UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE ITAPAJÉ

CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

THAÍS DE ANDRADE CASTRO

UMA PROPOSTA PARA A AVALIAÇÃO DE DESEMPENHO DE ALGORITMOS DE RECONHECIMENTO FACIAL

ITAPAJÉ

2024

THAÍS DE ANDRADE CASTRO

UMA PROPOSTA PARA A AVALIAÇÃO DE DESEMPENHO DE ALGORITMOS DE RECONHECIMENTO FACIAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do Campus de Itapajé da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Segurança da Informação.

Orientador: Prof. Dr. João Henrique Corrêa

ITAPAJÉ

2024

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)

C353p Castro, Thaís de Andrade.
Uma proposta para a Avaliação de desempenho de algoritmos de reconhecimento facial / Thaís de Andrade Castro. – 2024.
44 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Itapajé, Curso de Segurança da Informação, Fortaleza, 2024.
Orientação: Prof. Dr. João Henrrique.

1. Reconhecimento facial. 2. Eingenface. 3. Fisherface. 4. LBPH. I. Título.

CDD 005.8

THAÍS DE ANDRADE CASTRO

UMA PROPOSTA PARA A AVALIAÇÃO DE DESEMPENHO DE ALGORITMOS DE RECONHECIMENTO FACIAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do Campus de Itapajé da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Segurança da Informação.

Aprovada em: 26/09/2024

BANCA EXAMINADORA

Prof. Dr. João Henrique Corrêa (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Juan Sebastian Toquica Arenas
Universidade Federal do Ceará (UFC)

Prof. Dr. Israel Barros
Universidade Federal do Ceará (UFC)

Dedico este trabalho à minha família, professores e amigos, que sempre acreditaram em mim e investiram no meu crescimento. Sua confiança, apoio e encorajamento foram fundamentais para que eu superasse os desafios e alcançasse meus objetivos. Sou profundamente grata por tê-los ao meu lado nessa jornada.

AGRADECIMENTOS

Agradeço ao meu orientador, Dr. João Henrique Corrêa, que sempre me guiou com calma e paciência, especialmente nos momentos de inquietação, ajudando-me a focar no que realmente importava ao longo dessa trajetória. Ele esteve presente desde o início da minha graduação, como orientador da minha turma, inspirando-me e apoiando-me nos momentos difíceis.

À professora Elisângela, que sempre me auxiliou a lidar com as burocracias da vida acadêmica e que, além de uma excelente professora, tornou-se uma grande amiga.

Aos meus queridos amigos, Gabriel Barreto, João Filho e Maria Alyce, que espero levar além dessa fase acadêmica. Eles estiveram presentes em todos os momentos, tornando os dias difíceis mais leves. Serei uma pessoa mais feliz se levar comigo, em cada etapa da vida, as lembranças que cultivei ao lado deles.

Aos meus amigos de Ciência de Dados, João Davi, Bianca Sousa, Bruna Barreto, Thays Uchôa, Vanessa Mesquita e Eryca, que, mesmo pertencendo a outro curso, sempre estiveram ao meu lado, tornando os dias menos cansativos e mais alegres.

Ao meu querido irmão, Tiago de Andrade, que sempre me acalmou e nunca me deixou desistir.

Por fim, aos amigos do PET (Programa de Educação Tutorial), que aceitaram participar do meu projeto com paciência e foram ótimos companheiros nessa jornada.

“When will you realize, Vienna waits for you?,Slow down, you’re doing fine’

(Joel, 1977)

RESUMO

A tecnologia tem evoluído rapidamente, transformando o que antes era considerado futurista em algo comum e acessível. No entanto, apesar de tornar a vida mais prática, ela também traz desafios de segurança, especialmente no que diz respeito à proteção de dados.

Nesse contexto, o reconhecimento facial é uma ferramenta em crescente discussão, surge como uma solução que visa equilibrar praticidade e segurança.

Este trabalho explora o uso do reconhecimento facial em um ambiente acadêmico. O processo envolve três etapas principais: aquisição da imagem, comparação com um banco de dados e decisão final. Cada uma dessas etapas é crucial para garantir que o sistema funcione de forma segura e eficiente.

Embora o reconhecimento facial ofereça uma solução inovadora, ele não está isento de desafios. Este estudo busca não apenas construir um sistema funcional de reconhecimento facial. Sendo assim, este estudo busca construir um sistema funcional de reconhecimento facial.

Palavras-chave: reconhecimento facial; eingenface, fisherface; LBPH.

ABSTRACT

Technology has evolved rapidly, transforming what was once considered futuristic into something common and accessible. However, despite making life more practical, it also brings security challenges, especially when it comes to data protection.

In this context, facial recognition is a tool under increasing discussion, emerging as a solution that aims to balance practicality and security.

This work explores the use of facial recognition in an academic environment. The process involves three main steps: image acquisition, comparison with a database and final decision. Each of these steps is crucial to ensuring the system operates safely and efficiently.

While facial recognition offers an innovative solution, it is not without its challenges. This study seeks not only to build a functional facial recognition system. Therefore, this study seeks to build a functional facial recognition system.

Keywords: facial recognition; eingenface, fisherface; LBPH.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a segurança tornou-se uma questão crucial na vida cotidiana, mas, mesmo sendo amplamente debatida, parece que nunca é suficiente. Conforme discutido por P.W. Singer e Allan Friedman em seu livro "Cybersecurity and Cyberwar: What Everyone Needs to Know", a segurança é essencial para qualquer sociedade moderna. À medida que a tecnologia avança, as soluções de segurança devem evoluir para enfrentar novas ameaças. Portanto, é necessário desenvolver novas formas de segurança e mantê-las atualizadas, de modo que não se tornem obsoletas.(SINGER; FRIEDMAN,)

Além de inovadora, a segurança na era atual precisa ser prática, permitindo que as pessoas utilizem essas tecnologias de maneira funcional, evitando, problemas e dificuldades. As tecnologias de Internet das Coisas (IoT) são um exemplo claro disso, ao proporcionar mais facilidade e conveniência no uso cotidiano.

Muitas dessas inovações são viabilizadas pelo uso do Aprendizado de Máquina, que é uma área da inteligência artificial dedicada ao desenvolvimento de algoritmos que permitem que computadores aprendam a partir de dados e realizem previsões ou tomem decisões sem instruções explícitas. Isso impulsionou o surgimento de técnicas como o reconhecimento facial, que se tornaram cada vez mais úteis e acessíveis à sociedade. Agora, em vez de depender de senhas complexas ou dispositivos de autenticação, as pessoas podem usar o próprio rosto como meio de identificação.

O reconhecimento facial destaca-se como uma ferramenta poderosa de segurança, adicionando uma camada adicional de proteção a diversos sistemas. Seu uso tem sido amplamente adotado em aplicativos, serviços e plataformas que requerem autenticação. No entanto, a biometria facial enfrenta desafios relacionados à sua implementação e ao respeito à privacidade. Conforme a Electronic Frontier Foundation (EFF), apesar dos benefícios do reconhecimento facial, sua adoção deve ser feita com cautela para garantir a privacidade dos indivíduos e evitar abusos.(GRECO,) Assim, é fundamental haver uma documentação adequada, como termos de consentimento, que assegurem o uso legal das imagens dos usuários, conforme leis como a Lei Geral de Proteção de Dados (LGPD).

A LGPD estabelece que a proteção de dados pessoais é baseada em princípios fundamentais, como a inviolabilidade da intimidade, honra e imagem. Como a imagem é considerada um dado biométrico, e, portanto, sensível, ela recebe um tratamento especial na legislação, garantindo que sua utilização seja regulada para proteger os direitos dos indivíduos.

Diante deste cenário, o **objetivo geral** deste trabalho é desenvolver um algoritmo de reconhecimento facial utilizando as técnicas Eigenface, Fisherface e LBPH, com o intuito de explorar e aprimorar a segurança e a identificação de pessoas por meio de mecanismos de reconhecimento facial. Este sistema será projetado para otimizar a identificação em diversos contextos, avaliando o desempenho dos algoritmos aplicados.A partir do objetivo geral, foram estabelecidos os seguintes objetivos específicos:

a) analisar os principais algoritmos de reconhecimento facial (Eigenface, Fisherface e LBPH) em termos de desempenho e eficiência;
b) desenvolver um sistema de reconhecimento facial que aplique esses algoritmos, com foco na segurança e precisão;
c) avaliar a eficácia do sistema e a qualidade do reconhecimento facial;
d) propor melhorias futuras com base nos resultados obtidos durante o desenvolvimento e teste do sistema.

Este trabalho será organizado da seguinte forma: O Capítulo 2 revisará a literatura sobre os algoritmos de reconhecimento facial, enquanto o Capítulo 3 descreverá a metodologia aplicada no desenvolvimento e implementação do sistema. O Capítulo 4 apresentará os resultados práticos e suas análises, e o Capítulo 5 concluirá com um resumo das principais descobertas e sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Esta seção apresenta um estudo dos principais conceitos relacionados ao tema tratado, fornecendo uma base teórica para compreender os aspectos relevantes à pesquisa. São abordados tópicos essenciais, como segurança da informação e suas práticas fundamentais, bem como técnicas e ferramentas específicas que sustentam as análises e discussões propostas. O embasamento teórico busca contextualizar o estudo dentro da literatura existente, fornecendo uma visão geral dos conceitos necessários para a compreensão dos objetivos e das metodologias aplicadas.

2.1 Segurança da Informação

A segurança da informação visa proteger todos os ativos em um ambiente, incluindo softwares, ambientes físicos e dados. Contudo, essa proteção não se restringe apenas a aspectos tecnológicos, mas também envolve elementos humanos e sociais, como discute Ross Anderson (ANDERSON, 2020). Isso demonstra que a segurança precisa ser incorporada em diferentes contextos, abrangendo diversas subáreas que complementam o seu escopo.

