# Desenvolvimento de um Dispositivo para Segurança Biométrica Facial Usando Câmera NoIR

Tassany Onofre de Oliveira

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2024

Tassany Onofre de Oliveira

# Desenvolvimento de um Dispositivo para Segurança Biométrica Facial Usando Câmera NoIR

Monografia apresentada ao curso Engenharia de computação
do Centro de Informática, da Universidade Federal da Paraíba,
como requisito para a obtenção do grau de Bacharel em engenharia de computação

Orientador: Alisson Vasconcelos De Brito

Outubro de 2024

**Catalogação na publicação**
**Seção de Catalogação e Classificação**

O48d Oliveira, Tassany Onofre de.
Desenvolvimento de um dispositivo para segurança biométrica facial usando câmera NoIR / Tassany Onofre de Oliveira. - João Pessoa, 2024.
39 f. : il.

Orientação: Alisson Vasconcelos de Brito.
Coorientação: Leonardo Vidal Batista.
TCC (Graduação) - UFPB/CI.

1. Segurança biométrica. 2. Antispoofing. 3. NDVI. 4. Sistema embarcado. I. Brito, Alisson Vasconcelos de. II. Batista, Leonardo Vidal. III. Título.

UFPB/CI CDU 004.056:621.397

Elaborado por Michelle de Kássia Fonseca Barbosa - CRB-738

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

Trabalho de Conclusão de Curso de Engenharia de computaçãointitulado ***Desenvolvimento de um Dispositivo para Segurança Biométrica Facial Usando Câmera NoIR*** de autoria de Tassany Onofre de Oliveira, aprovada pela banca examinadora constituída pelos seguintes professores:

---

Prof. Dr. Leonardo Vidal Batista
Universidade Federal da Paraíba

---

Prof. Dr. Ewerton Monteiro salvador
Universidade Federal da Paraíba

---

Prof. Dr. Alisson Vasconcelos De Brito
Universidade Federal da Paraíba

---

Coordenador(a) do Departamento Departamento de Sistemas de Computação
Josilene Aires Moreira
CI/UFPB

João Pessoa, 3 de outubro de 2024

Centro de Informática, Universidade Federal da Paraíba
Rua dos Escoteiros, Mangabeira VII, João Pessoa, Paraíba, Brasil CEP: 58058-600
Fone: +55 (83) 3216 7093 / Fax: +55 (83) 3216 7117

*“Quarenta e dois” - Douglas Adams*

# DEDICATÓRIA

Dedico este trabalho à minha família e ao meu esposo, que estiveram ao meu lado em cada momento desta jornada.

# AGRADECIMENTOS

Agradeço profundamente aos meus professores, Alisson e Leonardo, por suas valiosas orientações, paciência e dedicação ao longo do desenvolvimento deste trabalho. Suas experiências e conselhos foram essenciais para a realização deste projeto e contribuíram significativamente para o meu crescimento acadêmico e pessoal.

Aos meus amigos de curso, que compartilharam comigo os momentos de dificuldade e celebração, tornando essa jornada mais leve e divertida. A amizade e o apoio de vocês foram fundamentais para que eu pudesse chegar até aqui.

Ao setor de Pesquisa de Hardware da Vsoft, que me proporcionou a oportunidade de me sentir como uma verdadeira engenheira de computação, permitindo-me aplicar o conhecimento adquirido e desenvolver habilidades essenciais para a minha carreira.

Por fim, expresso minha sincera gratidão a todos que, de alguma forma, direta ou indiretamente, contribuíram para a concretização deste trabalho. A cada um de vocês, o meu mais profundo agradecimento.

# RESUMO

Este trabalho teve como objetivo desenvolver um dispositivo de detecção anti-spoofing para segurança biométrica, utilizando a câmera NoIR para Raspberry Pi. A crescente necessidade de aprimorar a segurança em sistemas de reconhecimento facial, especialmente contra tentativas de falsificação usando fotos e vídeos, motivou a realização deste estudo. A solução proposta combina técnicas de visão computacional, como o cálculo do Índice de Vegetação por Diferença Normalizada (NDVI), adaptado para distinguir rostos reais de falsificações. A metodologia incluiu a criação de um dataset com imagens reais e falsificadas, e o desenvolvimento de algoritmos para análise dessas imagens. Os resultados mostraram que o sistema foi eficaz em identificar rostos reais e detectar tentativas de falsificação, validando a abordagem empregada e sugerindo seu potencial para aplicações práticas.

**Palavras-chave:** Segurança biométrica, antispoofing, detecção facial, NDVI, sistema embarcado.

# ABSTRACT

This work aimed to develop an anti-spoofing detection device for biometric security, using the NoIR camera for Raspberry Pi. The increasing need to enhance security in facial recognition systems, especially against spoofing attempts using photos and videos, motivated this study. The proposed solution combines computer vision techniques, such as the calculation of the Normalized Difference Vegetation Index (NDVI), adapted to distinguish real faces from forgeries. The methodology included the creation of a dataset with real and fake images and the development of algorithms for analyzing these images. The results showed that the system was effective in identifying real faces and detecting spoofing attempts, validating the approach employed and suggesting its potential for practical applications.



**Key-words:** Biometric security, antispoofing, facial detection, NDVI, embedded system.

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS

NDVI – Normalized Difference Vegetation Index

IR – Infrared

NoIR – No Infrared

NIR – Near infrared

RGB – Red Green Blue

## Sumário

# 1 INTRODUÇÃO

A biometria é um campo multidisciplinar dedicado à medição e mapeamento de características biológicas específicas, como impressões digitais, rosto e a palma da mão, para uso como um código individualizado de reconhecimento [15].

Com o desenvolvimento de tecnologias como computadores e a internet, surgiram novas preocupações relacionadas à segurança, especialmente no que diz respeito ao controle de acesso digital. O avanço nas áreas de eletrônica e ciência da computação proporcionou o acesso a dispositivos tecnológicos de ponta a preços mais acessíveis, ampliando o alcance das soluções biométricas para uma parcela significativa da população mundial.

A patir disso, sistemas biométricos poderam ser amplamente implementados em diversas aplicações práticas, como pagamentos online, segurança no e-commerce, autenticação baseada em smartphones, controle de acesso seguro, passaportes biométricos e verificações de fronteira. Dentre as diversas tecnologias biométricas, o reconhecimento facial destaca-se por suas inúmeras vantagens. Os rostos são altamente distintivos entre os indivíduos, permitindo que o reconhecimento facial seja implementado mesmo em cenários de aquisição não intrusivos ou a distância [1].

## 1.1 Definição do Problema

Com o advento da internet e das redes sociais, onde cada vez mais pessoas compartilham fotos ou vídeos de seus rostos, esses documentos podem ser usados por impostores para tentar enganar os sistemas de autenticação facial, com o propósito de personificação [16]. Esses ataques também são chamados de ataques de personificação (spoofing). Os atacantes capturam uma fotografia do usuário legítimo, seja de uma fonte publicamente disponível ou uma imagem tirada de forma oculta, e então a apresentam estrategicamente às câmeras do sistema biométrico durante o processo de autenticação. O objetivo é replicar os sinais visuais de uma interação genuína, enganando o sistema para conceder acesso ou autenticação.

