histogram-of-oriented-gradients-67ecd887675f. Acesso em: 04 nov. 2023.

YE, L. Investigation of facial age estimation using deep learning. **UPPSALA UNIVERSITET**, 2022.

ZHAO, W. e. a. **Face recognition: A literature survey.** [*S. l.*]: ACM Comput. Surv., 2003. 399–458 p.