A área da segurança da informação é composta por uma série de disciplinas que podem ser administradas por um ou vários indivíduos, como descrito no livro Segurança dos Sistemas de Informação. Essas disciplinas incluem segurança de redes, segurança física, segurança de computadores, segurança do pessoal, segurança aplicacional, criptografia, gestão de projetos, formação e conformidade, entre outras (SILVA,). Isso evidencia que a segurança da informação pode ser vista como um conjunto de vertentes interligadas, todas baseadas em pilares comuns.

De acordo com uma revisão realizada pela Treinaweb, a segurança da informação se fundamenta em três pilares principais: confidencialidade, integridade e disponibilidade. Esses pilares orientam as práticas de proteção de dados nas empresas (GUEDES,).

O pilar da confidencialidade está relacionado à privacidade dos dados, para restringir o acesso apenas às pessoas autorizadas. Já a integridade se refere à preservação da veracidade e confiabilidade das informações, assegurando que elas permaneçam inalteradas sem a devida autorização. A disponibilidade, por sua vez, garante que os dados e sistemas estejam sempre acessíveis a usuários ou processos autorizados, evitando interrupções que possam prejudicar a operação e a tomada de decisões.

Além desses três pilares tradicionais, outras literaturas, como A Guide to Building

Dependable Distributed Systems, apresentam pilares adicionais que também são essenciais para a segurança em ambientes físicos ou virtuais (ANDERSON, 2020). Entre esses, destaca-se a autenticidade, que visa assegurar que os dados realmente pertençam à fonte anunciada, evitando que remetentes se passem por terceiros ou que a mensagem seja alterada durante o envio. A autenticação de usuários, como o uso de login e senha, é um exemplo de prática nesse contexto.

A legalidade é outro aspecto fundamental, relacionada à conformidade com a legislação de segurança da informação. Empresas devem garantir que suas práticas estejam conforme as exigências legais, como a Lei Geral de Proteção de Dados (LGPD), que impõe maiores rigor e conformidade (SILVA,).

Por fim, conceitos como o não repúdio, que assegura que um indivíduo não possa negar a autoria de uma ação, e a autorização, que define as permissões de usuários num sistema, também são cruciais. No caso da autorização, é importante que usuários comuns não tenham acesso às funções e permissões reservadas aos administradores, garantindo a segurança do sistema.

Esses pilares e princípios fornecem a base teórica para a implementação da segurança da informação, mostrando que ela envolve uma abordagem ampla, englobando aspectos técnicos, jurídicos e organizacionais.

Além dos pilares mencionados, é fundamental considerar o impacto da Lei Geral de Proteção de Dados (LGPD) e a importância das questões éticas no contexto da segurança da informação (BRASIL, 2018). A LGPD estabelece normas rigorosas para a coleta, armazenamento e tratamento de dados pessoais, enfatizando a necessidade de consentimento explícito dos indivíduos para o uso de suas informações. Isso se alinha diretamente aos princípios de confidencialidade e integridade, garantindo que dados sejam mantidos de forma precisa e acessível apenas a pessoas autorizadas. A conformidade com essa legislação não apenas ajuda as organizações a evitar penalidades, mas também fortalece a confiança dos usuários, demonstrando que suas informações estão sendo tratadas com respeito e responsabilidade. Portanto, a segurança da informação deve incorporar não apenas aspectos técnicos, mas também uma compreensão ética e legal que promova a proteção dos dados pessoais em um ambiente digital cada vez mais complexo.

2.2 Inteligência Artificial

Atualmente, é difícil encontrar uma área na qual a inteligência artificial (IA) não esteja presente. No entanto, o entendimento de seu funcionamento ainda é complexo para a maioria da população, o que reforça a importância de esclarecer brevemente como ela opera.

A inteligência artificial refere-se a sistemas ou máquinas que podem simular a capacidade humana de pensar, aprender, raciocinar e tomar decisões. Trata-se de um campo da ciência que busca desenvolver algoritmos e modelos capazes de realizar tarefas que, normalmente, exigiriam inteligência humana. Em resumo, a IA se refere à criação de sistemas projetados para aprender, adaptar-se e tomar decisões com base em dados e algoritmos específicos.

Ao longo do tempo, diferentes linhas de pensamento foram propostas para definir a inteligência artificial. Rich e Knight, por exemplo, afirmam que a IA é o estudo de como fazer os computadores realizarem tarefas que, até então, os seres humanos realizavam melhor (RICH, 1993). Essa definição implica que as máquinas precisam agir de forma semelhante aos seres humanos, mas reconhece que ainda existem problemas que não podem ser solucionados nem por pessoas, nem por máquinas. Mesmo assim, ela oferece uma ideia clara sobre o que é inteligência artificial.

Seguindo essa mesma linha, Alan Turing, em 1950, propôs o famoso Teste de Turing. Esse teste foi desenvolvido para demonstrar como as máquinas poderiam evoluir a ponto de, um dia, serem confundidas com seres humanos (MAGALDI, 2019). Essa proposta de Turing sugere uma visão futurista de máquinas capazes de interagir de maneira tão natural que suas respostas não poderiam ser facilmente diferenciadas das de um ser humano.

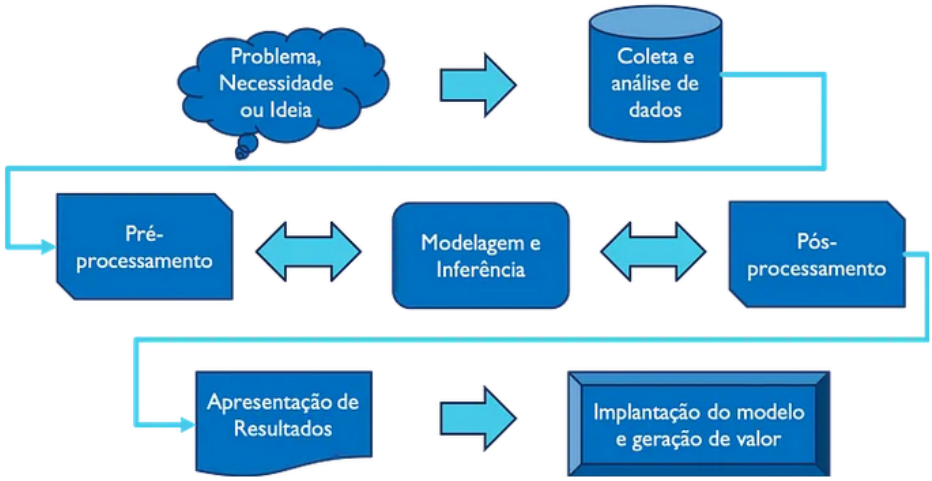
2.3 Aprendizado de Máquina

O livro **Machine Learning** (ZHOU,) apresenta a ideia de que, assim como os humanos, as máquinas também aprendem por meio da experiência. Para as máquinas, os dados funcionam como essas experiências, e é a partir delas que os modelos são construídos (ZHOU,). No contexto do reconhecimento facial, as imagens são as experiências que alimentam esse aprendizado, e é por esse motivo que o processo de aprendizado de máquina tem sido crucial, proporcionando alta precisão.

O conceito dessa subárea da inteligência artificial é destacado pelo livro *"Pattern Recognition and Machine Learning"* de Christopher M. Bishop, que explica que o aprendizado

de máquina surge da necessidade de processar e obter informações úteis a partir dos dados. De acordo com essa explicação, a crescente abundância de dados torna inviável realizar manualmente o processamento e a análise, o que cria a necessidade de automação, simulando o comportamento humano. Nesse sentido, o aprendizado de máquina pode ser definido como o uso de algoritmos para extrair informações de dados brutos e representá-los por meio de modelos matemáticos (BISHOP, 2006). Para entender melhor o aprendizado de máquina é necessário entender como ele funciona. A Figura 1, mostra o processo de um aprendizado de máquina

Figura 1 – Processo do aprendizado de máquina.



Fonte: (ESCOVEDO; KOSHIYAMA, 2020)

O aprendizado de máquina pode ser dividido em dois tipos:

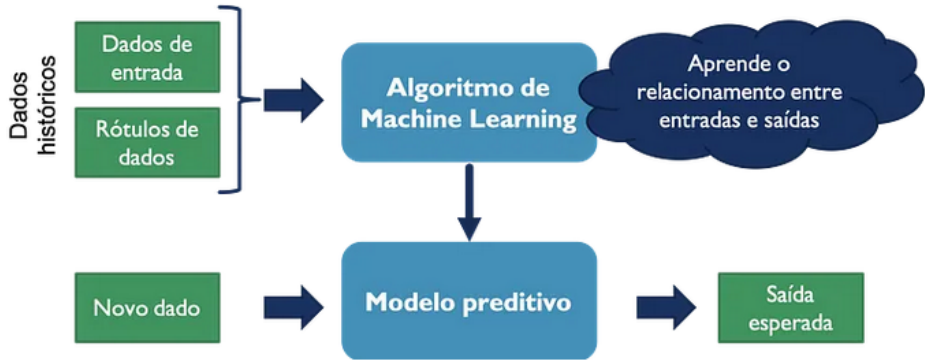
2.3.1 Aprendizado supervisionado

No aprendizado supervisionado, o modelo ou algoritmo é construído a partir de um conjunto de dados de entrada, conhecido como dataset, onde são apresentados pares ordenados de entrada e saída desejada. Esses dados são rotulados, pois a saída esperada para cada entrada é conhecida de antemão (BISHOP, 2006). Esses dados são divididos em dois grupos: treinamento e teste, também conhecido como conjunto de validação. O objetivo dessa divisão é verificar como o modelo se comporta com dados que não foram vistos anteriormente, permitindo ajustes, se necessário, antes de aplicá-lo em novos dados cuja saída esperada ainda não é conhecida (BISHOP, 2006).

A Figura 2, mostra como funciona essa organização de uma maneira mais visual.