## 1.2 Objetivo geral

O objetivo deste projeto é propor uma solução de hardware simples para implementar a proteção contra falsificação (anti-spoofing) na autenticação biométrica facial. A proposta utiliza módulos de câmera RGB sem filtro IR e um filtro fotográfico, visando melhorar a segurança e a confiabilidade dos sistemas de reconhecimento facial. A abordagem busca alcançar esses objetivos sem a necessidade de grandes processamentos e elevados custos materiais.

## 1.3 Objetivos específicos

O objetivo específico do projeto é aplicar algoritmos de visão computacional que possam distinguir de forma eficaz entre imagens reais de uma pessoa, fotos impressas e fotos exibidas em uma tela. Estes algoritmos devem ser capazes de identificar características únicas e sinais visuais que diferenciam um rosto verdadeiro de uma tentativa de falsificação, garantindo resultados precisos e confiáveis na autenticação biométrica facial.

## 1.4 Estrutura da monografia

O trabalho está organizado da seguinte forma: Capítulo 2 aborda toda a fundamentação teórica acerca dos conceitos e tecnologias inclusas no trabalho. No Capítulo 3 é apresentado o protótipo do sistema proposto. No Capítulo 4 são apresentados os resultados obtidos. No Capítulo 5 é feito o encerramento do trabalho assim como são apresentadas as perspectivas para futuras melhorias.

# 2 CONCEITOS GERAIS E REVISÃO DA LITERATURA

Nesta seção são apresentados os principais conceitos teóricos que foram utilizados para o desenvolvimento do trabalho. Inicialmente, é explicado o que se trata *Face Spoofing*, Ataques de apresentação Facial e seus diferentes tipos. Em seguida, são analisados os conceitos de câmeras *no-IR* e o algoritmo de *Normalized Difference Vegetation Index* (NDVI). Por fim, é explicada a utilização do hardware.

## 2.1 Ataque de falsificação biométrica

Um ataque falsificação facial é um ato enganoso onde uma pessoa ou programa finge ser outra pessoa falsificando dados para obter uma vantagem ilegítima. É comumente usado em cibersegurança para enganar indivíduos ou sistemas, fazendo-os acreditar que o atacante é uma fonte confiável.

Segundo [1], os ataques mais comuns são geralmente categorizados como Ataques de Imitação (Impersonation) e Ataques de Ofuscação (Obfuscation). Os Ataques de Imitação envolvem o uso de meios para ser reconhecido como outra pessoa, copiando atributos faciais de um usuário genuíno em suportes como fotos, telas eletrônicas e máscaras digitais. Já os Ataques de Ofuscação têm como objetivo esconder ou remover a identidade do atacante usando diversos métodos, como óculos, maquiagem, perucas e disfarces faciais.

Com base nas propriedades geométricas, os ataques podem ser classificados em Ataques 2D e Ataques 3D. Ataques 2D são realizados utilizando atributos faciais apresentados por meio de fotos ou vídeos ao sensor. Variantes comuns de ataques 2D incluem fotos impressas (planas ou enroladas), fotos com recortes nos olhos ou boca, e reprodução digital de vídeos. Em contraste, Ataques 3D empregam máscaras faciais tridimensionais para comprometer os sistemas de reconhecimento facial. Comparados aos ataques 2D tradicionais, as máscaras 3D oferecem maior realismo em termos de cor, textura e estrutura geométrica. As máscaras 3D podem ser confeccionadas com materiais rígidos, como papel, resina, gesso ou plástico, e com materiais flexíveis, como silicone ou látex.

Considerando a cobertura da região facial, os ataques de falsificação podem ser classificados em Ataques Totais e Ataques Parciais. Os Ataques Totais envolvem a cobertura completa da face, utilizando métodos como fotografias impressas, reproduções de vídeo e máscaras 3D. Enquanto que os Ataque Parciais envolvem a cobertura de apenas partes específicas da face, empregando técnicas como fotografias impressas com recortes, óculos que alteram a aparência dos olhos, e tatuagens parciais na região das bochechas.

A Figura 1 mostra exemplos de Ataques de Falsificação facial dos diferentes tipos já citados.

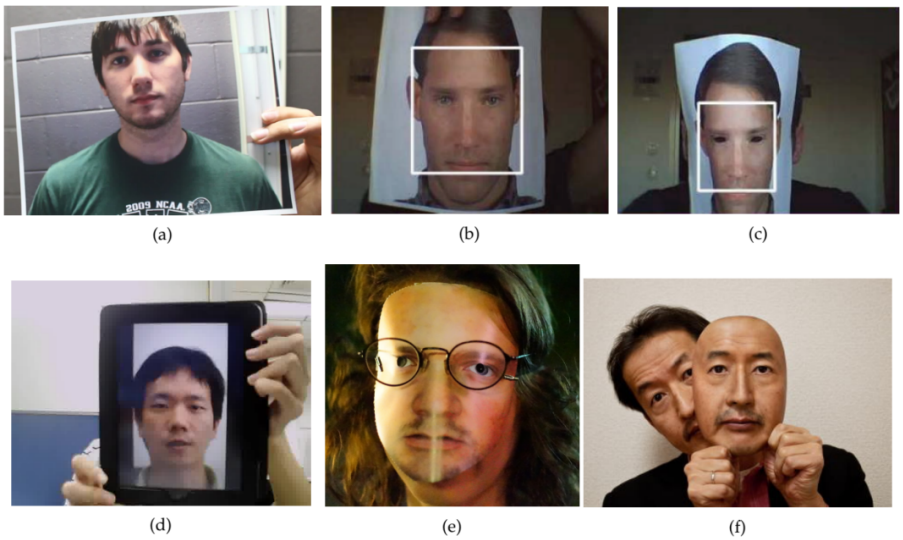


**Figura 1: Diferentes tentativas de falsificação [1]**

**(a) Ataque com foto impressa [11]; (b) Exemplo de ataque com foto distorcida [12]; (c) Exemplo de ataque com foto recortada [12]; (d) Ataque de replay de vídeo [13]; (e) Máscara feita de papel [14]; (f) Ataque com máscara 3D de alta qualidade [11]**

## 2.2 Soluções de detecção de falsificação biométrica

Até o presente momento, ainda não existe um método para detectar falsificações biométrica acordado para que consiga lidar com todos os tipos de ataque [1], conforme já foi discutido na seção anterior. De modo geral, as soluções de detecção de falsificação podem ser classificadas em duas grandes categorias: métodos baseados em hardware/sensores específicos para cada tipo de ataque e abordagens que utilizam dispositivos genéricos de consumidor, como câmeras de smartphones.

Os métodos que utilizam hardware específico costumam ser mais precisos e confiáveis, pois são desenvolvidos para detectar tipos específicos de ataques com base nas características físicas e comportamentais do objeto ou indivíduo autenticado. Esses métodos podem contar com sensores 3D de luz estruturada (structured-light 3D), sensores de Tempo de Voo (ToF), sensores de infravermelho próximo (NIR), sensores térmicos, entre outros. Cada tipo de sensor oferece vantagens distintas na detecção de falsificações.

Por exemplo, sensores 3D têm a capacidade de discriminar entre rostos tridimensionais e ataques com superfícies planas bidimensionais (como fotos ou vídeos), detectando mapas de profundidade que revelam a estrutura real do rosto [6]. Sensores de infravermelho próximo (NIR), por sua vez, são eficazes na detecção de ataques com faces em reproduções de vídeo ou fotos, pois conseguem identificar a diferença na reflexão de luz infravermelha entre superfícies vivas e inanimadas [7] [8]. Sensores térmicos também são amplamente utilizados, pois podem detectar a distribuição de temperatura característica

de rostos vivos, diferindo-a de objetos que não emitem calor ou que possuem padrões de calor uniformes [9].

Embora os métodos baseados em hardware específico tendam a ser mais precisos, eles ainda não são amplamente disponíveis para o público em geral devido ao alto custo e à complexidade dos dispositivos necessários. Além disso, esses sensores raramente estão embutidos em dispositivos genéricos de consumidor, com exceção de alguns aparelhos mais caros. Por esse motivo, essas soluções são frequentemente limitadas a cenários aplicativos específicos, como controle de acesso físico em locais altamente protegidos, pois oferecem maior precisão e segurança em cenários críticos.

## 2.3 Espectro de Refletância da Pele Humana

O espectro visível da luz é a faixa de radiação eletromagnética que pode ser percebida pelo olho humano. Ele abrange comprimentos de onda aproximadamente entre 380 nanômetros (nm) e 750 nanômetros (nm), que pode ser observado na Figura 2. Dentro dessa faixa, diferentes comprimentos de onda correspondem a diferentes cores, variando do violeta, passando pelo azul, verde, amarelo e laranja, até o vermelho.

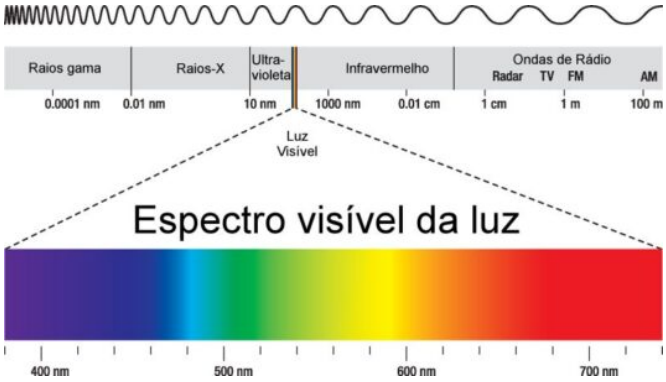


**Figura 2: Espectro de cores [10]**

A cor de um objeto é determinada pela interação da luz com o material do objeto e pela forma como essa luz é percebida pelos olhos humanos. Esse fenômeno pode ser explicado pela absorção, reflexão e transmissão da luz. Quando a luz atinge um objeto, parte dessa luz é absorvida pelas moléculas do material, enquanto a luz que não é absorvida é refletida. Além disso, alguns materiais permitem que a luz passe através deles, um processo conhecido como transmissão.

No caso da pele humana, a interação da luz com a melanina, hemoglobina e outras substâncias presentes na pele determina a sua cor aparente. A Figura 3, criada a partir do estudo do artigo [3], mostra a taxa de refletância da pele humana de acordo com o comprimento de onda. A pele tem uma menor refletância em comprimentos de onda mais curtos (cerca de 350 nm) do que em comprimentos de onda mais longos (cerca de 1050

nm). Em particular, a pele possui uma propriedade única de absorver luz ao redor de um comprimento de onda de 970 nm na região do infravermelho próximo (NIR), que se localiza entre 750nm e 2500nm.

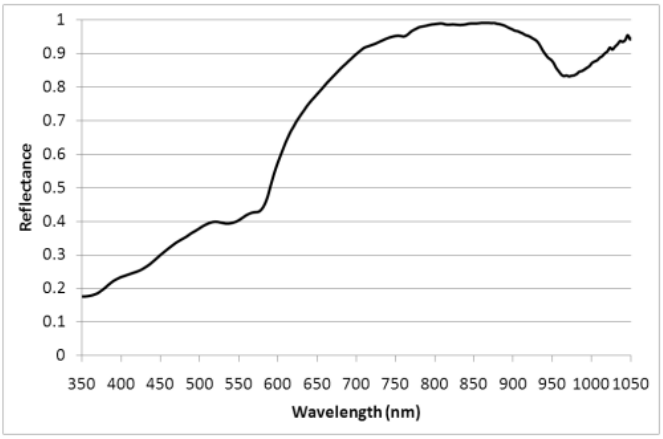


**Figura 3: Espectros de refletância da pele humana [3]**

Adicionalmente, a Figura 4, também produzida no estudo de [3], compara as curvas de refletância da pele humana com outros materiais como asfalto, vegetação e pinturas de rodovias. Esse estudo demonstrou que o padrão de refletância da pele no espectro infravermelho é distinto o suficiente para ser utilizado como critério de diferenciação em sistemas de segurança biométrica, confirmando a viabilidade do uso de infravermelho para distinguir a pele humana de outros materiais.

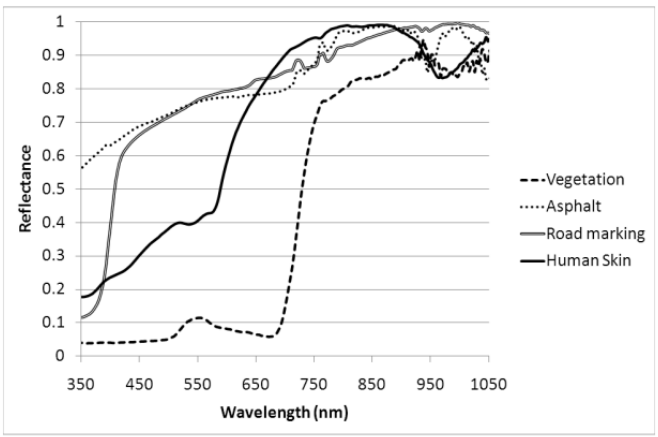


**Figura 4: Espectros de refletância de várias substâncias [3]**

## 2.4 Tecnologia infravermelho

O filtro ótico IR-CUT, também conhecido como hot mirror, é projetado para refletir ou bloquear comprimentos de onda no infravermelho médio, permitindo a passagem

apenas da luz visível. Este filtro é amplamente utilizado em câmeras coloridas e dispositivos de vídeo para evitar que a radiação infravermelha atinja o sensor de imagem. O objetivo é capturar imagens que se aproximem ao máximo daquelas percebidas pelo olho humano [2]. A Figura 5 mostra o diagrama de uma câmera comum sem modificações em sua estrutura.