O aprendizado supervisionado pode ser dividido em dois tipos principais: classificação e regressão. Conforme o livro "*Machine Learning: A Probabilistic Perspective*"de Kevin

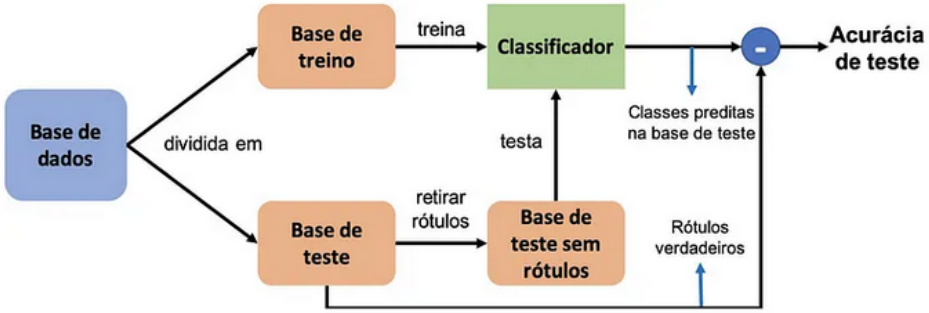
Figura 2 – Divisão de dados em treinamento e teste.



Fonte: (ESCOVEDO; KOSHIYAMA, 2020)

P. Murphy, a classificação é um modelo de aprendizado supervisionado usado para prever a categoria ou classe à qual um determinado ponto de dados pertence. Esse modelo é amplamente aplicado em tarefas como detecção de spam, análise de sentimentos e reconhecimento de imagens, onde o objetivo é associar um rótulo específico a um conjunto de características observadas (MURPHY, 2012). A figura 3 abaixo mostra isso.

Figura 3 – Etapas do processo de classificação.



Fonte: (ESCOVEDO; KOSHIYAMA, 2020)

Após a divisão dos processos, o sistema torna-se mais robusto e adaptável às necessidades específicas de cada problema. Em seguida, ocorre a verificação do desempenho desse processo. Uma forma comum de medir o desempenho é por meio da acurácia, que representa o percentual de acertos do classificador (BISHOP, 2006). Além disso, outra métrica amplamente utilizada é a matriz de confusão, que detalha o desempenho do modelo de classificação, fornecendo informações sobre classificações corretas e incorretas para cada classe. A matriz de confusão também permite calcular outras métricas importantes, como Falsos Positivos, Falsos Negativos, Verdadeiros Positivos e Verdadeiros Negativos (BISHOP, 2006).

Já o processo de regressão é utilizado para prever valores contínuos, sendo aplicado em situações que exigem a estimativa de uma quantidade específica, como preços de imóveis

ou previsões de vendas. As métricas mais comuns para avaliar modelos de regressão incluem o erro quadrático médio (MSE) e o coeficiente de determinação (R^2), que medem a precisão das previsões (MURPHY, 2012).

2.3.2 Aprendizado não supervisionado:

Segundo o livro "The Elements of Statistical Learning: Data Mining, Inference, and Prediction"de Trevor Hastie, Robert Tibshirani, e Jerome Friedman., o aprendizado não supervisionado é descrito como um método em que o modelo trabalha com dados sem rótulos ou respostas corretas, identificando padrões e grupos de maneira autônoma. Uma aplicação comum desse tipo de aprendizado é a redução de dimensionalidade, que simplifica dados complexos, preservando informações importantes (HASTIE *et al.*, 2009).

2.4 Visão Computacional

Algo que pode parecer simples para os humanos é, na verdade, uma tarefa bastante complexa para máquinas. Um exemplo disso pode ser visto no livro "*Computer Vision: Algorithms and Applications*"de Richard Szeliski, que discute a capacidade dos olhos humanos. Especialista afirmam que, se fosse possível quantificar a definição da imagem que vemos com nossos olhos, ela teria aproximadamente 274 megapixels — 137 em cada olho. Isso ressalta como tarefas naturais e aparentemente fáceis para os humanos envolvem uma complexidade considerável quando traduzidas para a visão computacional (SZELISKI, 2010).

Estudos como o de Backes e Junior, em seu livro sobre visão computacional, explicam que o processo vai muito além de apenas captar imagens. A visão computacional envolve a aquisição visual seguida de diversas etapas, como aprimoramento da imagem, remoção de ruídos, aumento de contraste, segmentação de objetos de interesse e extração de características como forma, cor e textura. Além disso, as imagens captadas são comparadas com outras já vistas para criar uma compreensão mais completa (BACKES, 2016).

A Figura 4, mostra como funciona o processo de visão computacional de uma forma mais visual.

Este livro cita que a visão computacional possui várias etapas que podem ser divididas da seguinte forma:

a) aquisição: responsável pela captura da imagem, como a utilização de câmeras nesse

caso em particular, mas podem ser scanners, filmadoras, etc;

b) processamento de Imagem: responsável por melhorar a imagem, tirar ruídos, salientar bordas e suavizar a imagem. Essa fase pode ser umas das partes finais para fornecer uma imagem melhorada para as próximas fases, essa fase também é conhecida como pré-processamento;
c) segmentação: responsável por extrair a parte principal da imagem como, por exemplo, uma análise de componentes principais;
d) extração de características: obtém um conjunto de características da imagem, a parte de identificação;
e) reconhecimento de padrões: responsável por enquadrar a foto a um grupo de acordo com seus padrões como, por exemplo, a classificação por classes;

Figura 4 – Etapas do processo de visão computacional.

Fonte: (BACKES; MESQUITA, 2019)

2.5 Reconhecimento Facial

Os primeiros sistemas de reconhecimento facial utilizavam características geométricas como pontos de referência com base na localização e distância entre diferentes partes do rosto, formando assim um vetor de características. No entanto, apesar de existirem diversas maneiras de extrair informações faciais e produzir uma assinatura facial, o processo é mais complexo do que pode parecer à primeira vista.

Nunes, em seu trabalho sobre reconhecimento facial biométrico em nuvens de pontos tridimensionais, menciona que as características biométricas, como a face, são amplamente estudadas atualmente no campo da autenticação. Ele afirma que o reconhecimento facial é um tipo de recurso biométrico com grande potencial para autenticação, ao lado de outras características

como digitais, íris e geometria das mãos (NUNES,).

Para os humanos, reconhecer essas características é algo automático, mas para as máquinas, o processo envolve lidar com grandes quantidades de dados, o que torna o reconhecimento facial um desafio que tem sido desenvolvido ao longo do tempo. Ainda assim, essa tecnologia oferece inúmeras vantagens. Um artigo sobre técnicas de reconhecimento facial através da inteligência artificial destaca que uma das principais vantagens desse método é que ele não requer a participação ativa do usuário, já que as imagens podem ser capturadas a diferentes distâncias, o que é especialmente útil em contextos de segurança e vigilância. Além disso, o artigo menciona que a detecção da face em uma imagem pode otimizar o desempenho dos sistemas de reconhecimento, economizando tempo ao identificar previamente os elementos de interesse antes da análise detalhada (FERNANDES JESSICA MARTINS,).

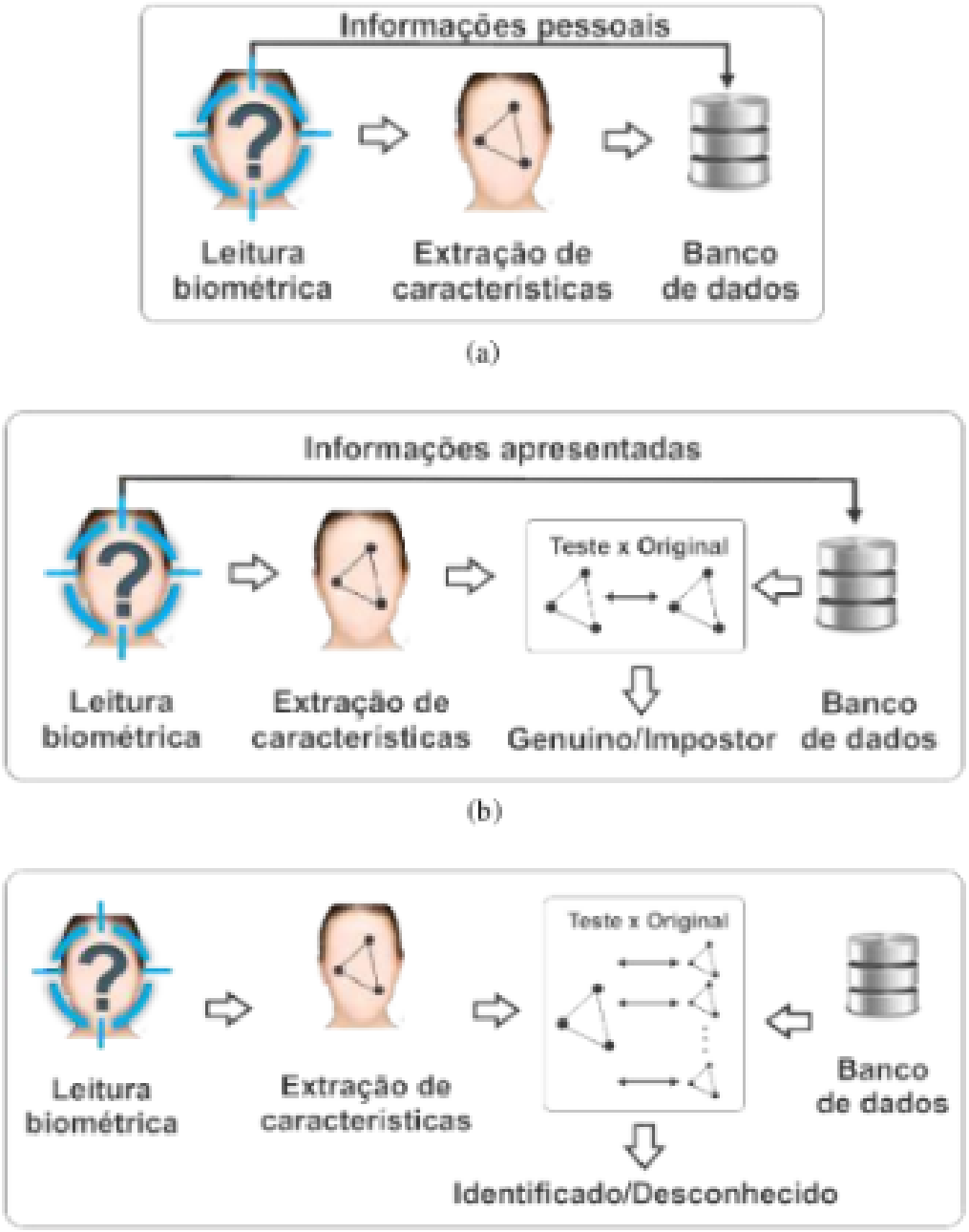
O processo de reconhecimento facial pode ser dividido em três etapas principais: registro, verificação e identificação biométrica, como descrito por Silva e Cintra em seu estudo sobre padrões faciais (BELUCO, a). Essas etapas são fundamentais para sistemas de controle de acesso e verificação de identidade, especialmente em contextos de segurança.