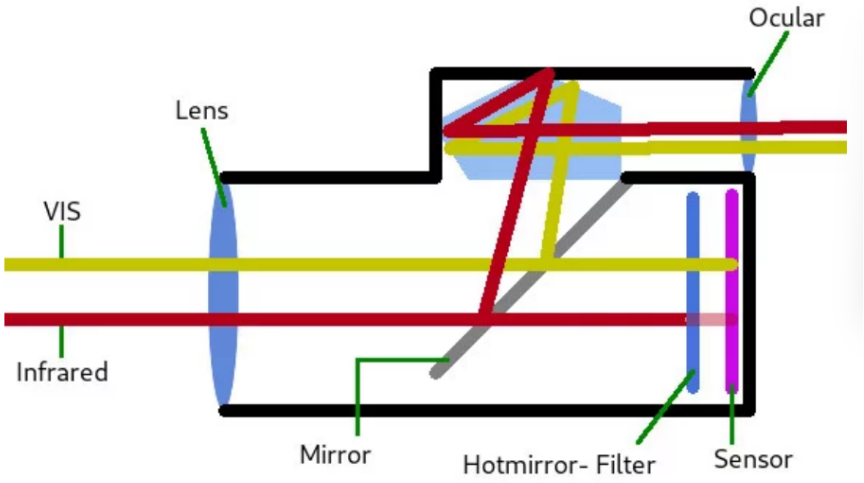


**Figura 5: Diagrama de uma câmera comum.**

Nas câmeras de infravermelho Figura 6, ocorre o oposto: o filtro utilizado bloqueia todas as frequências de luz visível e permite que apenas a frequência infravermelha chegue ao sensor. Estas câmeras não são ideais para capturar imagens com alto nível de detalhe, pois os detalhes podem irradiar a mesma quantidade de infravermelho que seu entorno, tornando-se invisíveis ao sensor e dificultando a distinção da imagem.

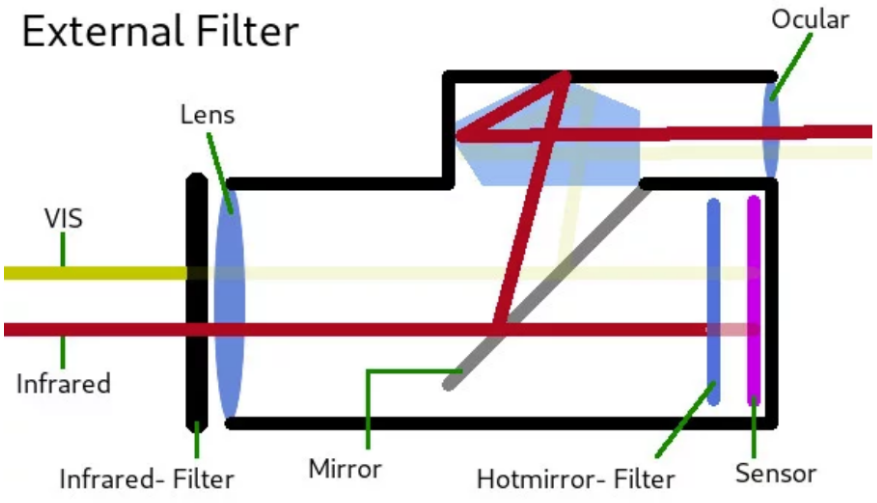


**Figura 6: Diagrama de uma câmera de infravermelho.**

As câmeras NoIR combinam as características das câmeras convencionais e infra-

vermelhas, removendo o filtro infravermelho de uma câmera comum RGB, é permitindo a captura tanto de luz visível quanto de infravermelho em uma única imagem. No entanto, essa abordagem apresenta um desafio: a saída é uma imagem em cores RGB, onde o sinal de infravermelho é capturado nos outros canais de cor.

Para utilizar este tipo de câmera em aplicações biométricas, é necessário adicionar um filtro, como na Figura 7 que remove os canais vermelho e verde, deixando passar apenas a luz azul e o infravermelho. Como essas duas frequências são muito distintas, não haverá interferência entre elas, permitindo uma captura precisa das características desejadas da face.

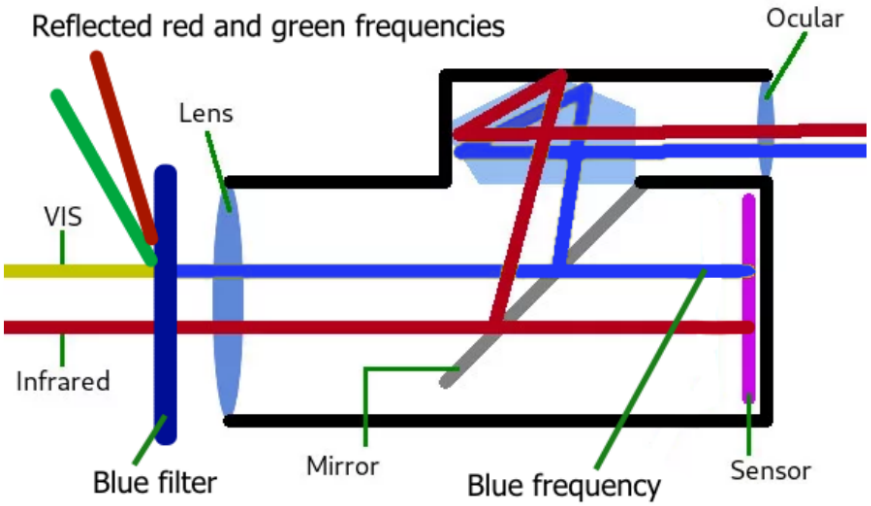


**Figura 7: Diagrama de uma câmera no-ir.**

# 3 METODOLOGIA

Este capítulo descreve o desenvolvimento e a construção do protótipo, detalhando tanto os aspectos de hardware quanto de software, além de apresentar o processo de implementação. O fluxo de funcionamento do sistema de identificação de falsificação é ilustrado na Figura 8, que mostra as etapas envolvidas desde a inicialização do dispositivo até a detecção final.

O funcionamento inicia-se com a ativação do dispositivo, que, em seguida, executa o algoritmo de detecção facial. Caso nenhuma face seja detectada, o processo continua em loop até que uma face seja identificada. Quando uma face é capturada, a imagem segue para o algoritmo de detecção de pele humana, cuja função é analisar a refletância da pele e determinar se a imagem representa uma pessoa real ou uma tentativa de falsificação. A decisão final, baseada nessa análise, classifica a imagem como verdadeira ou falsa.

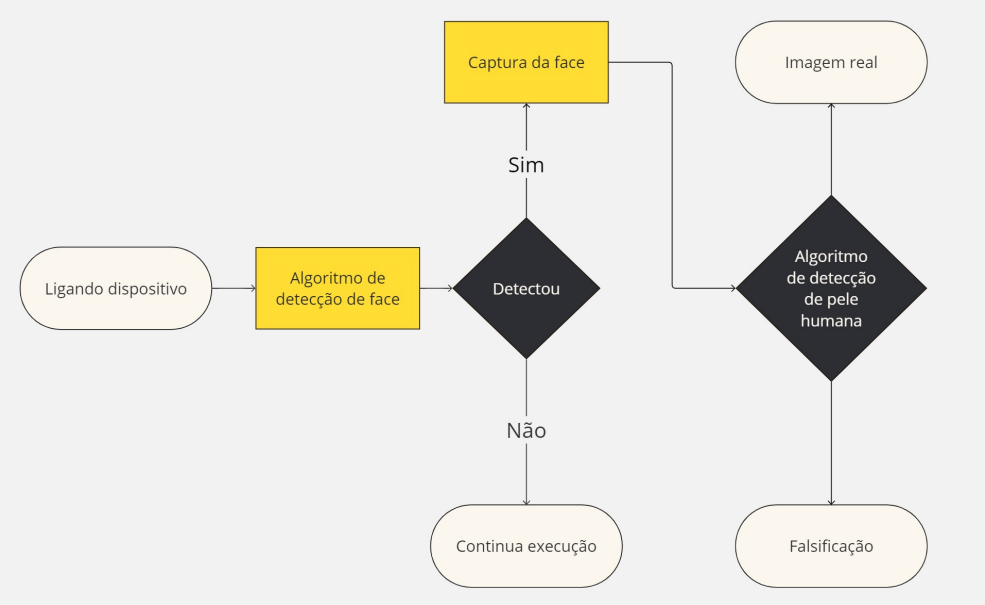


**Figura 8: Diagrama de fluxo do dispositivo**

## 3.1 Hardware utilizado

### 3.1.1 Raspberry Pi 3 B+

Foi utilizado o modelo Raspberry Pi 3 B+, mostrado na Figura 9 como responsável por interligar os dispositivos e execução dos algoritmos. O Raspberry Pi 3 B+ é um microcomputador de baixo custo e alto desempenho, amplamente utilizado em projetos de Internet das Coisas (IoT) e computação embarcada.

O Raspberry Pi 3 B+ possui um processador Broadcom BCM2837B0, Cortex-A53 (ARMv8) de 64 bits e 1.4 GHz, memória RAM de 1 GB LPDDR2 SDRAM, e

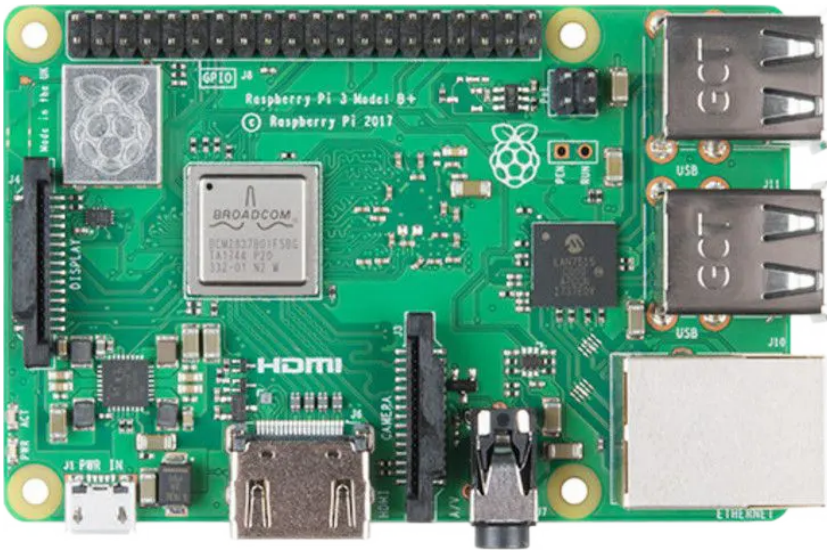


**Figura 9: Raspberry pi 3 modelo B+.**

conectividade abrangente, incluindo Ethernet Gigabit (via USB 2.0), Wi-Fi 802.11ac de banda dupla e Bluetooth 4.2. Além disso, conta com quatro portas USB 2.0, uma porta HDMI, uma porta de saída de áudio e vídeo composto, e um conector de câmera CSI, que permite a integração direta de módulos de câmera, como o módulo de câmera NoIR (sem filtro IR) [18].

A escolha do Raspberry Pi 3 B+ justifica-se pela sua versatilidade, facilidade de uso, e extensa documentação disponível, o que facilita a implementação e testes do sistema proposto. O ambiente de desenvolvimento foi configurado com o sistema operacional Raspbian, uma distribuição baseada em Debian otimizada para o hardware do Raspberry Pi.

### 3.1.2 Câmera NoIR para Raspberry Pi

Neste trabalho, será utilizada a Câmera NoIR, Figura 10, para Raspberry Pi como parte essencial para a captura das imagens para a criação do dataset de testes.

A Câmera NoIR é um módulo de câmera para Raspberry Pi que não possui filtro de infravermelho (IR), permitindo a captura de imagens tanto no espectro visível quanto no espectro infravermelho. A ausência do filtro IR é particularmente útil para a detecção de vivacidade, uma vez que permite diferenciar características de superfícies vivas, como a pele humana, de superfícies artificiais.

Além disso, o módulo possui um sensor de imagem OV5647 com uma resolução de 5 megapixels, suportando resoluções de até 2592 $\times$ 1944 pixels. Ela é capaz de capturar vídeo em 1080p a 30 quadros por segundo (fps), 720p a 60 fps e 640x480 a 60/90 fps. A câmera utiliza uma lente fixa com uma distância focal de aproximadamente 3,6 mm e

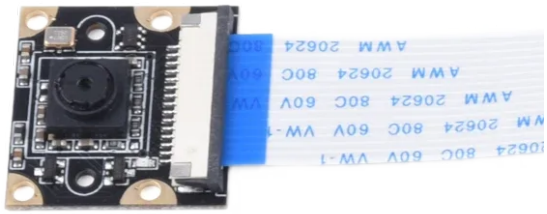

**Figura 10: Câmera NoIR para Raspberry Pi.**

possui um ângulo de visão de cerca de 54 graus na horizontal e 41 graus na vertical [17].

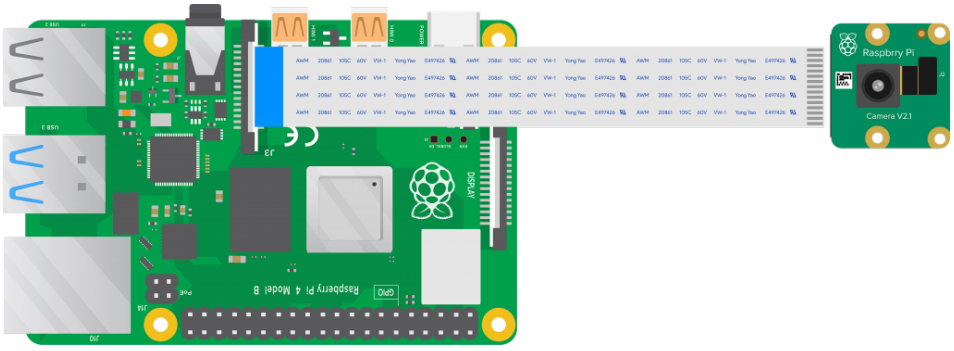


**Figura 11: Conexão da câmera com Raspberry.**

A conexão entre a câmera e o Raspberry Pi é realizada através do conector SFW15R-2STE1LF, conforme mostrado na Figura 11. Este conector de 15 pinos é utilizado para a interface CSI (Camera Serial Interface), que oferece uma largura de banda suficiente para suportar a transmissão de vídeo de alta resolução.

### 3.1.3 Visão noturna

Para que o sistema possa operar em ambientes com pouca iluminação, foi utilizada uma lâmpada com LEDs infravermelhos, comumente empregada em sistemas de segurança. A lâmpada é alimentada por uma fonte de 12V e emite luz infravermelha na faixa de 850nm do espectro. O acionamento dos LEDs infravermelhos ocorre apenas quando o sensor fotoresistor LDR detecta baixos níveis de luz no ambiente. Caso haja iluminação suficiente, os LEDs permanecem desligados, garantindo economia de energia e eficiência no funcionamento do sistemas.