A Figura 5, a seguir ilustra essas etapas detalhadamente. Na primeira etapa, características biométricas, como contornos faciais e distâncias entre os olhos, são extraídas e convertidas em formato digital para armazenamento em um banco de dados seguro. Posteriormente, durante a autenticação, os dados capturados são comparados com as informações armazenadas, garantindo que o indivíduo é realmente quem afirma ser. A precisão dessa comparação depende da qualidade dos dados e do algoritmo utilizado, o que torna essa abordagem eficaz e prática para diversas aplicações (SILVA; CINTRA,).

2.6 Detecção de Faces

A detecção de faces é uma etapa fundamental no processo de reconhecimento facial, pois identifica a localização e o tamanho das faces em uma imagem, preparando-as para fases posteriores, como a própria etapa de reconhecimento. De acordo com Lopes, essa detecção desempenha um papel crucial, já que localizar a face antes de analisar suas características específicas economiza esforço computacional. Isso ocorre porque muitos algoritmos analisam a imagem completa em busca de características, e ao detectar a face antecipadamente, a análise subsequente pode ser focada apenas na região de interesse, otimizando o processo.(LOPES; FILHO, 2005)

Figura 5 – Etapas do processo de Reconhecimento facial.



Fonte: (BELUCO, b)

Os métodos de detecção de faces são classificados em várias categorias, cada uma com técnicas e abordagens distintas, adequadas para diferentes contextos e desafios do reconhecimento facial. Conforme demonstrado a seguir:

a) métodos baseados em conhecimento: Segundo (LOPES; FILHO, 2005), os métodos baseados em conhecimento aplicam regras pré-definidas para identificar características comuns das faces humanas, como os olhos, o nariz e a boca, que estão dispostos de forma específica no rosto. Esses métodos dependem de informações previamente

conhecidas sobre a estrutura das faces para realizar a detecção;

b) métodos baseados em características invariantes: de acordo com (YANG *et al.*,), os métodos baseados em características invariantes buscam identificar características da face que permanecem consistentes sob diferentes condições, como variações de iluminação. No entanto, esses métodos podem ser desafiados por distorções causadas por iluminação inadequada ou ruído na imagem, o que pode comprometer a detecção;

c) métodos baseados em modelos e aparência: segundo (LOPES; FILHO, 2005) também discutem os métodos baseados em modelos e aparência. Os métodos baseados em modelos envolvem a procura de correspondências na imagem com base em modelos geométricos simples, como círculos, quadrados ou triângulos, onde a detecção é realizada encontrando a melhor correspondência com uma função de energia. Diferentemente dos métodos baseados em conhecimento, os métodos baseados em aparência não dependem de informações prévias sobre o objeto ou suas características. Em vez disso, esses métodos utilizam aprendizado e treinamento, onde as informações necessárias para realizar a detecção são extraídas do próprio conjunto de imagens sem intervenção externa.

A detecção de faces é fundamental para o sucesso do reconhecimento facial, pois prepara a imagem para análise subsequente, limitando o foco a uma área específica e, assim, aumentando a precisão e a eficiência do sistema.

3 METODOLOGIA

O capítulo em questão fará a amostragem das etapas necessária para o processo de reconhecimento facial dentro do meio institucional. Este trabalho é desenvolvido de forma qualitativa, para criar um algoritmo capaz de fazer um processo de reconhecimento facial e selecionar a qual classe o individuo pertence. Para fortalecer este processo foi feito o embasamento mediante pesquisas bibliográficas por meio de sites, artigos e livros, conhecidos no ambiente de reconhecimento facial e controle de acesso, dessa forma deixando o processo mais confiável. Para chegar ao objetivo levantado inicialmente, foi necessário o levantamento de uma pesquisa sobre algoritmos utilizados no processo de reconhecimento facial, onde se chegou a três tipos de tecnologias amplamente utilizadas nesse mercado: LBPH*(Local Binary Patterns Histograms)*, Fisherface, Eingenface. O processo metodológico utilizado durante o desenvolvimento deste trabalho é composto por algumas etapas que são:

a) autorização do uso de imagem: antes do processo de coleta de imagens um documento foi formulado com o intuito de pedir a autorização das pessoas que iram ceder sua imagem em prol do projeto, no documento a pessoal concordava em ceder sua imagem para fins acadêmicos somente.O documento completo pode ser encontrado no Apêndice A;
b) coleta de dados: a partir de então foi feita a coleta de dados que consistia em um total de 225 imagens, inicialmente, de diversos discentes do campus. Esse conjunto diversificado de dados é essencial para garantir uma melhor desempenho do algoritmo. Para o processo de coleta de imagens algumas ponderações foram colocadas em prática, como o ambiente que a foto foi tirada, no caso em questão foi um ambiente iluminado onde a câmera pudesse capturar a imagem da pessoa nitidamente, as pessoas foram indicadas a fazer diferentes expressões e se caso fizessem uso de óculos que tirassem fotos com os óculos e sem eles. Desta maneira o processo de reconhecimento facial se torna mais eficaz;
c) pré-processamento de imagem: nesta etapa, foram adicionadas alguns filtros ao código para que as imagens tivessem uma qualidade maior, como o processo de iluminação, onde a foto só era registrada com uma qualidade adequada;
d) gerador de imagens: a partir da coleta de imagens foi feito o processo de geração de novas imagens, processo esse necessário para dividir o dataset em trino e teste, as imagens capturadas inicialmente, fizeram parte do treinamento e as imagens geradas

a partir das imagens de treinamento foram usadas para o processo de teste, o gerador de imagens fazia o processo de redimensionar a imagem em diferentes ângulos, aumentava sua luz, diminuia, aumentava a imagem ou diminuia caso necessário. Esta etapa foi feita com o intuito de aumentar o dataset, fazendo com que assim o código fique mais robusto;

e) detecção de imagem: para a detecção de imagem, utilizamos o classificador Haar Cascade, que é um método popular para a detecção de objetos, incluindo faces e olhos, em imagens. Esse classificador foi treinado com inúmeras imagens positivas (contendo o objeto a ser detectado) e imagens negativas (sem o objeto). A detecção foi realizada em duas etapas principais:
   - detecção de faces: a câmera capta imagens em tempo real, convertidas para escala de cinza para simplificar o processamento.A região detectada é marcada com um retângulo para facilitar a visualização;
   - detecção de olhos: após a detecção da face, a mesma técnica é aplicada para detectar os olhos dentro da região facial identificada.Essa detecção é útil para verificar se a face está posicionada corretamente para a captura, melhorando a precisão do reconhecimento.

f) treinamento: o treinamento teve como base os três algoritmos citados anteriormente, EigenFace, FisherFace, e LBPH. Cada um desses algoritmos tem características e desempenho específicos que são detalhados a seguir:
   - EigenFace: treinado utilizando as imagens capturadas em escala de cinza. Este algoritmo baseia-se na Análise de Componentes Principais (PCA), que reduz a dimensionalidade dos dados, mantendo as características mais relevantes;
   - FisherFace: o algoritmo FisherFace melhora o EigenFace ao considerar não apenas a variância nas imagens, mas também a discriminação entre classes. Ele utiliza LDA (Análise de Discriminantes de Fisher) para maximizar a separação entre as diferentes classes (indivíduos);
   - LBPH: trabalha ao nível de píxeis, capturando padrões de textura local em pequenas regiões da imagem. Ele cria um histograma para cada região e, em seguida, combina esses histogramas para representar a imagem facial. O LBPH é particularmente eficaz em condições variadas de iluminação e

expressões faciais.

g) teste: os modelos treinados foram testados utilizando um conjunto de imagens aumentado, gerado a partir das imagens originais. Esse aumento incluiu rotação, espelhamento, ajuste de brilho e zoom, para simular diversas condições reais. A precisão dos modelos foi avaliada utilizando métricas como acurácia, matriz de confusão e relatório de classificação. Essas métricas ajudam a entender o desempenho dos modelos em termos de falsos positivos, falsos negativos e a capacidade de distinguir entre diferentes classes;
h) comparação de desempenho e análise de resultados: foi realizado um estudo comparativo entre os três algoritmos de reconhecimento facial (EigenFace, FisherFace e LBPH). Essa análise permitirá avaliar qual algoritmo apresenta o melhor desempenho para a aplicação proposta, fornecendo resultados precisos para escolher o algoritmo mais adequado.

3.1 Modelo Proposto

O modelo proposto envolve o desenvolvimento de um algoritmo construído em Python, para realizar reconhecimento facial em um ambiente acadêmico. Utilizando técnicas de inteligência artificial, mais especificamente de visão computacional, o algoritmo é capaz de reconhecer faces e identificar se a pessoa é um professor ou aluno.

O processo ocorre da seguinte maneira: a primeira parte do código é responsável por captar 25 imagens de uma pessoa através da webcam. Essas imagens são convertidas para escala de cinza, e só serão realmente registradas se a luminosidade da imagem for superior a 110. Além disso, o código também verifica a presença de olhos na face detectada, garantindo que as imagens capturadas tenham uma qualidade adequada para o treinamento do modelo. As imagens são salvas em um formato específico, utilizando um identificador fornecido pelo usuário.