Este dispositivo pode ser visualizado na Figura 12 em uma estrutura modelada e impressa para suportar a câmera e a lâmpada de LEDs juntas.

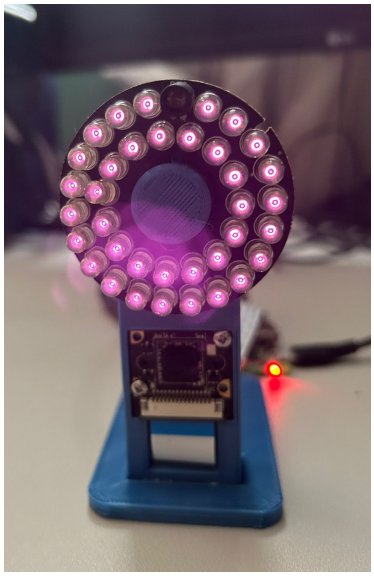

**Figura 12: Lâmpada de infravermelho**

## 3.2 Construção do dataset

O dataset criado para a classificação das imagens de uma pessoa foi dividido em três categorias: imagens reais, falsas em papel e falsas em tela. As imagens reais foram subdivididas em diurnas e noturnas. As imagens diurnas foram capturadas com a luz solar incidindo diretamente sobre a pessoa alvo. Já as imagens noturnas foram obtidas em um ambiente completamente escuro, onde a única fonte de iluminação disponível era a lâmpada de infravermelho. Ambas as imagens falsas foram capturadas com luz solar presente no ambiente.

As imagens para falsificação, mostradas na Figura 13, fora feitas com um celular no modelo Iphone 14 que possui uma câmera de 12 megapixels. Uma câmera com alta resolução é capaz de capturar detalhes finos, texturas da pele, nuances de cor e outros atributos visuais críticos, essenciais para criar imagens falsas realistas. Essas imagens de alta qualidade aumentam a dificuldade para os algoritmos de detecção de falsificação, pois as falsificações apresentam um nível de detalhe e qualidade muito próximos aos das imagens reais.

Para as imagens falsas em papel, foram utilizadas impressões de alta qualidade reveladas em papel fotográfico A4 colorido. Já para as imagens falsas na tela, foi utilizado um monitor de 60 Hz com tecnologia IPS.

## 3.3 Detecção facial e captura de imagens

Para detectar a presença de rostos e capturar fotos para a criação de um dataset, utilizamos a biblioteca OpenCV. Essa biblioteca oferece uma ampla gama de ferramentas

**Figura 13: Fotos com Iphone 14.**

para processamento de imagens e visão computacional, incluindo algoritmos eficientes para detecção facial.

A técnica escolhida para a detecção facial foi a Detecção de Objetos usando Classificadores em Cascata baseados em características Haar. Essa abordagem é baseada em aprendizado de máquina, onde uma função em cascata é treinada com um grande número de imagens positivas (contendo rostos) e negativas (sem rostos). Após o treinamento, essa função pode ser aplicada a novas imagens para identificar a presença de rostos [4].

O processo de detecção começa carregando o classificador em cascata previamente treinado fornecido pelo OpenCV. Em seguida, a imagem é convertida para escala de cinza, pois a detecção de características Haar funciona mais eficientemente em imagens monocromáticas. Após a conversão, o algoritmo de detecção é aplicado, resultando em coordenadas das regiões da imagem onde os rostos foram detectados.

A Figura 14 mostra um exemplo de detecção realizada pelo OpenCV, onde a região retangular do rosto é destacada, apenas região do rosto é salva para o dataset. Isso evita interferências que podem ocorrer devido ao fundo da imagem ou outros elementos não relevantes.

O processo completo de identificação de uma pessoa como verdadeira ou uma falsificação começa com a detecção do rosto. Após a detecção facial, o algoritmo de detecção de pele humana é executado. O sucesso deste processo depende da identificação precisa de um rosto, seguida pela confirmação de que o rosto pertence a uma pessoa real. Assim, o sistema pode determinar com eficácia se a imagem representa uma pessoa autêntica ou uma tentativa de falsificação.

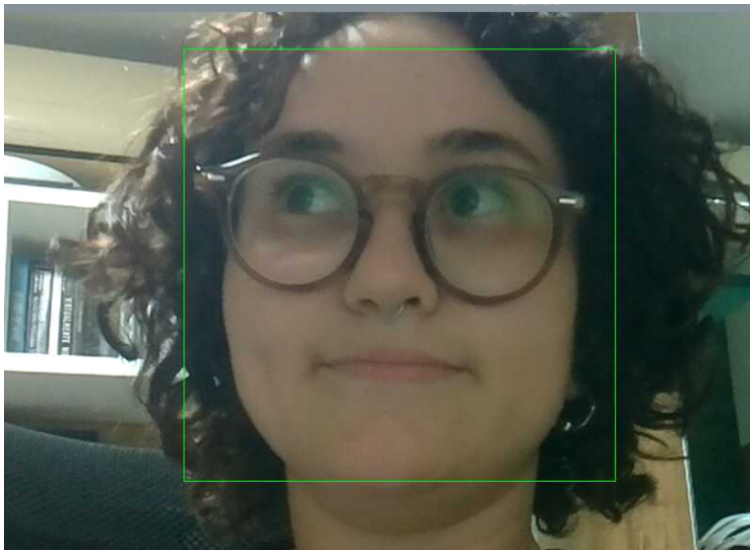

**Figura 14: Exemplo de detecção feita pelo OpenCV**

### 3.4 Algorítmo para detecção de pele humana

Neste projeto, foi implementado um algoritmo em Python baseado no conceito de Normalized Difference Vegetation Index (NDVI), adaptado para a detecção de pele humana, inspirado pelo trabalho de [19] sobre o Normalized Difference Skin Index (NDSI). O NDSI demonstrou ser uma ferramenta eficaz para a detecção de pele em imagens, explorando a diferença na refletância da pele humana nos comprimentos de onda do infravermelho próximo (NIR). A abordagem é motivada pela capacidade da pele humana de refletir a luz de forma diferente dependendo do nível de melanina e da absorção de água nas camadas dérmicas.

A adaptação do NDVI para a detecção de pele humana segue uma lógica semelhante à utilizada para a vegetação. No caso das plantas, elas parecem verdes ao olho humano porque o pigmento de clorofila reflete a luz verde e absorve outros comprimentos de onda. Além disso, as plantas evoluíram para refletir a maior parte da luz infravermelha, evitando o superaquecimento [5]. Esse princípio, onde uma planta saudável reflete infravermelho e absorve luz visível, é essencial para o cálculo do NDVI e, ao ser aplicado à pele humana, permite explorar as características únicas da reflexão de luz na pele, similar ao processo de detecção de vegetação.

O NDVI é calculado utilizando a fórmula abaixo, onde a diferença entre o infravermelho próximo (NIR) e a luz visível (VIS) é dividida pela soma desses dois valores:

$$NDVI = \frac{NIR - VIS}{NIR + VIS}$$

Adaptando este conceito para a pele humana, o algoritmo calcula o valor final do NDVI de cada pixel, simplesmente calculando a diferença entre o infravermelho próximo

(que está sendo armazenado no canal vermelho) e a luz visível (no canal azul), e dividindo pela soma de ambos, de modo que cada pixel terá um valor entre -1 e 1 no final.