A segunda etapa do código consiste na geração de imagens aumentadas a partir das imagens originais capturadas na primeira etapa. Este processo é realizado para expandir o conjunto de dados, criando variações das imagens existentes para melhorar a robustez do algoritmo de reconhecimento facial. Nesta etapa, são geradas 9 imagens adicionais para cada pessoa, utilizando diferentes técnicas de processamento de imagens. As variações incluem:

a) rotação: as imagens são rotacionadas em ângulos variados, como 15, -15, 30, e -30 graus, para simular diferentes perspectivas;

b) espelhamento: as imagens são espelhadas horizontalmente, criando uma nova versão invertida da imagem original;
c) ajuste de brilho: o brilho das imagens é modificado para criar versões mais claras e mais escuras, utilizando fatores de brilho de 0.5 e 1.5. Isso ajuda o modelo a lidar melhor com variações de iluminação;
d) zoom: é aplicado um efeito de zoom, onde a imagem é cortada em torno do centro e depois redimensionada ao tamanho original, simulando aproximações e distanciamentos.

Essas técnicas de aumento de dados são implementadas para garantir que o modelo de reconhecimento facial seja treinado com uma variedade maior de exemplos, melhorando sua capacidade de generalização ao reconhecer faces sob diferentes condições.

Na próxima etapa do projeto, desenvolveu-se um código em Python para realizar o processo de reconhecimento facial utilizando os três algoritmos discutidos anteriormente: EigenFace, FisherFace e LBPH.

A seleção dos algoritmos Eigenface, Fisherface e LBPH para o presente estudo foi fundamentada em uma análise cuidadosa das suas características e eficiência em comparação com abordagens mais complexas, como Redes Neurais Convolucionais (CNNs) e técnicas de Deep Learning. Embora as CNNs tenham se mostrado altamente eficazes em diversas tarefas de reconhecimento facial, elas geralmente demandam um alto consumo de recursos computacionais, tornando-se menos viáveis em ambientes com limitações de hardware.

Em contrapartida, os algoritmos escolhidos apresentam um bom equilíbrio entre desempenho e eficiência, proporcionando uma solução mais acessível e rápida para a tarefa de reconhecimento facial. Além disso, sua implementação é mais simples e menos custosa, o que os torna adequados para aplicações práticas em contextos onde os recursos são limitados.

Em seguida, o código realiza o treinamento dos três algoritmos, utilizando as imagens coletadas. O modelo treinado é então salvo para ser utilizado na fase de testes. Na fase de teste, o código utiliza o modelo treinado para prever a categoria das imagens do conjunto de teste. A precisão do modelo é avaliada por métricas como acurácia, matriz de confusão e F1-score. Esses resultados são registrados e comparados para determinar qual dos algoritmos é mais eficaz para a aplicação proposta.

Por fim, o código gera uma matriz de confusão que visualiza o desempenho do modelo na classificação das categorias "professor"e "aluno". Essa visualização, juntamente

com as demais métricas, é fundamental para a análise comparativa entre os algoritmos LBPH, EigenFace, e FisherFace, a ser apresentada posteriormente.

3.2 Tecnologias utilizadas

Para o desenvolvimento do projeto em questão as seguintes tecnologias foram utilizadas:

a) opencv2 (Open Source Computer Vision Library): a biblioteca Opencv2 é uma das melhores alternativas quando se quer trabalhar com reconhecimento facial, isto porque esta biblioteca é muito utilizada quando se fala em algoritmos para visão computacional. Além do Opencv2 existem outras bibliotecas utilizadas para se trabalhar com este tema como TensorFlow, porém a biblioteca Opencv2 é mais popular em termos de aderência para iniciantes, além de ter um vasto material disponível; Está biblioteca tem como principal proposito a manipulação de imagens e vídeos, incluindo captura de vídeo, detecção e reconhecimento facial. Segundo "*Learning OpenCV: computer Vision with the OpenCV Library*"de Gary Bradski e Adrian Kaehler(BRADSKI; KAEHLER, 2008), o OpenCV é uma biblioteca de código aberto amplamente utilizada para aplicações de visão computacional e aprendizado de máquina. Com sua licença permissiva (Apache 2.0), é especialmente atrativa para o uso comercial, permitindo a modificação e distribuição de seu código. A biblioteca oferece uma ampla gama de funcionalidades, como detecção e reconhecimento facial, rastreamento de objetos, registro de imagens e até aplicações de realidade aumentada;

b) numpy: é uma biblioteca que tem como proposito a manipulação de arrays multidimensionais e funções matemáticas de alto desempenho. De acordo como site oficial a biblioteca "é o pacote fundamental para a computação científica em Python. É um Biblioteca Python que fornece um objeto de matriz multidimensional, vários objetos (como matrizes mascaradas e matrizes), e uma variedade de rotinas para operações rápidas em matrizes, incluindo matemática, lógica, manipulação de forma, classificação, seleção, E/O, transformadas discretas de Fourier, álgebra linear básica, operações estatísticas básicas, simulação aleatória e muito mais."(COMMUNITY, 2024);

c) os: está biblioteca traz a função de Navegação em diretórios e manipulação de arquivos no sistema operacional."Este módulo fornece uma maneira portátil de usar o sistema operacional dependente de funcionalidade."(FOUNDATION, 2024a);

d) scikit-learn: está biblioteca tem como função o aprendizado de máquina de código aberto para a linguagem de programação Python, entre outras vantagens citadas no site oficial (DEVELOPERS, 2024) como "Ferramentas simples e eficientes para análise de dados preditivos, acessível a todos, e reutilizável em vários contextos, construído em NumPy, SciPy, e matplotlib, licença de código aberto;

e) matplotlib: utilizada para criar gráficos e visualizar dados, incluindo a exibição de matrizes de confusão e outros tipos de gráficos para análise de desempenho. A biblioteca fornece uma interface flexível para personalizar gráficos e é amplamente utilizada para visualização em projetos de ciência de dados (TEAM., 2024);

f) datetime: usada para manipulação e formatação de datas e horários, o que é essencial para o registro e organização de resultados e experimentos. Esta biblioteca facilita a obtenção e a formatação de informações temporais em um formato compreensível (FOUNDATION., 2024);

g) seaborn: uma biblioteca baseada em Matplotlib que oferece uma interface de alto nível para criar gráficos estatísticos mais sofisticados. Ela é utilizada para melhorar a estética dos gráficos e facilitar a visualização de dados complexos, como a matriz de confusão, proporcionando uma interpretação mais clara dos resultados (WASKOM, 2024);

h) time: empregada para manipulação de tempo, incluindo a geração de timestamps e a medição de durações. É útil para registrar o tempo de execução dos processos e salvar informações temporais durante a execução de experimentos (FOUNDATION, 2024b).

3.3 Modelagem

O algoritmo desenvolvido visa o reconhecimento facial. Para isso, a capta de imagens será realizada por meio de uma câmera, que pode ser um dispositivo específico ou qualquer câmera disponível. O algoritmo solicita um identificador para cada pessoa que realiza a foto, que pode ser um número ou um nome. Após a identificação do rosto, a foto é salva em uma pasta correspondente ao identificador fornecido.

Além disso, um conjunto de dados será gerado a partir dessas imagens, e essas imagens passarão por um processo de identificação para determinar se a pessoa é um aluno ou um professor. O processo inclui a avaliação das métricas de validação, que serão registradas em um arquivo separado para análise futura.

3.4 Diagrama

O diagrama é uma ferramenta visual essencial para entender o funcionamento do código, especialmente no contexto de casos de uso. Ele facilita a compreensão das decisões que podem ser tomadas dentro do algoritmo, tornando o processo mais claro.

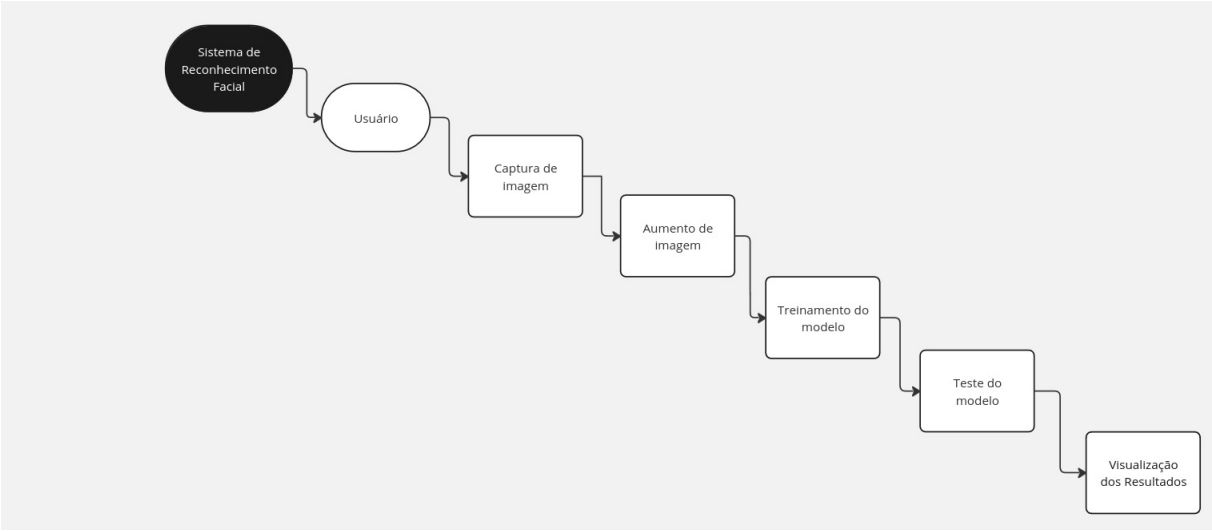
Para isso é necessário identificar os principais autores do sistema. No contexto deste trabalho, os autores são:

a) usuário: pessoa que fornece o identificador para captura de imagem;
b) sistema de detecção facial: o sistema que realiza a capta de imagens, treinamento do modelo e teste.

No estudo de caso em questão iremos trabalhar com o cenário da Figura 6 que ilustra o funcionamento do processo de reconhecimento facial.

A priori a Figura 6 ilustra o funcionamento do processo de reconhecimento facial. Inicialmente, é necessário obter as imagens dos usuários, que serão capturadas e adicionadas ao dataset. Com base nesse conjunto de imagens, o treinamento do modelo será realizado. Em seguida, o modelo será testado para avaliar seu desempenho e visualizar os resultados obtidos.

Figura 6 – Diagrama do estudo de caso.



Fonte: Elaborado pela autora (2024).

O presente trabalho é fortemente influenciado pela pesquisa realizada por Danilo Cardoso Beluco e Jorge Luiz Fortuna Filho em "Reconhecimento Facial Aplicado para Registro de Ponto"(BELUCO, a). Esta pesquisa oferece uma análise concisa do desempenho de três algoritmos de reconhecimento facial — Eigenface, Fisherface e LBPH — em um sistema específico, realizando uma comparação detalhada para identificar qual algoritmo se adapta melhor às variáveis presentes durante o processo. As metodologias e os resultados apresentados nesse estudo constituem uma base sólida para a implementação da proposta de "Uma proposta para a Avaliação de desempenho de algoritmos de reconhecimento facial"deste trabalho, ressaltando a relevância de utilizar algoritmos de reconhecimento facial que não requerem um processamento robusto para operar de forma eficaz.

4 RESULTADOS

Para analisar os resultados será feito um levantamento comparativo tendo como parâmetro três componentes principais tirados das métricas presentes nos códigos:

a) acurácia: mede a proporção de previsões corretas em relação ao total de previsões feitas. Representa a taxa de acertos do modelo no conjunto de dados;
b) recall: mede a capacidade do modelo de identificar corretamente as instâncias positivas (ou a classe de interesse), sendo calculado como a razão entre verdadeiros positivos e a soma de verdadeiros positivos e falsos negativos;
c) f1-score: uma média harmônica entre a precisão e o recall, que dá uma visão balanceada entre ambos. O F1-score é especialmente útil quando há um desbalanceamento entre as classes.

As métricas utilizadas serviram para avaliar o desempenho dos algoritmos de reconhecimento facial em termos de precisão na classificação. Os testes foram realizados com base em um dataset interno, composto por imagens de acadêmicos que autorizaram o uso de suas imagens para este estudo. O dataset totalizou 306 imagens, divididas entre conjuntos de treinamento e teste.

Os resultados obtidos estão apresentados nas tabelas a seguir. Cada tabela contém quatro colunas: a primeira coluna refere-se à pessoa e sua classificação, enquanto as segunda, terceira e quarta colunas correspondem às métricas de avaliação calculadas pelos algoritmos. Essas métricas incluem Acurácia, Recall e F1-score, empregadas para medir a eficácia de cada algoritmo na tarefa de reconhecimento facial.

Tabela 1 – Desempenho do Algoritmo Eigenface

Eigenface			
Pessoa	**Acurácia**	**Recall**	**F1-score**
01-Aluno	0.94	1.00	0.97
02-Aluno	0.93	1.00	0.96
03-Aluno	0.89	0.93	0.94
04-Professor	0.83	0.89	0.90
05-Aluno	0.93	1.00	0.96
06-Aluno	0.83	0.81	0.89
07-Aluno	0.94	0.97	0.97
08-Professor	0.84	0.88	0.91
09-Professor	0.95	1.00	0.97

Fonte: Elaborado pela autora (2024).

O algoritmo Eigenface apresentou desempenho razoável nas métricas de acurácia,

recall e F1-score. A acurácia variou entre 0.83 e 0.95, indicando uma sensibilidade maior às variações nas características faciais entre as pessoas. Apesar disso, tanto o recall quanto o F1-score mantiveram-se acima de 0.80, demonstrando um desempenho consistente, ainda que com algumas limitações na distinção de certas classes, especialmente no caso dos professores.

Tabela 2 – Desempenho do Algoritmo Fisherface

Fisherface			
Pessoa	**Acurácia**	**Recall**	**F1-score**
01-Aluno	0.95	1.00	0.97
02-Aluno	0.95	1.00	0.97
03-Aluno	0.95	1.00	0.97
04-Professor	0.95	1.00	0.97
05-Aluno	0.95	1.00	0.97
06-Aluno	0.95	1.00	0.97
07-Aluno	0.95	1.00	0.97
08-Professor	0.95	1.00	0.97
09-Professor	0.95	1.00	0.97

Fonte: Elaborado pela autora (2024).

O Fisherface, embora inicialmente pareça promissor devido à consistência dos resultados, revelou-se inadequado em comparação com os outros algoritmos. Todos os participantes apresentaram a mesma acurácia de 0.95 e F1-score de 0.97. Esse padrão uniforme sugere um possível sobreajuste (overfitting) do modelo aos dados de treinamento, o que indica que o Fisherface pode não estar capturando bem as variações específicas entre as diferentes pessoas.

Tabela 3 – Desempenho do Algoritmo LBPH

LBPH			
Pessoa	**Acurácia**	**Recall**	**F1-score**
01-Aluno	0.94	0.93	0.93
02-Aluno	0.96	0.97	0.98
03-Aluno	1.00	1.00	1.00
04-Professor	0.96	0.99	0.98
05-Aluno	0.99	1.00	0.99
06-Aluno	0.98	1.00	0.99
07-Aluno	0.98	1.00	0.99
08-Professor	0.96	0.97	0.98
09-Professor	0.99	1.00	0.99

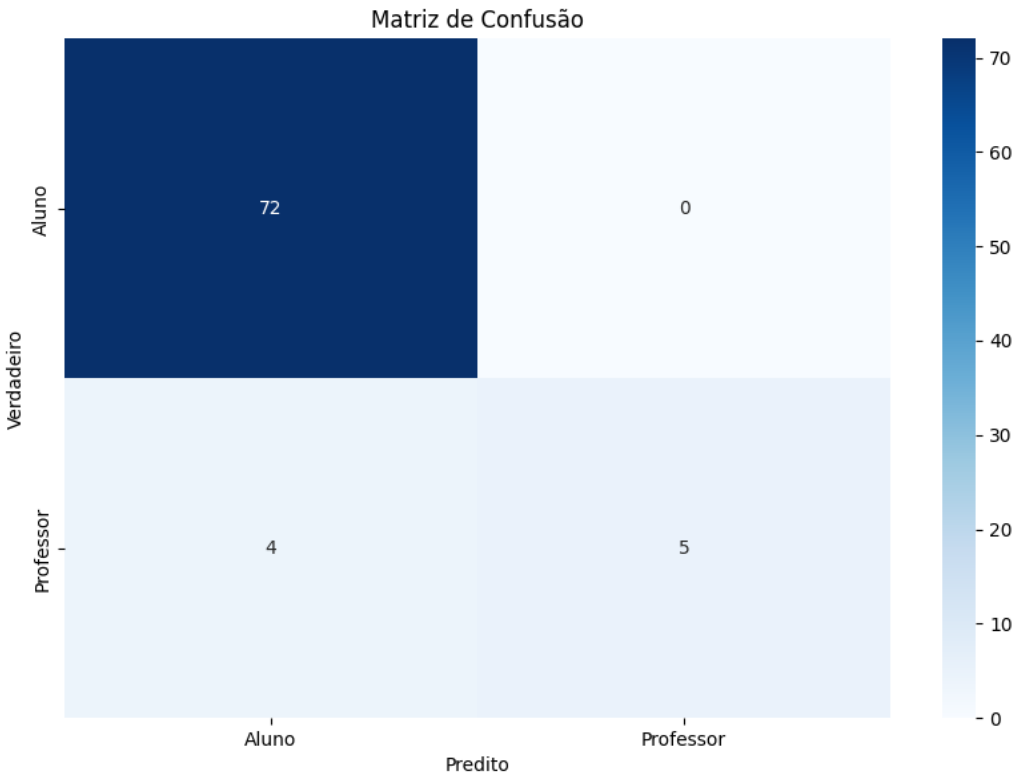
Fonte: Elaborado pela autora (2024).

Por outro lado, o LBPH destacou-se como o algoritmo mais eficaz, com acurácia acima de 0.90 para todas as classes. Os resultados de recall e F1-score acompanharam essa tendência, reforçando a superioridade do LBPH em termos de precisão e capacidade de gene-

ralização. Isso sugere que o LBPH é mais robusto em lidar com variações nas imagens, como iluminação e expressões faciais, tornando-o uma escolha mais adequada para o reconhecimento facial no contexto analisado. Com base nos logs dos 3 algoritmos se obteve um tempo médio entre 3 e 5 minutos de processamento.

A matriz de confusão é uma ferramenta eficaz para visualizar e interpretar os resultados de classificação. Ela permite analisar o desempenho de um modelo ao mostrar a relação entre as classes previstas e as classes reais. Neste contexto, iremos avaliar o desempenho dos três algoritmos de reconhecimento facial (Fisherface, Eigenface e LBPH) usando uma amostra que representa uma pessoa da classe professor. Ao aplicar os algoritmos, cada um tentará classificar essas amostras nas categorias corretas. A matriz de confusão nos ajudará a identificar os casos em que o modelo classificou corretamente as amostras e os casos em que cometeu erros, fornecendo uma visão clara da precisão e dos tipos de erros cometidos (falsos positivos e falsos negativos).

Figura 7 – Matriz de Confusão - pessoa 9 - classe – Professor - algoritmo Eigenface.