Com todos os valores de NDVI calculados para cada pixel, o algoritmo então pega a porção central de 15% da imagem e calcula a média dos pixels nessa região. Esse procedimento é realizado para minimizar a influência de reflexões externas, como o plano de fundo da imagem, garantindo que o foco seja direcionado exclusivamente à pele. Se a média obtida for superior ao limiar estabelecido, o canal azul é utilizado para executar o algoritmo biométrico facial, pois indica que a imagem contém uma representação clara do rosto. Caso contrário, se a média não atingir o limiar, a imagem é rejeitada.

Inicialmente, o limiar foi definido como 0, para diferenciar de forma clara entre imagens falsas e reais. No entanto, com a introdução de imagens reais capturadas em ambientes noturnos, o limiar foi ajustado para -0.07, de acordo com os resultados obtidos no Capítulo 4, garantindo que esse novo cenário fosse adequadamente considerado sem comprometer a precisão dos resultados.

# 4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

As imagens reais, como ilustrado na Figura 15, apresentaram uma coloração rosada devido à alta incidência de infravermelho originada da pele humana. Essa característica é esperada, uma vez que a pele humana reflete mais luz infravermelha, resultando em uma tonalidade distinta que auxilia na identificação de rostos reais no dataset.

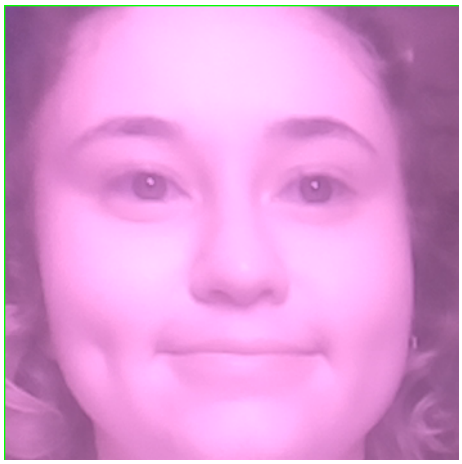

**Figura 15: Captura de uma imagem real diúrna.**

A Tabela 1 mostra as médias de nove imagens diúrnas reais que serviram para testar o algorítmo. Pode ser observado que a média dos valores de NDVI fica em torno de 0,01 até 0,09 em todos os testes realizados, corroborando a consistência dos resultados obtidos para as imagens reais.

Os resultados das imagens reais noturnas apresentaram o mesmo tom rosado observado nas imagens diurnas, porém com um fundo completamente escuro, destacando apenas o rosto da pessoa alvo, como mostrado na Figura 16.

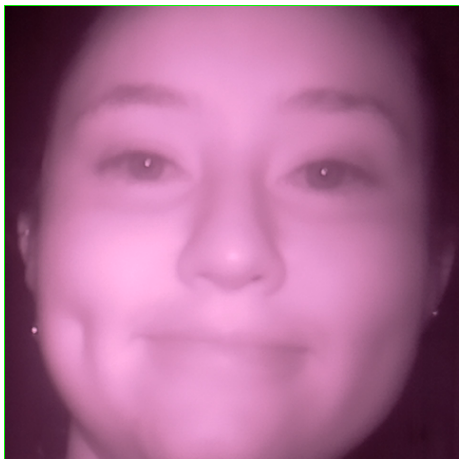

**Figura 16: Captura de uma imagem real noturna.**

Já para as imagens capturadas em ambientes noturnos, com iluminação infraver-

**Tabela 1: Teste em imagens reais diúrnas.**

| Imagem | Média | Resultado |
|---|---|---|
| **2024-06-09_12-38-00.png** | 0.065 | Real |
| **2024-06-09_12-38-41.png** | 0.0173 | Real |
| **2024-06-09_12-38-54.png** | 0.0158 | Real |
| **2024-06-09_12-38-56.png** | 0.0179 | Real |
| **2024-06-09_12-38-58.png** | 0.0218 | Real |
| **2024-06-09_12-38-59.png** | 0.0521 | Real |
| **2024-06-09_12-39-04.png** | 0.0580 | Real |
| **2024-06-09_12-39-04.png** | 0.0318 | Real |
| **2024-06-09_12-38-37.png** | 0.0127 | Real |

melha, os resultados foram um pouco mais variáveis. Assim como nas imagens diurnas, as imagens noturnas também apresentaram uma coloração rosada, devido à reflexão da luz infravermelha pela pele humana. No entanto, como ilustrado na Tabela 2, alguns valores de NDVI foram ligeiramente negativos, como -0,002 e -0,064, o que indicou a necessidade de ajuste no limiar de detecção.

Inicialmente, o limiar estava estabelecido em 0, adequado para a detecção de imagens diurnas. Contudo, devido à maior variabilidade nas imagens noturnas, o limiar foi ajustado para -0,07, permitindo que o sistema considerasse essas imagens sem comprometer a precisão dos resultados. Esse ajuste foi essencial para abranger as condições de baixa iluminação e garantir que as imagens noturnas fossem corretamente classificadas como reais, apesar das variações nos valores de NDVI.

No grupo das imagens de falsificação utilizando uma tela, como mostrado na Figura 17, observou-se uma predominância de coloração azul, característica da luz emitida pelas telas digitais. Este padrão de coloração é um indicativo claro de uma tentativa de falsificação, diferenciando-se significativamente das imagens reais capturadas.

A Tabela 3 mostra as médias de 9 imagens de falsificação em tela, de cada foto indicadas na Figura 13. É possível observar que a média dos valores de NDVI, independentemente da foto, se mantém em torno de -0,9. Por outro lado, o grupo das falsificações utilizando papel, apresentada na Figura 18 falhou na etapa de identificação de existência

**Tabela 2: Teste em imagens reais noturnas**

| Imagem | Média | Resultado |
|---|---|---|
| **2024-09-21_14-03-06.png** | 0.066 | Real |
| **2024-09-21_14-03-07.png** | 0.0412 | Real |
| **2024-09-21_14-03-08.png** | 0.093 | Real |
| **2024-09-21_14-03-19.png** | -0.002 | Real |
| **2024-09-21_14-03-20.png** | -0.060 | Real |
| **2024-09-21_14-03-22.png** | -0.064 | Real |
| **2024-09-21_14-03-39.png** | 0.096 | Real |
| **2024-09-21_14-03-40.png** | 0.024 | Real |
| **2024-09-21_14-03-43.png** | 0.093 | Real |

de rostos pela câmera, tanto de dia quanto de noite. Esse insucesso na detecção inicial significa que essas imagens nem sequer prosseguiram para o algoritmo de detecção de pele humana. A incapacidade de identificar rostos nessas imagens pode ser atribuída à falta de nitidez ocasionada pela absorção do infravermelho do papel, fazendo com que a imagem do rosto apresente um baixo contrastem, diferente das imagens reais.

Em resumo, a análise dos resultados mostrou que o sistema foi eficaz em distinguir entre imagens reais e tentativas de falsificação, seja por tela ou papel. As imagens reais apresentaram as características esperadas de reflexão de infravermelho, enquanto as tentativas de falsificação foram corretamente identificadas e rejeitadas pelo sistema.

**Figura 17: Captura de uma imagem falsa na tela.**

**Figura 18: Captura de uma imagem falsa no papel.**

**Tabela 3: Teste em imagens falsas na tela.**

| Imagem | Média | Resultado |
|---|---|---|
| **2024-07-07_23-27-30.png** | -0.997 | False |
| **2024-07-07_23-27-48.png** | -0.999 | False |
| **2024-07-07_23-28-06.png** | -0.991 | False |
| **2024-09-15_22-42-25.png** | -0.9985 | False |
| **2024-09-15_22-47-15.png** | -0.9983 | False |
| **2024-09-15_22-49-31.png** | -0.974 | False |
| **2024-09-15_22-52-09.png** | -0.921 | False |
| **2024-09-15_22-53-30.png** | -0.865 | False |
| **2024-09-15_22-55-11.png** | -0.839 | False |

# 5 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou uma metodologia para a detecção de vivacidade em imagens utilizando a Câmera NoIR para Raspberry Pi e algoritmos de processamento de imagem baseados no NDVI e na detecção facial. O objetivo principal era desenvolver um sistema simples, porém capaz de diferenciar entre imagens reais e tentativas de falsificação, utilizando características únicas de reflexão de luz infravermelha pela pele humana.

Os resultados obtidos demonstraram que o sistema é eficaz em identificar rostos reais tanto em cenários diúrnos e norturnos, caracterizados por uma coloração rosada devido à alta reflexão de infravermelho, e em detectar falsificações, que apresentaram colorações distintas, como o azul das telas digitais e a baixa nitidez das impressões em papel. As médias dos valores de NDVI para as imagens reais de dia ficaram entre 0,01 e 0,09 e para imagens reais de noite variam entre 0,09 até -0,07, enquanto as imagens falsas na tela apresentaram valores consistentes em torno de -0,9, confirmando a capacidade do algoritmo em identificar falsificações.

Apesar dos resultados promissores, o sistema apresentou uma quantidade considerável de falsos-positivos durante a detecção de rostos. Isso sugere a necessidade de explorar métodos de detecção mais avançados, que possam melhorar a precisão e reduzir as falhas nas classificações. Além disso, futuras pesquisas poderiam se concentrar em explorar tentativas mais sofisticadas de burlar o sistema, como o uso de filtros de cores distintas, para testar a robustez do algoritmo frente a novas técnicas de falsificação.

Em resumo, este trabalho oferece uma contribuição significativa ao campo da segurança biométrica, apresentando uma solução prática para a detecção de falsificações com base na refletância infravermelha da pele humana. As melhorias e expansões futuras poderão aumentar ainda mais a confiabilidade e a aplicabilidade deste sistema em cenários reais, tornando-o uma ferramenta valiosa para a segurança de sistemas biométricos

# REFERÊNCIAS


[1] Ming, Zuheng, et al. A survey on anti-spoofing methods for facial recognition with rgb cameras of generic consumer devices. **Journal of imaging**, v. 6, n. 12, p. 139, 2020.

[2] LIU, Yan; YU, Feihong. Automatic inspection system of surface defects on optical IR-CUT filter based on machine vision. **Optics and Lasers in Engineering**, v. 55, p. 243-257, 2014.

[3] KANZAWA, Yusuke; KIMURA, Yoshikatsu; NAITO, Takashi. Human skin detection by visible and near-infrared imaging. **IAPR Conference on Machine Vision Applications**, v. 20, p. 14-22, 2011.

[4] Cascade Classifier. OpenCV, 2024. Disponível em: <https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html>. Acesso em: 03 de Agosto de 2024.

[5] RASPBERRY PI FOUNDATION. Astro Pi: NDVI. Disponível em: <https://projects.raspberrypi.org/en/projects/astropi-ndvi/1>. Acesso em: 14 set. 2024.

[6] LAGORIO, Andrea; TISTARELLI, Massimo; CADONI, Marinella; FOOKES, Clinton; SRIDHARAN, Sridha. Liveness detection based on 3D face shape analysis. **In: 2013 International Workshop on Biometrics and Forensics (IWBF)**, p. 1–4. IEEE, 2013.

[7] ZHANG, Zhiwei; YI, Dong; LEI, Zhen; LI, Stan Z. Face liveness detection by learning multispectral reflectance distributions. **In: Face and Gesture 2011**, p. 436–441. IEEE, 2011.

[8] YI, Dong; LEI, Zhen; ZHANG, Zhiwei; LI, Stan Z. Face anti-spoofing: Multi-spectral approach. **In: Handbook of Biometric Anti-Spoofing**, p. 83–102. Springer, 2014.

[9] SUN, Lin; HUANG, WaiBin; WU, MingHui. TIR/VIS correlation for liveness detection in face recognition. **In: International Conference on Computer Analysis of Images and Patterns**, p. 114–121. Springer, 2011.

[10] UNIVERSIDADE FEDERAL DE MINAS GERAIS. Como o olho funciona. Belo Horizonte: Espaço do Conhecimento, 2024. Disponível em: <https://www.ufmg.br/espacodoconhecimento/como-o-olho-funciona/>. Acesso em: 14 set. 2024.

[11] LIU, Siqi; YANG, Baoyao; YUEN, Pong C.; ZHAO, Guoying. A 3D mask face anti-spoofing database with real world variations. **In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops**, p. 100–106, 2016.

[12] KOLLREIDER, Klaus; FRONTHALER, Hartwig; BIGUN, Josef. Verifying liveness by multiple experts in face biometrics. **In: CVPR Workshops**, p. 1–6. IEEE, 2008.

[13] ZHANG, Zhiwei; YAN, Junjie; et al. A face antispoofing database with diverse attacks. **In: International Conference on Biometrics**, p. 26–31. IEEE, 2012.

[14] URME SURVEILLANCE. URME Surveillance. Chicago: URME, 2024. Disponível em: <http://www.urmesurveillance.com/>. Acesso em: 14 set. 2024.

[15] Erdogmus, Nesli; Marcel, Sébastien. Introduction. **In: Handbook of Biometric Anti-Spoofing**, p. 1-11. Springer, 2014.

[16] SOUZA, Luiz; OLIVEIRA, Luciano; PAMPLONA, Mauricio; PAPA, Joao. How far did we get in face spoofing detection? **Engineering Applications of Artificial Intelligence**, v. 72, p. 368–381, 2018.

[17] RASPBERRY PI FOUNDATION. Camera Module Documentation. Cambridge: Raspberry Pi, 2024. Disponível em: <https://www.raspberrypi.com/documentation/accessories/camera.html>. Acesso em: 10 set. 2024.

[18] RASPBERRY PI FOUNDATION. Raspberry Pi 3 Model B+. Cambridge: Raspberry Pi, 2024. Disponível em: <https://www.raspberrypi.com/products/raspberry-pi-3-model-b-plus/>. Acesso em: 14 set. 2024.

[19] MENDENHALL, Michael J.; NUNEZ, Abel S.; MARTIN, Richard K. Human skin detection in the visible and near infrared. **Applied Optics**, v. 54, n. 35, p. 10559-10570, 2015.