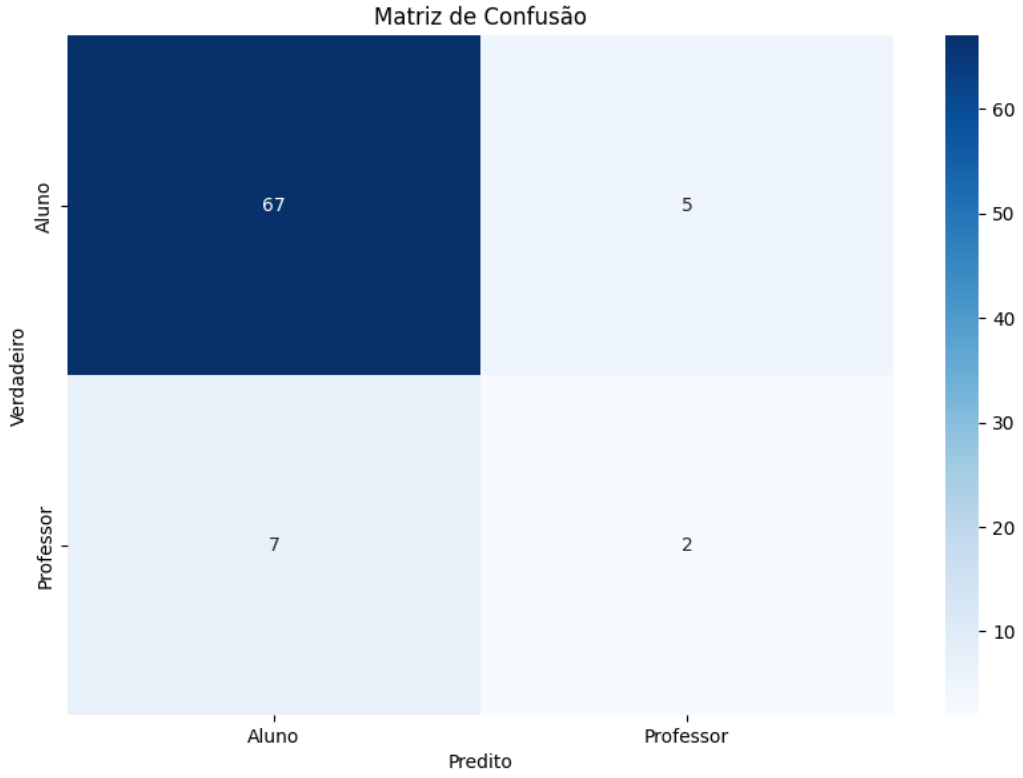


Fonte: Elaborado pela autora (2024).

A Figura 7 mostra a matriz de confusão referente à pessoa 9, utilizando o algoritmo

Eigenface, indica que o modelo classificou corretamente todas as 72 imagens da classe ’Aluno’, não havendo nenhum caso de alunos classificados incorretamente como ’Professor’. No entanto, para a classe ’Professor’, o modelo cometeu alguns erros: 4 imagens de professores foram erroneamente classificadas como alunos, enquanto apenas 5 imagens foram corretamente identificadas como pertencentes à classe ’Professor’.

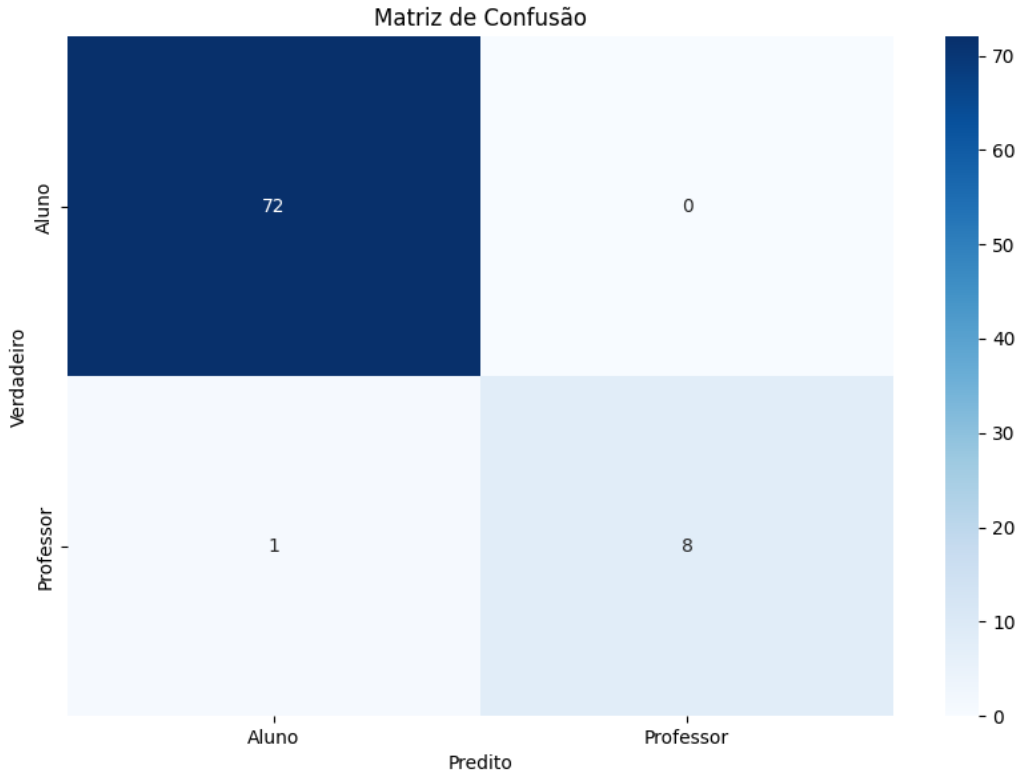
Figura 8 – Matriz de Confusão - pessoa 9 - classe – Professor - algoritmo Fisherface.



Fonte: Elaborado pela autora (2024).

A Figura 8 traz a matriz de confusão referente à pessoa 9, utilizando o algoritmo Fisherface, mostra que o modelo conseguiu classificar corretamente 67 imagens da classe ’Aluno’, mas cometeu 5 erros, identificando esses alunos, incorretamente como ’Professor’. Em relação à classe ’Professor’, o desempenho foi ainda menos satisfatório: 7 imagens de professores foram erroneamente classificadas como alunos, e apenas 2 imagens foram corretamente identificadas como ’Professor’. Esses resultados indicam que o algoritmo Fisherface teve maior dificuldade em distinguir professores de alunos, apresentando uma quantidade significativa de erros em ambas as classes, especialmente na identificação de professores.

Figura 9 – Matriz de Confusão - pessoa 9 - classe – Professor - algoritmo LBPH.



Fonte: Elaborado pela autora (2024).

Como mostrado na Figura 9 a matriz de confusão para a pessoa 9, utilizando o algoritmo LBPH, mostra que o modelo teve um ótimo desempenho na classificação da classe ’Aluno’, acertando todas as 72 imagens corretamente e não cometendo nenhum erro ao classificá-las como ’Professor’. Em relação à classe ’Professor’, houve apenas um erro, onde uma imagem de professor foi identificada como ’Aluno’. No entanto, o modelo conseguiu classificar corretamente 8 imagens de professores. Esses resultados indicam que o LBPH teve um desempenho superior em comparação aos outros algoritmos, mostrando uma capacidade elevada de distinção entre as duas classes, especialmente ao identificar alunos de forma precisa.

Com base nestes resultados, pode-se observar que o algoritmo LBPH se destacou em relação aos demais, classificando as pessoas de acordo com sua classificação real de maneira eficaz. A acurácia foi consistentemente alta em todos os resultados individuais, o que demonstra a robustez do LBPH em reconhecer e classificar corretamente as pessoas, mesmo com a presença de nove classes, onde apenas três são de professores.

O algoritmo Eigenface, embora tenha apresentado um desempenho inferior ao

LBPH, ainda demonstrou resultados relativamente bons. No entanto, observou-se uma queda no desempenho ao distinguir entre as classes de alunos e professores, como evidenciado pelos resultados para a Pessoa 04 e Pessoa 06 (professores).

Por outro lado, o algoritmo Fisherface apresentou um resultado consistente, porém com a mesma desempenho para todas as pessoas e classes. Esse comportamento indica que o modelo pode estar sobre ajustado aos dados de treinamento e não está generalizando bem para novos dados. Isso pode ser atribuído à quantidade limitada de dados disponíveis, que é relativamente pequena para um problema de reconhecimento facial. Além disso, a qualidade e a diversidade do dataset também podem ter influenciado esses resultados, sugerindo que uma maior variedade e quantidade de dados poderiam melhorar a generalização do modelo.

5 CONCLUSÃO

Este trabalho teve como principal objetivo o desenvolvimento de um sistema de reconhecimento facial utilizando as técnicas Eigenface, Fisherface e LBPH, com foco na segurança e precisão da identificação. A implementação e os testes realizados demonstraram que esse objetivo foi alcançado de maneira satisfatória, evidenciando a eficácia das técnicas aplicadas em diferentes cenários de uso.

Durante o desenvolvimento, foi possível realizar uma análise detalhada dos três algoritmos abordados. Ao longo da pesquisa, foram exploradas suas principais características, destacando suas vantagens e desvantagens, tanto em termos de desempenho quanto de eficiência. Essa análise teórica foi complementada pelos testes práticos, que revelaram variações no comportamento dos algoritmos em diferentes condições, como iluminação e ângulos de captura. O LBPH, por exemplo, se destacou em situações de baixa iluminação, enquanto o Eigenface apresentou melhor desempenho em termos de velocidade, sendo mais eficiente em ambientes com iluminação controlada.

Além disso, o sistema de reconhecimento facial foi desenvolvido com sucesso, integrando as três técnicas para permitir uma comparação consistente. A implementação mostrou-se robusta, permitindo a identificação precisa de indivíduos em diferentes cenários. As medidas de segurança adotadas durante a construção do sistema garantiram uma maior precisão, demonstrando a relevância das técnicas aplicadas.

Os testes realizados evidenciaram a eficácia do sistema em diferentes condições de uso, reforçando sua adaptabilidade. A qualidade do reconhecimento facial foi testada sob variações de iluminação e ângulo, e os resultados indicaram que, embora todos os algoritmos tivessem um desempenho aceitável, cada um se destacou em cenários específicos. Essas avaliações mostram que o sistema é confiável e tem potencial para ser utilizado em ambientes variados, desde que sejam feitas algumas adaptações conforme as necessidades.

Por fim, com base nos resultados obtidos, foram propostas algumas melhorias futuras para o sistema. A principal sugestão envolve o aprimoramento das técnicas em situações de alta variabilidade nas condições de luz e expressão facial. Adicionalmente, considera-se que o uso de algoritmos mais avançados, como aqueles baseados em aprendizado profundo, poderia trazer benefícios adicionais em termos de precisão e velocidade, especialmente em contextos mais desafiadores.

Em resumo, os objetivos propostos neste trabalho foram atingidos, e a pesquisa trouxe

contribuições relevantes tanto no desenvolvimento de um sistema eficaz de reconhecimento facial quanto na compreensão dos pontos fortes e limitações de cada algoritmo utilizado. A partir dos resultados obtidos, novas possibilidades de aperfeiçoamento foram identificadas, sugerindo caminhos promissores para pesquisas futuras e aprimoramentos técnicos.

REFERÊNCIAS

ANDERSON, R. **Security Engineering:** A Guide to Building Dependable Distributed Systems, 3rd Edition. [S.l.: s.n.], 2020. Disponivel em: https://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/1119642787. Acesso em: 14 mar. 2024.

BACKES, A.; MESQUITA, J. de. **Introdução á Visão Computacional Usando MATLAB**. [S.l.]: Alta Books, 2019. Disponivel em: https://books.google.com.br/books?id=m0YlDQAAQBAJ. Acesso em: 7 mar. 2024.

BACKES, J. J. d. M. S. J. A. R. **Introdução à Visão Computacional Usando MATLAB**. [S.l.: s.n.], 2016. Disponivel em: https://altabooks.com.br/wp-content/uploads/2021/07/Capitulo$_a mostra_I ntroducao_{av} isao_c omputacional_M ATLAB.pdf$. Acesso em: 22 ago. 2024.

BELUCO, J. L. F. F. D. C. **Reconhecimento facial aplicado a registro de ponto**. Disponivel em: https://repositorio.animaeducacao.com.br/items/77a858a8-6faf-4d78-8148-6e34e0008c21. Acesso em: 9 set. 2024.

BELUCO, J. L. F. F. D. C. **Reconhecimento facial aplicado para registro de ponto**. Disponivel em: https://repositorio.animaeducacao.com.br/items/77a858a8-6faf-4d78-8148-6e34e0008c21. Acesso em: 10 set. 2024.

BISHOP, C. M. **Pattern Recognition and Machine Learning**. [S.l.]: Springer, 2006. Disponivel em: https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf. Acesso em: 8 set. 2024.

BRADSKI, G.; KAEHLER, A. **Learning OpenCV:** Computer Vision with the OpenCV Library. [S.l.]: O'Reilly Media, Inc., 2008. Disponivel em: https://books.google.com.br/books?id=seAgiOfu2EIC. Acesso em: 20 ago. 2022.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. 2018. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponivel em: https://www.planalto.gov.br/ccivil$_0 3/_{ato} 2015-2018/2018/lei/l 13709.htm$. Acesso em: 9 ago. 2024.

COMMUNITY, T. N. **NumPy Documentation**. 2024. Disponivel em: https://numpy.org/doc/stable/. Acesso em: 2 set. 2023.

DEVELOPERS, S. learn. **Scikit-learn: Machine Learning in Python**. 2024. Disponivel em: https://scikit-learn.org/stable/index.html. Acesso em: 2 set. 2023.

ESCOVEDO, T.; KOSHIYAMA, A. **Introdução a Data Science:** Algoritmos de Machine Learning em todos de análise. [S.l.]: Casa do Código, 2020. Disponivel em: https://books.google.com.br/books?id=cL7TDwAAQBAJ. Acesso em: 7 mar. 2024.

FERNANDES JESSICA MARTINS, R. V. G. **Técnicas de Reconhecimento Facial Através da Inteligência Artificial**. Disponivel em: https://congresso.fatecmococa.edu.br/index.php/congresso/article/download/454/163/937. Acesso em: 10 set. 2024.

FOUNDATION., P. S. **Datetime — Basic date and time types**. 2024. Disponivel em: https://docs.python.org/3/library/os.htmlhttps://docs.python.org/3/library/os.html. Acesso em: 7 set. 2024.

FOUNDATION, P. S. **Python 3: os — Miscellaneous operating system interfaces**. 2024. Dispinivel em: https://docs.python.org/3/library/os.html. Acesso em: 7 set. 2024.

FOUNDATION, P. S. **Time - Python 3 documentation**. 2024. Disponivel em: https://docs.python.org/3/library/os.htmlhttps://docs.python.org/3/library/os.html. Acesso em: 7 set. 2024.

GRECO, K. J. D. **Facial Recognition Technology:** Ensuring Transparency in Government Use. Disponivel em: https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use. Acesso em: 8 ago. 2024.

GUEDES, M. **Pilares da Segurança da Informação**. Disponivel em: https://www.treinaweb.com.br/blog/pilares-da-seguranca-da-informacao. Acesso em: 8 mar. 2024.

HASTIE, T.; TIBSHIRANI, R.; FRIEDMAN, J. **The Elements of Statistical Learning:** Data Mining, Inference, and Prediction. [S.l.]: Springer Science & Business Media, 2009. Disponivel em: https://www.sas.upenn.edu/ fdiebold/NoHesitations/BookAdvanced.pdf. Acesso em: 20 ago. 2022.

LOPES, F.; FILHO, C. B. **Segmentação e Detecção de Faces em Imagens Coloridas com Informações de Cor e Movimento**. 2005. Acesso em: 1 set. 2023.

MAGALDI, R. **O que é o Teste de Turing?** 2019. Disponível em: https://encurtador.com.br/811DY. Acesso em: 15 ago. 2024.

MURPHY, K. P. **Machine Learning:** A Probabilistic Perspective. [S.l.]: MIT Press, 2012. Disponivel em: https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf. Acesso em: 10 set. 2024.

NUNES, L. F. d. M. **Reconhecimento facial biométrico em nuvens de pontos tridimensionais**. Disponivel em: http://repositorio.unb.br/handle/10482/39185. Acesso em: 10 set. 2024.

RICH, K. K. E. **Inteligencia artificial**. [S.l.: s.n.], 1993. Note = Disponivel em: https://books.google.com.br/books?id=yunOPQAACAAJ. Acesso em: 20 abr. 2024.

SILVA, A.; CINTRA, M. **Reconhecimento de padrões faciais:** Um estudo. Disponivel em: https://api.semanticscholar.org/CorpusID:7022786. Acesso em: 7 abr. 2022.

SILVA, H. C. C. B. T. P. T. **SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO** Gestão Estratégica da Segurança Empresarial. [S.l.: s.n.]. Disponivel em: https://docente.ifrn.edu.br/rodrigotertulino/livros/sistema-de-seguranca-da-informacao. Acesso em: 22 ago. 2024.

SINGER, P. W.; FRIEDMAN, A. **Cybersecurity and Cyberwar:** What Everyone Needs to Know**, year=2014**. New York: Oxford University Press. Disponivel em: https://www.amazon.com.br/Cybersecurity-Cyberwar-Everyone-Needs-English-ebook/dp/B00GJG6ZB2. Acesso em: 15 mar. 2024.

SZELISKI, R. **Computer Vision: Algorithms and Applications**. [S.l.]: Springer Science & Business Media, 2010. Disponivel em: https://encurtador.com.br/Rw5Az. Acesso em: 22 ago. 2024.

TEAM., M. development. **Using Matplotlib**. 2024. Disponivel em: https://scikit-learn.org/stable/index.html. Acesso em: 7 set. 2024.

WASKOM, M. L. **Seaborn:** Statistical data visualization. 2024. Disponivel em: https://seaborn.pydata.org/. Acesso em: 7 set. 2024.

YANG, M. H.; KRIEGMAN, D. J.; AHUJA, N. **Detectando Rostos em Imagens:** Uma Revisão. Disponivel em: https://ieeexplore.ieee.org/abstract/document/982883. Acesso em: 1 set. 2024.

ZHOU, Z. hua. **"Machine learning"**. [S.l.: s.n.]. Disponivel em: https://www.amazon.com.br/Machine-Learning-English-Zhi-Hua-Zhou-ebook/dp/B09D92YBFG. Acesso em: 23 ago. 2024.

APÊNDICE A – TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Termo de autorização de uso de imagem submetido ao *imagem submetido ao projeto acadêmico "Proposta de controle de acesso em um ambiente acadêmico: uma contribuição do uso do aprendizado de máquina no reconhecimento facial"para fins de coleta e análise de dados, conforme detalhado no Apêndice A desta documentação.*

UNIVERSIDADE FEDERAL DO CEARÁ

UNIVERSIDADE FEDERAL DE CEARÁ

TERMO DE AUTORIZAÇÃO DE IMAGEM

Eu,_____, nacionalidade _____, estado civil _____, portador da Cédula de identidade RG nº._____, inscrito no CPF/MF sob nº _____, residente à Av./Rua _____, nº. _____, município de _____/Itapajé-CE. AUTORIZO o uso de minha imagem em todo e qualquer material, incluindo imagens de vídeo, fotografias e documentos, para ser utilizada no Trabalho de Pesquisa intitulado "Controle de Acesso Físico com o Uso de Reconhecimento Facial".

A presente autorização é concedida de forma gratuita e abrange o uso da minha imagem em todo o território nacional, conforme descrito abaixo:

Finalidade do Uso:

- A imagem será usada para fins educacionais;
- Com o intuito de se fazer uma pesquisa para aumentar a segurança do acesso físico.

Fica ainda **autorizada**, de livre e espontânea vontade, para os mesmos fins, a cessão de direitos da veiculação das imagens, não recebendo para tanto qualquer tipo de remuneração.

Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

_____, dia _____ de _____ de _____.

_____

(Assinatura)

Nome:
Telefone p/ contato: