

# **DIMPE: UMA APLICAÇÃO DE VISÃO COMPUTACIONAL COM DRONE PARA AUXILIAR NO MONITORAMENTO DE PERÍMETRO**

## **DIMPE: A COMPUTER VISION APPLICATION WITH DRONE TO ASSIST IN PERIMETER MONITORING**

Gabriel Silva Pimentel\*  
Andressa Bezerra Ferreira\*\*  
Alexandro Lima Damasceno\*\*\*

### **RESUMO**

O DIMPE apresenta a aplicação de um modelo de inteligência artificial para classificar e identificar objetos em imagens, executando diretamente no navegador e identificando, em tempo real, possíveis invasores a partir de imagens de um drone autônomo. A finalidade deste trabalho é auxiliar profissionais de segurança no processo de patrulhamento e vigilância, diminuindo a exposição a riscos iminentes. Este estudo apresenta resultados de uma pesquisa feita com mais de 20 seguranças, onde foram constatados problemas psicológicos causados pela exposição a situações de risco. Com isso, busca contribuir para a redução do risco enfrentado pelos profissionais de segurança, promovendo assim um ambiente de trabalho mais seguro e tranquilo.

**Palavras-chave:** 1. Drone. 2. Inteligência Artificial. 3. Segurança

### **ABSTRACT**

DIMPE presents the application of an artificial intelligence model to classify and identify objects in images, running directly in the browser and identifying, in real time, possible intruders from images of an autonomous drone. The purpose of this work is to assist security professionals in the patrolling and surveillance process, reducing exposure to imminent risks. This study presents the results of a survey conducted with more than 20 security guards, where psychological problems caused by exposure to risky situations were found. With this, the aim is to contribute to reducing the risk faced by security professionals, thus promoting a safer and calmer work environment.

**Keywords:** 1. Drone. 2. Artificial Intelligence. 3. Security Data de submissão para publicação: 20 set. 2024.

Data de aprovação para publicação: 06 jun. 2018.

\* Currículo sucinto do autor, com vinculação corporativa e endereço de contato.

\*\* Currículo sucinto do autor, com vinculação corporativa e endereço de contato.

\*\*\* Currículo sucinto do autor, com vinculação corporativa e endereço de contato.

Aqui pode ser indicado o endereço eletrônico, DOI, suportes e outras informações relativas ao acesso do documento.

## 1 INTRODUÇÃO

Inicialmente, os drones foram projetados para atender a operações civis e militares, sendo usados em tarefas como resgate, monitoramento climático, vigilância e previsão meteorológica (AHMED, 2022). Com o aprimoramento e popularização dessa tecnologia, sua aplicação expandiu para diversas áreas. Ainda assim, um dos usos mais comuns dos drones está associado a sistemas de câmeras, já que, conforme Ghamari (2022), a maior parte da movimentação no mercado de drones provém das indústrias de infraestrutura, agricultura e segurança, devido à sua capacidade de capturar imagens (GHAMARI, 2022).

No Brasil, o uso de drones no setor público está cada vez mais disseminado, principalmente na área de segurança. Jorge (2018) apresenta diversas aplicações, como perseguição de criminosos, observação de locais perigosos para policiais e combate a incêndios (JORGE, 2018). Além disso, esses aparelhos são frequentemente usados para monitorar ambientes externos, sendo considerados eficazes na prevenção de atos ilícitos e invasões, além de garantir o controle de acesso.

Nesse contexto, é importante destacar os desafios e riscos enfrentados pelos profissionais de segurança, e como os drones podem auxiliá-los. De acordo com o Anuário Brasileiro de Segurança Pública, em 2022, cerca de 161 policiais civis e militares foram assassinados e 98 cometeram suicídio (PÚBLICA, 2023). Entre os mortos, 7 em cada 10 estavam de folga, representando mais de 20 assassinatos em relação ao ano anterior. Esses dados revelam a realidade da insegurança enfrentada por esses profissionais, muitas vezes pela falta de equipamentos adequados ou tecnologias que possam reduzir os riscos em suas operações.

Com base nos desafios enfrentados pelos profissionais de segurança, este trabalho tem como objetivo desenvolver um sistema de monitoramento composto por um drone autônomo e software de visão computacional, capaz de identificar invasores e auxiliar no controle perimetral de áreas públicas e privadas. O projeto abrange dois objetivos principais: a construção de um drone para captar imagens em áreas de segurança e o desenvolvimento de um sistema para processar e classificar essas imagens. Uma pesquisa realizada com mais de 20 profissionais de segurança mostrou que o uso de tecnologias como câmeras, drones e sensores biométricos contribui significativamente para o controle de acesso e a vigilância de grandes áreas, reduzindo a exposição ao risco e oferecendo maior segurança.

Este trabalho visa aumentar a segurança dos vigilantes, permitindo que eles antecipem e reajam de forma mais eficaz a invasões de propriedades, especialmente em locais como o IFCE Campus Aracati, onde já ocorreram furtos de materiais de construção. A justificativa para este estudo se baseia na vulnerabilidade desses profissionais, agravada pela falta de autorização para portar armas, o que os coloca em desvantagem em situações de confronto. Assim, este trabalho propõe um sistema integrado com drone para otimizar o controle de acesso em áreas externas,

protegendo tanto as pessoas quanto os bens materiais, com possíveis aplicações no IFCE e em outros contextos similares.

As seções seguintes deste trabalho está organizada em seis seções principais. O Referencial Teórico revisa os conceitos fundamentais e as bases teóricas relevantes ao tema abordado. A seção de Trabalhos Correlatos discute pesquisas anteriores relacionadas ao tecnologias em questão. Na Metodologia, detalha-se o processo e os métodos adotados para o desenvolvimento da solução proposta, que é descrita na seção de Proposta de Solução. A Validação da Solução demonstra os experimentos e análises que comprovam a eficácia da abordagem sugerida. Em Limitações e Trabalhos Futuros, são discutidas as restrições identificadas e possíveis melhorias para pesquisas futuras. Por fim, as Considerações Finais sintetizam as principais conclusões obtidas ao longo do estudo.

## 2 REFERENCIAL TEÓRICO

Com a finalidade de proporcionar uma compreensão completa e aprofundada sobre o tema abordado neste artigo, esta seção fornecerá uma base teórica essencial que constitui a fundação deste trabalho. Além disso, serão apresentados termos técnicos e as tecnologias empregadas no desenvolvimento da proposta, buscando esclarecer de maneira abrangente os elementos-chave envolvidos na abordagem proposta.

### 2.1 Drones

Conhecidos como Veículos Aéreos Não Tripulados (VANTs) ou Unmanned Aerial Vehicle (UAV), os drones são aeronaves que podem ser controladas remotamente por um operador ou seguir um caminho pré-programado. Segundo Cinnamon (2016), os drones possuem uma ampla gama de aplicações, e as áreas mais promissoras para o uso estão relacionadas à topologia, agricultura, entretenimento e entregas (CINNAMON; TEPPER; KADRI, 20216).

A primeira tentativa bem sucedida de criação de VANT teve sua aplicação na área militar, desenvolvido pelos EUA, o modelo Hewitt-Sperry teve uma versão mais avançada produzida em grande escala chamada: Kettering Bug. Produzido em 1918 ele chegou tarde demais para ser usado na primeira guerra mundial, estes modelos são classificados como planadores pelo fato de parecerem com aviões (MARTINEZ, 2018).

Existem vários modelos de drones, e dentro deles há especificações que classificam o uso de cada modelo. Os mais comuns são os planadores ou aeromodelos, que utilizam o mesmo princípio dos aviões; os multirotores, que possuem dois ou mais motores e podem ter asas ou não; e, por último, os quadricópteros, que possuem quatro motores dispostos em formato de X. Dentre os modelos citados, cada um tem finalidades distintas, como por exemplo: filmagem, corrida, manobras e monitoramento.

Para filmagem de grandes extensões territoriais, o modelo de drone mais utilizado é o drone FPV (First Person View) *Long Range*, que é uma subclassificação de quadricóptero. As características atribuídas a esse tipo de drone são: transmissão de imagem em um raio de

5 km a 15 km, adição de GPS para auxiliar na função de *return to home* e a capacidade de carregar baterias maiores. Esses elementos combinados não apenas proporcionam uma autonomia estendida, mas também ampliam significativamente a distância de voo. Além disso, a presença do GPS desempenha um papel crucial, permitindo que o drone retorne automaticamente à coordenada de decolagem em caso de perda de sinal de rádio.

O uso civil de drones se difundiu nos últimos anos. De acordo com Santos (2022), houve um crescimento de 11,3% no número de drones registrados no Brasil. Em 2020, foram 79.859 registros, aumentando para 90.030 em 2021. Esses números representam uma ampliação dos campos de aplicação dessa tecnologia, já que a justificativa para esse crescimento foi a adaptação a novos formatos de trabalho exigidos pela pandemia, o que gerou alta demanda por empresas especializadas em inspeções, mapeamentos e levantamentos com drones (SANTOS, 2022). Cada aplicação exige um modelo com especificações próprias; por isso, o foco deste trabalho será na utilização dos modelos quadricópteros.

A montagem de drones, especialmente os modelos *Long Range*, oferece maior autonomia e abrangência, representando um campo importante de exploração tecnológica. Nesse contexto, a escolha de um quadricóptero *Long Range* implica a consideração das características especificadas anteriormente. No tópico seguinte, serão discutidos os processos de configuração, montagem e teste de drones, considerando que drones FPV são geralmente montados pelos próprios pilotos, sendo importante a compreensão de todo o processo para este trabalho.

## 2.2 Configuração, montagem e teste de drone

Existe uma grande gama de modelos, tamanhos e marcas de drones, mas muitas delas trabalham com o conceito de código fechado, onde o projeto não permite aprimoramentos por parte da comunidade. Entretanto, existem *hardwares* e *softwares* voltados para drones que adotam o conceito de código aberto. Para isso, é necessário que toda a montagem, configuração e teste sejam realizados pelo usuário. A escolha de montar um drone neste trabalho se dá pela necessidade de ter acesso aos códigos e *datasheets* dos equipamentos utilizados, para modificá-los conforme necessário.

A plataforma utilizada para configurar o drone se chama INAV<sup>1</sup>. Nela, é possível ajustar os parâmetros PID (Proporcional, Integral e Derivativo), filtros e modos de voo (INAVFLIGHT, 2021). Os modos de voo são responsáveis por configurar a forma como o piloto controla o equipamento. Os modos de voo que serão utilizados são: *acro*, *angle* e *waypoint*. O modo *acro* desabilita o giroscópio e o acelerômetro, transferindo o controle de estabilização para o piloto. O modo *angle* nivela automaticamente o drone na ausência de comandos, ao contrário do *acro*, que mantém o drone na mesma posição em que foi deixado caso não haja comandos. O modo *waypoint* utiliza uma rota definida pelo piloto no INAV, e o drone seguirá essa rota de forma autônoma, sem necessidade de intervenção.

---

<sup>1</sup> <https://github.com/iNavFlight/inav>.

Antes de iniciar o processo de configuração, é necessário adicionar os modos de voo que serão utilizados. No INAV, ao acessar a aba "Modos", deve-se selecionar o canal auxiliar que corresponde à chave desejada no rádio. Em seguida, basta ajustar as barras de intervalo para definir em qual posição da chave cada modo de voo será ativado (GROUP, 2021). Esse procedimento deve ser realizado antes dos voos de configuração do drone, evitando que o piloto perca o controle durante o voo ou que o drone fique travado no chão. A Figura 1 apresenta um exemplo do processo descrito acima para a escolha do modo *waypoint*.

Figura 1 – Modo *waypoint* sendo definido no canal 6 do rádio, o slider apresenta o intervalo definido para o modo de voo.



Fonte: Autor.

Para configurar o drone, é necessário ativar uma funcionalidade do INAV chamada Black Box. Quando ativada, a controladora gera um arquivo de log do voo, que contém informações relacionadas ao balanceamento do PID e à presença de vibrações que podem impedir o drone de voar de forma estável (GROUP, 2021). Para analisar esses arquivos de log, utiliza-se a ferramenta PidToolBox<sup>2</sup>, que auxilia na configuração de PID e filtros, apresentando de forma gráfica o comportamento do drone e indicando como ajustar os parâmetros para melhorar o voo.

Para iniciar o processo de configuração, é necessário ajustar os filtros de D-term e os filtros de giroscópio. Esses filtros são responsáveis por ignorar vibrações causadas por turbulências das hélices e por vibrações absorvidas pela estrutura do drone, que são transmitidas ao giroscópio da controladora. Cada tipo de ruído é tratado por um filtro diferente, e a frequência de vibração pode variar de acordo com a montagem do drone. É necessário realizar vários voos e analisar cada um deles até que a maior parte dos ruídos seja eliminada pela ferramenta. O uso excessivo de filtros pode causar superaquecimento e queima dos motores, portanto, o ajuste dos filtros deve seguir a documentação da ferramenta.

Para o processo de configuração do PID, é necessário voar com o drone por 30 segundos em modo angle e girar os sticks de roll e pitch. O roll se refere à inclinação lateral do drone, movendo-o para a esquerda ou direita, enquanto o pitch controla a inclinação para frente e para trás. Esses movimentos são essenciais para gerar informações suficientes para o PidToolBox. De acordo com Liang (2024), os parâmetros de P e D devem estar na posição inicial, e o de I deve estar em 0 (LIANG, 2023).

Inicialmente, é necessário encontrar a proporção de P e D em que o drone não exiba comportamento de mola ao final de um comando, indicando que a proporção está equilibrada (LIANG, 2023). O processo segue a linha de tentativa e erro. Após encontrar o equilíbrio entre P e D, para ajustar o valor de I, é necessário subir o drone a uma altura de 3 a 4 metros, desligar os

<sup>2</sup> <https://pidtoolbox.com/home>.

motores e acelerar rapidamente. Quanto menos vibrações o drone apresentar ao acelerar, melhor será o valor de I.

O INAV possui uma funcionalidade chamada *Mission Control*, que permite o planejamento de missões de voo para drones. Essas missões são carregadas no drone e, com o auxílio de um GPS, ele analisa as coordenadas da missão e se desloca automaticamente para os pontos pré-definidos, chamados de *waypoints*. Após completar o circuito, o drone retorna ao ponto inicial. O *Mission Control* oferece uma ampla gama de recursos de controle e configurações para as missões, mas, para o entendimento do que será apresentado neste trabalho, essa explicação é suficiente (GROUP, 2021).

### 2.3 Drones e Segurança

O uso de algoritmos de identificação de objetos tem grande potencial em diversas áreas, e a segurança é uma delas. Embora a agricultura de precisão já aproveite consideravelmente esse recurso, com drones e visão computacional promovendo maior eficiência e precisão nas práticas agrícolas, o mesmo conceito é altamente relevante para a segurança. Na agricultura, por exemplo, drones como o Agras T40 e o T20P, desenvolvidos pela DJI, são empregados para otimizar as operações agrícolas. No entanto, na área de segurança, os drones ainda não são utilizados em todo o seu potencial para melhorar a proteção de vigilantes e recursos materiais. Apesar de os modelos de drones serem amplamente utilizados na segurança pública e militar, oferecendo benefícios significativos em operações de monitoramento e controle, a segurança privada ainda explora apenas uma fração desse potencial.

Os primeiros modelos de drones foram projetados para uso bélico, em reconhecimento de campo e ataques *kamikaze*. Com a disseminação do uso de drones, tornou-se comum sua aplicação em operações policiais para reconhecimento de áreas em patrulhas ou operações. Em entrevista, Linhares (2018) explica que o equipamento possibilita a geração de imagens online para instrução da tropa em operações corriqueiras (LINHARES, 2018). Costa (2019) apresenta um caso em que drones equipados com câmeras térmicas foram utilizados para garantir a segurança do Rock in Rio (Brasil), possibilitando a identificação de pessoas que tentavam invadir o evento sem autorização. Dessa forma, uma equipe de segurança foi enviada ao local para interceptar os invasores (COSTA, 2019).

Como demonstrado, é possível perceber a importância da utilização de drones na segurança. No entanto, para a implementação dessa tecnologia, é necessário considerar vários aspectos, como treinamento para operação e manutenção do equipamento, além da observância das leis referentes ao seu uso. Portanto, para facilitar o manuseio do equipamento, existem funcionalidades que tornam o uso mais prático, implementadas por meio de sensores, geolocalização, algoritmos de inteligência artificial e identificação de objetos.

Na próxima seção, será abordado como é feita a identificação de objetos em tempo real por meio de Inteligência Artificial, quais modelos estão disponíveis e qual será utilizado neste trabalho. Esse tópico é essencial para entender como os drones e outros sistemas realizam a

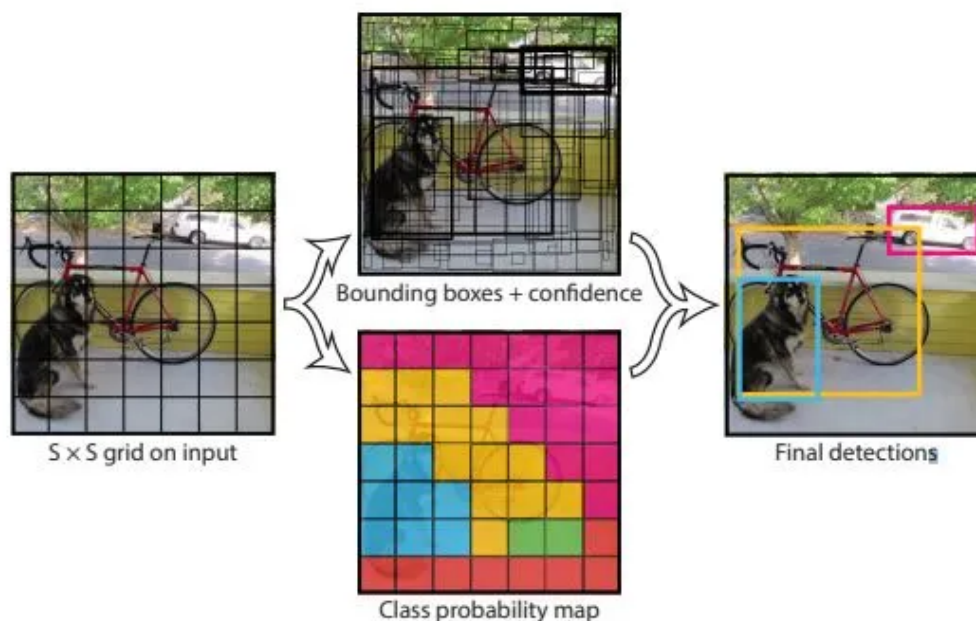
identificação e classificação de objetos em uma imagem.

## 2.4 Identificação de Objetos

A identificação de objetos utilizando visão computacional refere-se ao processo de localizar e reconhecer objetos específicos em imagens ou vídeos. Isso envolve a aplicação de algoritmos e técnicas para detectar a presença de objetos de interesse e atribuir a eles uma classe ou categoria específica (FORSYTH; PONCE, 2012). O reconhecimento de objetos tornou-se uma tarefa fundamental na área de visão computacional, com o objetivo de automatizar a identificação e a interpretação de conteúdo visual por meio de algoritmos e técnicas computacionais. Szeliski (2021), em seu livro, destaca uma ampla variedade de aplicações da visão computacional no mundo real, como o reconhecimento óptico de caracteres (OCR), imagens médicas, condução autônoma, entre outras (SZELISKI, 2021).

A Figura 2 apresenta o processo realizado pelo modelo para identificar e classificar os objetos na imagem. Basicamente, a imagem é dividida em vários quadrados, e são extraídas informações de diferentes partes do objeto. Em seguida, é criado um *bounding box* em cada quadrado, atribuído um valor de confiança, e gerado um mapa de classificação do objeto. Esse mapa considera todas as instâncias, calcula a média entre confiança e classificação, e, por fim, gera a detecção final.

Figura 2 – Retrata o processo que é feito para a detecção.



Fonte: (REDMON et al., 2016).

Atualmente existem diferentes abordagens para classificação de objetos em imagens, e a mais utilizada é a YOLO (You Only Look Once) uma arquitetura de rede neural desenvolvida com objetivo de classificar objetos em tempo real. “A YOLO pode processar imagens em tempo real a 45 quadros por segundo aprendendo representações gerais de objetos e superando outros métodos

de detecção como a R-CNN (Region Based Convolutional Neural Networks)” (REDMON et al., 2016).

A seguir, discutiremos a arquitetura do modelo utilizado na detecção de objetos para analisar as imagens captadas pelo drone. Além disso, abordaremos aspectos técnicos relacionados à visão computacional.

## 2.5 Algoritmo de Identificação

Com a criação de modelos baseados em redes neurais, temos à disposição modelos bem otimizados e reaplicáveis em vários contextos (REDMON et al., 2016). A versão mais atual até o início das atividades deste trabalho é o modelo YOLOv7 e será utilizada especificamente a versão tiny.

A YOLOv7 se destaca por ser considerada a mais otimizada e mais precisa que outras versões e sendo utilizada na indústria para automação de rotinas. A arquitetura do algoritmo se baseia no conceito de “você só olha uma vez”, a imagem só precisa ser passada uma vez pela rede para produzir a classificação e a vantagem disso é a detecção em tempo real, dando a possibilidade de aplicação que necessitam rodar sem nenhum atraso.

A arquitetura do modelo pode ser dividida em três partes principais que são: *Backbone*, *Neck* e *Head*. Começando pelo *Backbone*, resumidamente é uma rede neural convolucional profunda chamada E-ELAN (Extended Efficient Layer Aggregation Network) que extrai as características visuais da imagem de entrada. (WANG; BOCHKOVSKIY; LIAO, 2022) baseou a eficiência da camada convolucional pelo custo necessário para manter a camada na memória, juntamente com a distância do gradiente que percorre a rede. Chegou-se à conclusão que, ao controlar o caminho de gradiente mais longo e mais curto, uma rede mais profunda pode aprender e convergir de forma eficaz. Este controle é feito a partir do embaralhamento e a mesclagem de cardinalidade que resulta no aumento contínuo da capacidade de aprendizagem.

O *Neck* é uma coleção de camadas de rede neural que combina e mistura recursos para passá-los para o próximo estágio de previsão. Ele é responsável por agregar as características de diferentes níveis de resolução do *backbone*. Usando uma estrutura chamada SPP (Spatial Pyramid Pooling), que aplica diferentes tamanhos de janela de *pooling* para capturar as características de diferentes escalas.

O *Head* consome recursos do *Neck* e cria saídas de previsão, que consiste em três camadas de detecção que produzem três saídas de diferentes tamanhos. Cada saída contém uma grade de células, e cada célula contém vários *anchors* ou caixas de ancoragem, que são caixas pré-definidas com diferentes formas e tamanhos. Cada anchor contém um vetor de predição, que consiste em cinco valores: a probabilidade de existir um objeto, as coordenadas do centro e as dimensões da caixa delimitadora do objeto, e a probabilidade de pertencer a um das classes de objetos.



## 2.6 Dataset e treinamento

Modelos de redes neurais, como o YOLO, podem identificar as características dos objetos que irão classificar. Para isso, é necessário um *dataset* que contenha arquivos de imagens e dados relacionados à posição do objeto na imagem. Esses arquivos, chamados de anotações, indicam a posição, o tamanho e a classe do objeto na imagem.

O processo de anotação pode ser feito de várias maneiras, mas a mais comum é utilizando a plataforma chamada roboflow. Jacob (2020) mostra como a plataforma conta com vários recursos, sendo algumas delas a possibilidade de exportar todas as imagens para criação de um *dataset*, fazer anotações e importar para o formato de outras versões da família YOLO. Além disso, é possível ver, contribuir e utilizar *datasets* criados por outros usuários (SOLAWETZ, 2020).

Após a anotação das imagens, o *dataset* é dividido em três partes: treinamento, validação e teste. Durante o treinamento, o conjunto de treinamento é processado pela rede neural, que gera previsões de *bounding boxes* e classes para os objetos nas imagens, em um processo chamado *Forward Pass*. Cada ciclo completo em que todos os exemplos do *dataset* de treinamento passam pela rede é chamado de época. O treinamento de um modelo geralmente envolve múltiplas épocas, permitindo que o modelo se ajuste progressivamente com base nos erros identificados nas épocas anteriores.

Ao final do treinamento, os pesos do modelo que produziram os melhores resultados nos dados de validação são salvos. Esses pesos serão usados na fase de inferência, quando o modelo for aplicado em novas imagens e apresentado gráficos dos resultados obtido.

## 2.7 Métricas de acurácia

As métricas de acurácia avaliam o desempenho do modelo no contexto em que ele foi treinado. No caso do modelo YOLOv7, essas métricas incluem, entre outras, a precisão (precision), o recall, a média de precisão média (mAP) e a pontuação F1. Diante disso, os tópicos seguintes apresentam métricas que serão aplicadas neste trabalho para avaliar o modelo.

### 2.7.1 Precision (Precisão)

Em um contexto de classificação, a precisão é uma das métricas de avaliação mais amplamente utilizadas (SANTOS; BEKO; LEITHARDT, 2022). Ela indica a proporção de predições corretas em relação ao total de predições realizadas pelo modelo. Em termos práticos, a precisão é a fração de detecções verdadeiras (True Positives - TP) em relação ao total de detecções positivas, ou seja, a soma das detecções verdadeiras (True Positives) e das detecções falsas (False Positives). Assim, a precisão avalia a capacidade do modelo de minimizar as falsas detecções ao classificar corretamente as instâncias positivas.

$$\text{Precisão} = \frac{\text{verdadeiro positivo}}{\text{verdadeiro positivo} + \text{falso positivo}}$$

- **True Positives (TP):** São as detecções em que o modelo corretamente identifica um objeto, ou seja, quando a predição corresponde a um objeto real.
- **False Positives (FP):** São as detecções onde o modelo identifica incorretamente algo como um objeto, ou seja, quando a predição não corresponde a nenhum objeto real.

### 2.7.2 Recall (Sensibilidade)

O *recall* é outra métrica essencial para avaliar o desempenho de modelos de detecção de objetos, como o YOLOv7 (CUNHA; CAMARGO, 2019). Enquanto a Precisão foca na proporção de predições corretas entre todas as predições positivas feitas pelo modelo, o *recall* mede a capacidade do modelo de detectar corretamente todos os objetos presentes na imagem.

$$Recall = \frac{\text{verdadeiro positivo}}{\text{verdadeiro positivo} + \text{falso negativo}}$$

- **True Positives (TP):** São as detecções em que o modelo corretamente identifica um objeto, ou seja, quando a predição corresponde a um objeto real.
- **False Negatives (FN):** São os objetos reais que o modelo não conseguiu detectar, ou seja, quando existe um objeto na imagem, mas o modelo não o previu.

### 2.7.3 F1-score

O F1-Score é uma métrica que combina a precisão e o *recall* em uma única pontuação, fornecendo um equilíbrio entre essas duas métricas (NAYEEM; RANA; ISLAM, 2022). É especialmente útil quando você deseja um meio-termo entre a precisão e o *recall*, ou quando precisa avaliar o desempenho do modelo em um cenário onde ambos são igualmente importantes.

$$F1 = 2 \times \frac{\text{precisão} \times \text{recall}}{\text{precisão} + \text{recall}}$$

- **F1-Score Alto (próximo de 1):** Indica que tanto a precisão quanto o *recall* são altos, ou seja, o modelo é bom em detectar a maioria dos objetos (alto recall) e comete poucos erros ao identificar objetos incorretamente (alta precisão).
- **F1-Score Baixo (próximo de 0):** Indica que ou a precisão ou o *recall* (ou ambos) são baixos, o que significa que o modelo está falhando em identificar corretamente os objetos ou está perdendo muitos deles.

### 2.7.4 Average Precision (AP)

O mAP@0.5, é uma métrica abrangente que avalia tanto a precisão quanto a localização das detecções em um modelo de detecção de objetos. Para cada classe, é calculada a precisão em diferentes níveis de recall e, em seguida, calculada a área sob a curva de precisão-recall

(AP). Finalmente, você tira a média das APs (Average Precision) de todas as classes para obter o mAP@0.5.

## 2.8 Interoperabilidade entre frameworks

O ONNX é um formato aberto que facilita a transferência de modelos de redes neurais entre diferentes *frameworks*. Criado pela Microsoft e pelo Facebook em 2017, o ONNX foi projetado para promover a interoperabilidade no desenvolvimento de modelos de IA (MICROSOFT, 2024).

Para que a YOLO possa ser executada diretamente no navegador de um usuário, é necessário realizar um processo de conversão. Após o treinamento do modelo, são gerados arquivos de peso que contêm os parâmetros aprendidos pela rede neural. Esses pesos são originalmente compatíveis apenas com o *framework* PyTorch. No entanto, utilizando o ONNX, é possível converter esses pesos para um formato compatível com o TensorFlow.js<sup>3</sup>, um *framework* de *machine learning* desenvolvido para uso com JavaScript. Isso possibilita a execução do modelo diretamente no navegador.

Esse processo de conversão oferece inúmeras vantagens, pois permite que aplicações web com IA sejam executadas em qualquer dispositivo sem a necessidade de desenvolver uma nova aplicação para cada plataforma. *Frameworks* como Vue.js e Tailwind facilitam o desenvolvimento de aplicações responsivas, garantindo que essas aplicações funcionem em diversos dispositivos, seguindo os padrões de design adequados para cada modelo.

## 3 TRABALHOS CORRELATOS

O uso de drones tornou-se amplamente popular devido a diversos projetos bem-sucedidos em várias áreas. Os estudos apresentados nesta seção destacam a aplicação desses dispositivos em contextos como mapeamento e segurança.

Olive (2020) Este estudo propôs uma abordagem utilizando a rede neural Darknet-53, implementada na YOLOv3, para identificar componentes em redes elétricas a partir de imagens capturadas por drones. A rede foi treinada com imagens de sete tipos diferentes de componentes elétricos, capturadas em várias resoluções. Como resultado, a rede neural obteve uma precisão média (mAP) de 84,16% na detecção dos componentes (OLIVO, 2020).

Kumar (2020) O estudo visa desenvolver um sistema automático de inspeção de trilhos ferroviários utilizando drones. Para isso, drones foram usados para capturar imagens de trilhos simulados, e o modelo VGG16, com aprendizado por transferência, foi empregado para análise. O sistema de visão computacional alcançou uma taxa de sucesso de 96,09% durante o treinamento (KUMAR, 2020).

Munawar (2022) Este estudo tem como objetivo inspecionar edifícios utilizando drones e visão computacional para detectar rachaduras e danos estruturais. Imagens foram capturadas

<sup>3</sup> <https://www.tensorflow.org/js?hl=pt-br>.

por drones e analisadas com técnicas de processamento de imagem para identificar falhas. A abordagem proposta demonstrou alta precisão na detecção de danos em edificações, sendo eficaz na identificação de rachaduras (MUNAWAR et al., 2022).

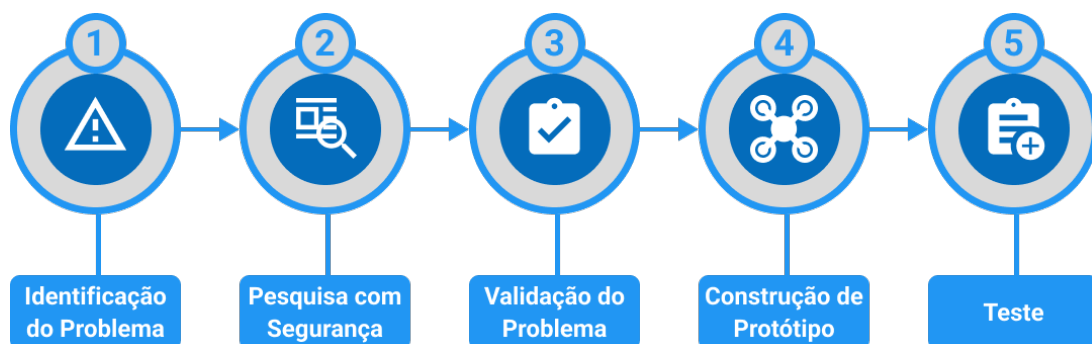
Corturato (2023) descreve o desenvolvimento do sistema Sky Mapping, composto por um drone baseado na plataforma Arducopter, derivada do Arduino, e um software desenvolvido em Python que processa imagens em tempo real obtidas pela câmera do drone. O sistema oferece funcionalidades como voo autônomo, controle manual, transmissão de vídeo em tempo real, reconhecimento de pessoas, geolocalização e captura de imagens. Isso torna o Sky Mapping uma ferramenta valiosa para diversas aplicações, especialmente na vigilância patrimonial, onde é capaz de reconhecer pessoas em diferentes cenários (CORTURATO, 2023).

Embora muitos estudos se concentrem em aplicações de infraestrutura e mapeamento, poucos abordam a identificação em tempo real, como é o caso do trabalho de (CORTURATO, 2023). Este artigo visa preencher essa lacuna ao implementar uma solução de segurança que detecta invasores em tempo real, automatiza a patrulha e melhora o monitoramento de áreas de difícil acesso.

## 4 METODOLOGIA

Esta seção apresenta as etapas da metodologia de desenvolvimento do DIMPE. A Figura 3 resume as atividades desenvolvidas para solucionar o problema abordado neste trabalho. A primeira etapa consiste na identificação de um problema na área de segurança; a segunda, na realização de entrevistas com os vigilantes; a terceira envolve a análise e validação do problema com base nos dados coletados; a quarta etapa abrange a criação do protótipo; e a quinta inclui a realização de testes e a coleta de dados para apresentação dos resultados.

Figura 3 – Apresenta o fluxo de execução da proposta, composta por 5 etapas principais. Cada etapa é detalhada na sequência deste trabalho.



Fonte: Autor.

### 4.1 Etapa 1: Identificação do problema

A primeira etapa da proposta consiste em identificar os problemas de segurança que podem ser abordados neste trabalho. Em instituições de ensino e em locais de construções,

ocorrem incidentes de furto de materiais de construção, gerando prejuízos materiais e colocando os vigilantes em uma posição vulnerável. Esses profissionais são responsáveis por proteger o patrimônio público, mas, em muitos casos, não possuem recursos suficientes para se defender de criminosos, ficando expostos a situações de risco.

A partir de suposições levantadas como: vulnerabilidade dos vigilantes, à falta de tecnologias que possam auxiliar na segurança e a necessidade de soluções mais eficientes, será elaborado um conjunto de perguntas na etapa de pesquisa que abrange validar essas suposições como também entender como é o contexto de trabalho do público alvo. É necessário levar em consideração que o uso de ferramentas tecnológicas pode aprimorar o monitoramento e a proteção, oferecendo dados valiosos que contribuem para uma resposta mais eficaz às ameaças.

Com a identificação desse cenário, a próxima etapa será entender a rotina dos vigilantes e verificar como as questões discutidas se refletem no dia a dia desses profissionais.

#### **4.2 Etapa 2: Pesquisa com segurança**

A Etapa 2 tem como objetivo coletar dados que confirmem as suposições levantadas na etapa anterior. O público-alvo da pesquisa inclui seguranças, policiais e guardas municipais. As perguntas foram elaboradas para entender a rotina desses profissionais, os problemas enfrentados durante rondas ou vistorias, e as situações em que precisaram lidar com invasores ou criminosos. Além disso, busca-se compreender a percepção deles sobre o uso da tecnologia em suas atividades diárias.

As entrevistas foram realizadas com base em um formulário contendo 13 perguntas, possibilitando a obtenção de informações detalhadas para o próximo passo e para a construção de um protótipo. O quadro 1 apresenta as perguntas realizadas aos entrevistados.

#### **4.3 Etapa 3: Validação do problema**

A validação foi realizada com base nas respostas dos entrevistados, com o objetivo de identificar uma necessidade de mercado que possa ser explorada para melhorar a segurança no local e para os vigilantes. A pesquisa incluiu 30 profissionais de segurança, entre eles, a equipe de segurança do IFCE Campus Aracati e seguranças de outras localidades. As perguntas abertas permitiram que os entrevistados abordassem múltiplos aspectos da segurança.

As perguntas não possuíam opções de múltipla escolha, permitindo que os seguranças respondessem mais de um ponto abordado nos gráficos. Isso tornou o processo de classificação das respostas desafiador e complexo. No entanto, após uma análise minuciosa, foram identificadas palavras-chave que possibilitaram a classificação das respostas.

Quadro 1 – Formulário de perguntas.

<b>Questionário</b>	
1	Quais tarefas são realizadas durante um turno típico?
2	Você se sente seguro exercendo sua profissão?
3	Quais são os riscos associados a essa profissão?
4	Existe algo que faria você se sentir mais seguro durante seu serviço?
5	Quais equipamentos e recursos são fornecidos aos vigilantes para realizar seu trabalho?
6	Que tipo de treinamento os vigilantes recebem para lidar com diferentes situações?
7	Em que medida a tecnologia, como recursos tecnológicos, etc., ajuda na detecção e prevenção de invasões?
8	Quais são os problemas mais comuns enfrentados pelos vigilantes em seu trabalho? Como esses problemas afetam sua saúde física e mental?
9	Quais são os procedimentos-padrão que você segue quando suspeita ou presencia uma invasão de propriedade?
10	Existem medidas de autoproteção que você segue?
11	Qual o procedimento de vigia feito em locais com baixa visibilidade ou que não tem acesso viável?
12	Você já fez vistorias em áreas extensas?
13	Você sente que algo pode afetar a estabilidade do seu trabalho, algo que pode lhe substituir?

Fonte: Autor.

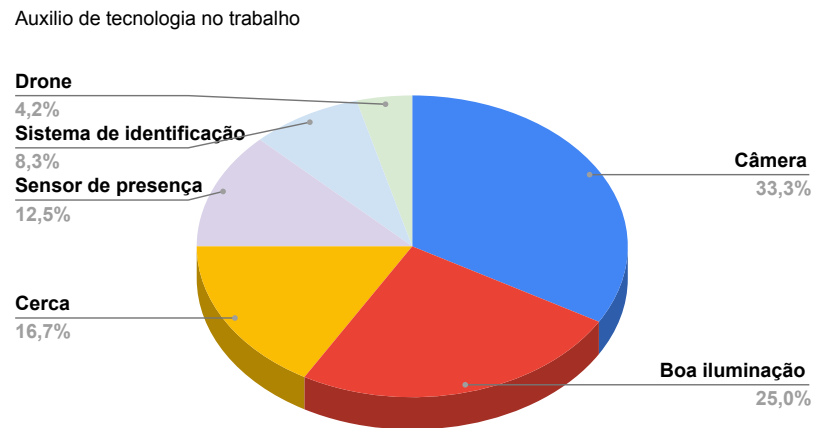
Figura 4 – O gráfico apresenta respostas para as perguntas 3 e 8 que estão relacionadas aos riscos associados à profissão.



Fonte: Autor.

A Figura 4 mostra que o principal ponto identificado foram os riscos associados à profissão enfrentados no dia a dia. Alguns entrevistados relataram múltiplos riscos, incluindo o risco de vida por se sentirem vulneráveis, além de riscos relacionados às condições climáticas e acidentes devido ao transporte durante as rondas.

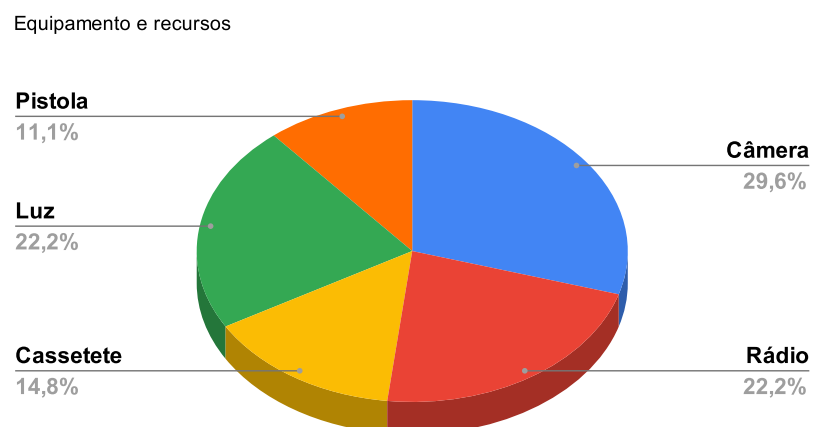
Figura 5 – O gráfico representa as respostas da pergunta 7 que por sua vez esta relacionada com equipamentos que são usados ou que foram sugeridos para melhorar a segurança na rotina de trabalho.



Fonte: Autor.

A Figura 5 apresenta os dados obtidos entre os entrevistados, dos quais 29,6% relataram que permanecem exclusivamente em guaritas e utilizam câmeras de vigilância, pois não realizam rondas e, portanto, não necessitam de outros equipamentos. Por outro lado, 11,1% mencionaram o uso de armas de fogo, embora tenham observado que, em alguns casos, isso pode aumentar o risco, já que há situações em que invasores furtam as armas dos vigilantes.

Figura 6 – O gráfico representa as respostas da pergunta 5, demonstrando os equipamento e recursos utilizados durante o trabalho dos entrevistados.

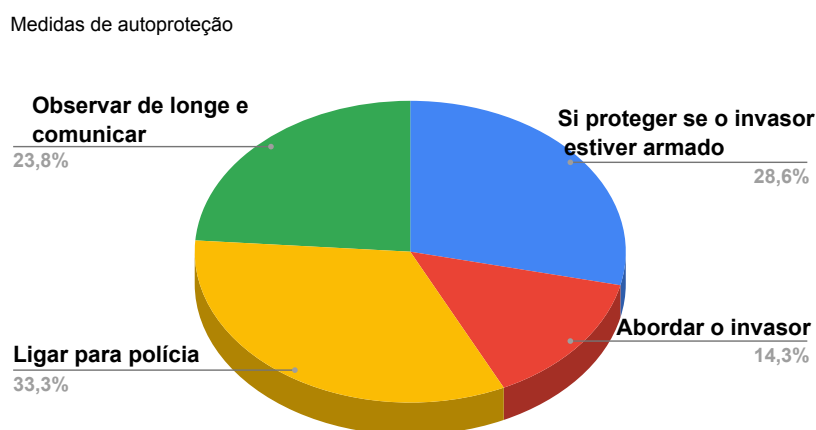


Fonte: Autor.

Na Figura 6, observou-se que o recurso mais utilizado são as câmeras de vigilância, seguido por boa iluminação e cercas, que servem como um paliativo para impedir a entrada de invasores. Uma pequena parcela utiliza sensores de presença, sistemas de identificação e drones.

A baixa adoção dessas tecnologias deve-se ao custo de implementação e ao desconhecimento sobre elas.

Figura 7 – O gráfico representa as respostas das perguntas 9 e 10 que por sua vez está relacionada as ações de autoproteção em situações de risco ou de invasão.



Fonte: Autor.

Na Figura 7, pode-se observar que 28,6% dos entrevistados relatam que, ao se depararem com um invasor armado, priorizam a proteção e a avaliação da situação. Por outro lado, 14,3% abordam o invasor e tentam desencorajá-lo, enquanto comunicam o restante da equipe de segurança, realizando a abordagem apenas quando há vantagem numérica ou de equipamento. Além disso, 33,3% acionam a polícia ao se depararem com um invasor, seja por meio de imagens de câmeras ou durante as rondas. Finalmente, 23,8% optam por observar de longe, evitando locais escuros ou áreas onde um invasor possa estar escondido, e comunicam a equipe de segurança ou a polícia.

Concluída a etapa da pesquisa, pode-se afirmar que o maior risco associado à profissão é o risco de vida. Apesar das precauções e do uso de tecnologias de monitoramento, os vigilantes frequentemente enfrentam a falta de recursos adequados para enfrentar invasores, tornando-os alvos vulneráveis a crimes. Essa vulnerabilidade é ainda mais acentuada em áreas com presença policial limitada ou inexistente, colocando os profissionais de segurança em uma situação mais precária. Assim, é essencial implementar medidas adicionais de segurança e apoio para proteger a vida dos vigilantes e assegurar um ambiente de trabalho mais seguro.

#### 4.4 Etapa 4: Construção de protótipo

Na Etapa 4, após a validação do problema, iniciaremos a construção de um protótipo para abordar as questões identificadas. Este protótipo foi projetado para atender às necessidades específicas da equipe de segurança do IFCE durante suas rondas. Além de garantir a segurança dos guardas, o protótipo permitirá o monitoramento em tempo real de áreas de baixa visibilidade, oferecendo uma visão abrangente e detalhada do ambiente.



Para alcançar esses objetivos, o protótipo incluirá uma câmera com visão noturna e será desenvolvido com foco na usabilidade e simplicidade de operação. Assim, a equipe de segurança poderá utilizar o equipamento sem necessidade de treinamento extensivo. O sistema contará com um design intuitivo e funcional, facilitando a visualização das filmagens da câmera.

#### **4.5 Etapa 5: Teste**

A fase final do projeto envolverá a realização de voos de teste para identificação no Campus do IFCE Aracati, também será feito um teste com o drone voando em orbital de uma pessoa para avaliar o desempenho identificando uma única pessoa. Durante esses testes, serão avaliadas as imagens capturadas para verificar o desempenho do protótipo.

Os critérios de avaliação incluem a precisão na identificação de pessoas em áreas abertas do campus, tanto durante o dia quanto à noite, e a capacidade de detectar múltiplas pessoas simultaneamente. Esta etapa será fundamental para validar a eficácia e a robustez do sistema desenvolvido.

### **5 PROPOSTA DE SOLUÇÃO**

Nesta seção, serão abordados diversos aspectos da proposta de solução, incluindo a construção do drone, o modelo utilizado para identificação de objetos e o desenvolvimento da interface e suas funcionalidades. Também serão discutidos os resultados das pesquisas realizadas com profissionais de segurança.

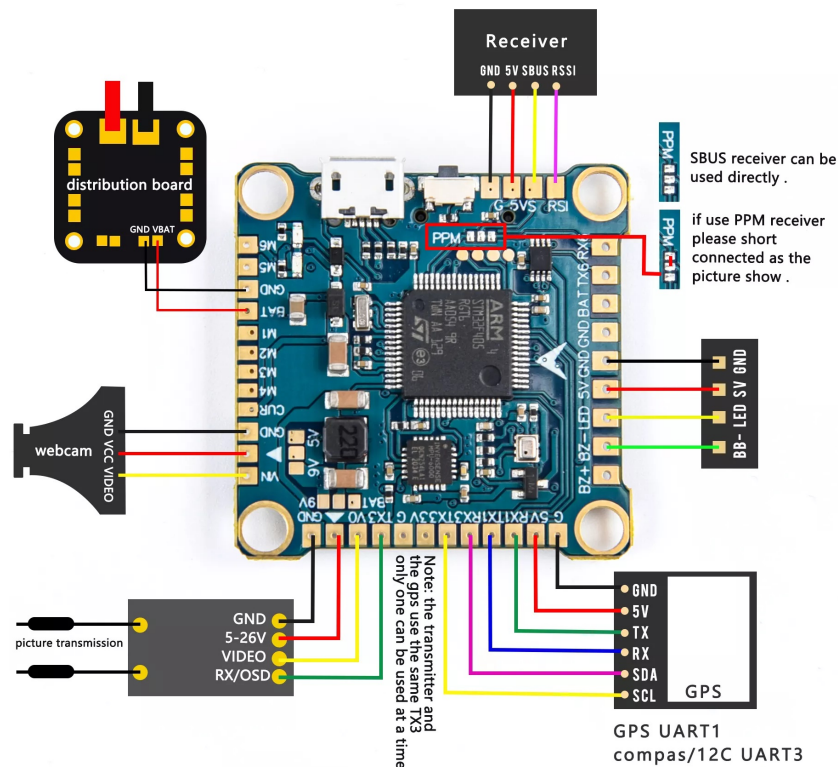
#### **5.1 Construção do drone**

A construção do drone se baseou em projetos já existentes feito pelo Fabiano Regra no canal do youtube chamado “mundo drone”, onde a autonomia com a bateria cotada no projeto era de 30 minutos no máximo. Para este trabalho foi utilizado uma bateria com 1100mAh a mais para maximizar o tempo de voo.

Na Figura 8, é apresentado o diagrama de montagem eletrônica usado no drone. A figura retrata de forma gráfica a controladora e os outros componentes eletrônicos que compõem o restante do circuito. Existem muitas marcas de rádio, e cada uma delas conta com um protocolo de comunicação diferente entre a controladora e o receptor. Ainda na Figura 7, é mostrado como deve ser a ligação para protocolos como PPM, SBUS e ELRS. Para este trabalho, utiliza-se o PPM, pois é o protocolo utilizado pela Flysky.

Nos drones FPV, a câmera possui uma posição fixa, não permitindo o uso de um *gimbal* para movimentação. Por isso, foi definida uma inclinação de 45 graus na vertical para a câmera, com uma resolução de 1000 TVL, equivalente a mil linhas de TV. Além disso, o campo de visão abrange uma angulação de 120 graus.

Figura 8 – Ligação dos fios entre a controladora e os demais periféricos eletrônicos do drone.



Fonte: Autor.

Quadro 2 – Tabela de valores para construção

Componentes	Referência	Valor R\$
Frame	Mark 4 v2 10"	137,00
Controladora	Omnibus f4 v3s plus	122,00
ESC	4 in 1 45A mak4	155,00
Motor	Racestar 920KV 2212	98,00
Hélices	1045R	40,00
Receptor de vídeo	Eachine rotg01	60,00
Transmissor de vídeo	Eachine ts805	70,00
Câmera	Eachine 1000 tvl ccd	30,00
Bateria	HRB 3300mAh 3s 60c	120,00
Rádio	FlySky FS-i6	300,00
GPS	BZ-181	42,00
Total		1.174,00

Fonte: Autor.

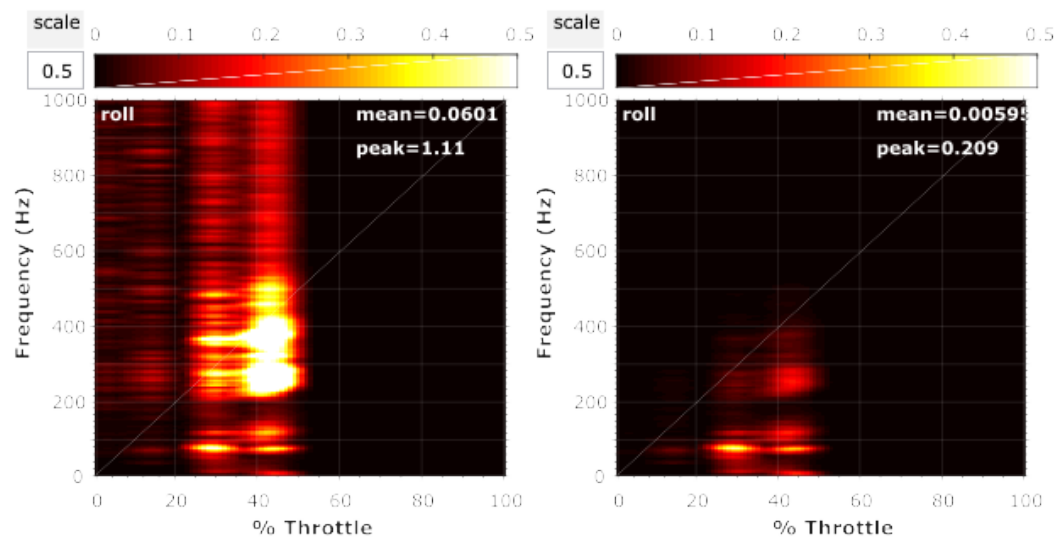
O Quadro 2 apresenta os valores de cada peça que compõe o drone; não foram considerados outros periféricos, como carregador e pilha para o rádio. Os valores podem variar ao longo do tempo e não foram incluídos os custos de frete, pois nenhuma peça tinha custo de frete. Todos os componentes foram adquiridos pela plataforma AliExpress.

## 5.2 Configuração do drone

O processo de configuração do drone gera dados apresentados nas Figuras 9 e 10, que representam a frequência de ruídos capturados pela controladora do drone após a aplicação dos filtros de Gyro e D-term.

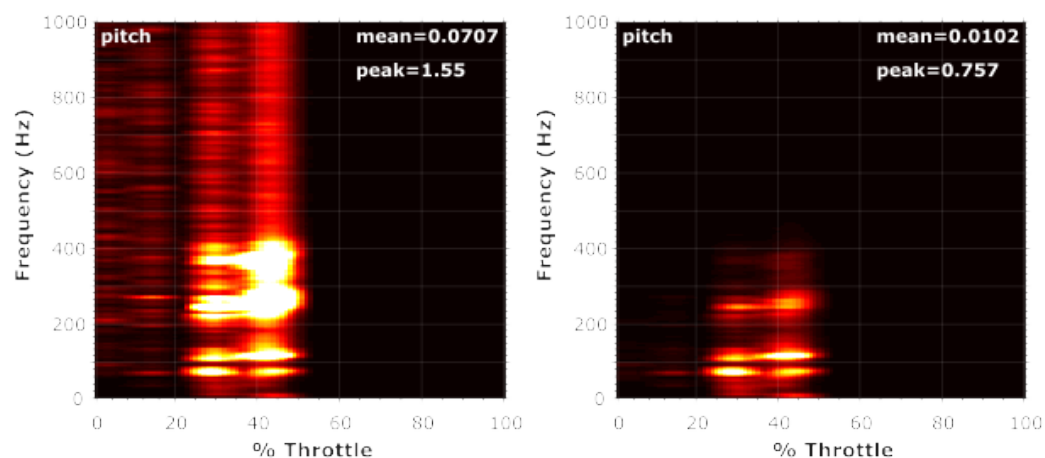
As Figura 9 e 10, apresentam os ruídos gerados pelo D-term. Esses ruídos ocorrem porque, quando o valor do D não é proporcional ao P, o drone ultrapassa o ponto de parada e tenta corrigir sua posição, resultando em vibrações e geração desses ruídos. É possível observar ligeiras oscilações entre 100 Hz e 200 Hz quando o throttle está entre 20% e 50%. Oscilações abaixo de 100 Hz são desconsideradas, pois são causadas por comandos do rádio.

Figura 9 – Ruídos antes e depois de ser aplicado os filtros do D-term no eixo roll.



Fonte: Autor.

Figura 10 – Ruídos antes e depois de ser aplicados os filtros do D-term no eixo pitch.

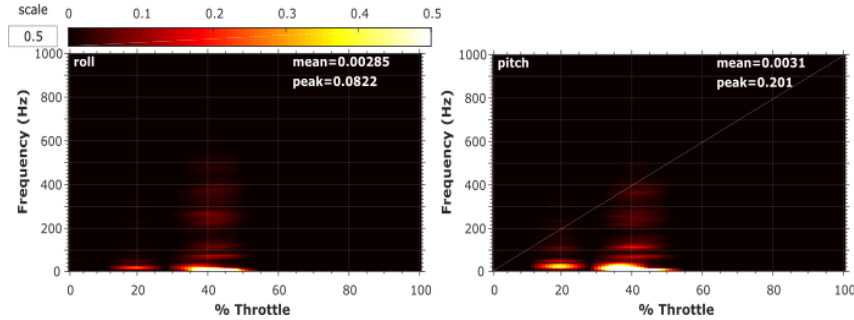


Fonte: Autor.

A Figura 11, o gráfico de calor demonstra os ruídos capturados pelo giroscópio da controladora, mostrando a relação entre as frequências de oscilação e a aceleração dos motores.

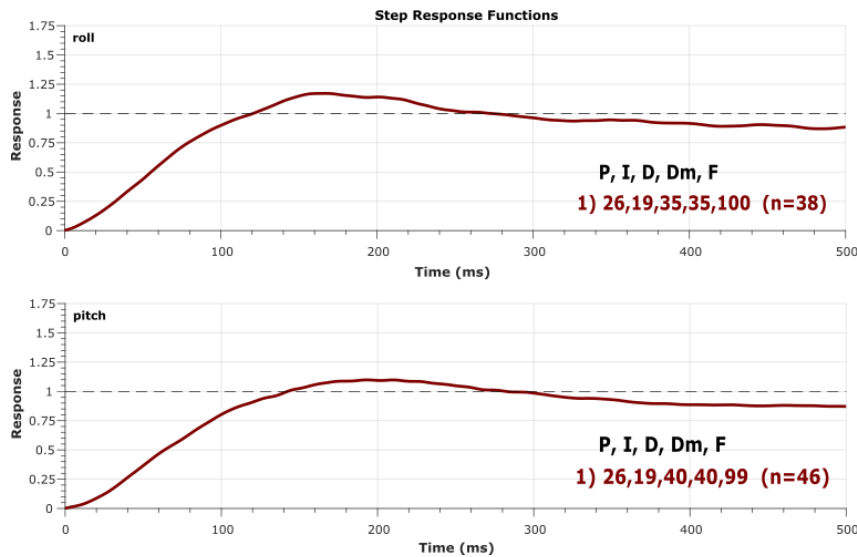
Esses ruídos são gerados por vibrações causadas pelas hélices, motores e o *frame*. Assim como na Figura 6, as oscilações abaixo de 100 Hz podem ser ignoradas, pois são causadas por comandos do rádio.

Figura 11 – Ruídos depois de serem aplicados os filtros de gyro.



Fonte: Autor.

Figura 12 – Gráfico de balanço de PID.



Fonte: Autor.

A Figura 12 exibe o gráfico de balanço do PID. De acordo com a documentação do PidToolBox, a linha vermelha do gráfico deve seguir a linha pontilhada para indicar que o processo de configuração foi bem-sucedido. Embora tenha ocorrido uma leve elevação acima da linha pontilhada, tanto no eixo de roll quanto no de pitch, os voos de teste foram bastante satisfatórios, sem apresentar instabilidade ou imprecisão.

### 5.3 Algoritmo de identificação

Para a criação do *dataset*, foi necessário utilizar uma ferramenta de anotação. A ferramenta escolhida para o trabalho foi o Roboflow. No total, foram coletadas 8.426 imagens para treinamento, 1.924 para validação e 1.972 para teste.

Várias técnicas foram aplicadas para aumentar a quantidade de imagens, como rotação de 15 graus para a direita e para a esquerda, adição de filtro preto e branco, inclusão de imagens

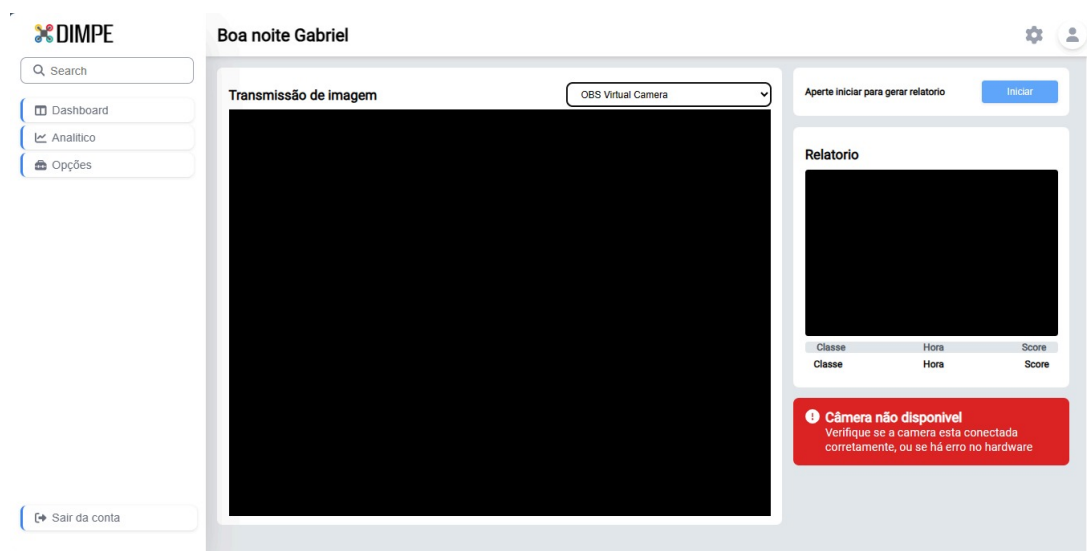
sem nenhuma classe e recortes de outras imagens do *dataset*. Muitas imagens eram bastante similares em locais e horários semelhantes; portanto, para melhorar a inferência do modelo, foi essencial empregar essas técnicas. Além disso, os testes incluíram situações em que o modelo deveria identificar objetos à noite, com imagens em preto e branco, o que tornou necessário adicionar o filtro preto e branco para simular o efeito de modo noturno.

Após a conversão, foram gerados alguns arquivos .bin com os pesos e um arquivo em formato .json com a arquitetura, que pode ser lido pelo TensorFlow.js. Todo o processo descrito nesta seção está disponível no GitHub.<sup>4</sup>

#### 5.4 Sistema de identificação

Desenvolvemos um sistema web que pode ser executado em qualquer dispositivo por meio do navegador. Os testes foram realizados em um notebook com processador Intel i3-7020U, 8 GB de RAM e vídeo integrado com 128 MB de VRAM, o que estabeleceu esses como os requisitos computacionais mínimos. O sistema foi projetado para ser intuitivo e simples, sem exigir conhecimentos de programação do usuário para a execução do algoritmo. Ele possui três telas principais, conforme ilustrado nas Figuras 13, 14 e 15: a primeira exibe o modelo em execução em tempo real, a segunda apresenta uma lista de relatórios, e a terceira fornece detalhes dos relatórios.

Figura 13 – Tela onde o modelo analisa a imagem em tempo real.

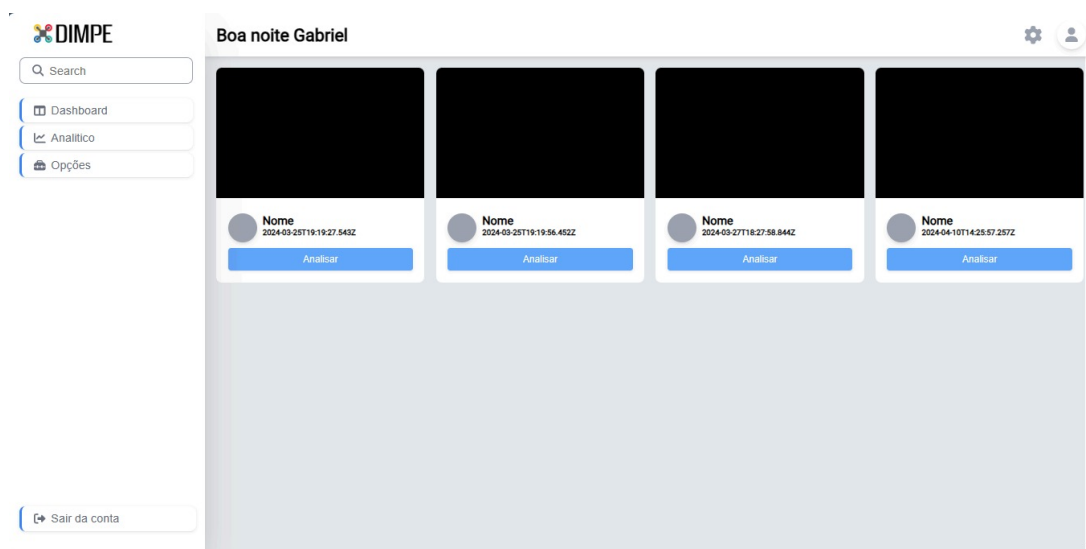


Fonte: Autor.

A Figura 13 exibe a tela onde o modelo processa as imagens em tempo real. Após conectar o receptor de imagem do drone ao computador, ele será reconhecido como uma opção de câmera na aba de transmissão de imagem. Em seguida, basta pressionar o botão de iniciar, e as imagens nas quais o modelo identificar um objeto serão enviadas para o servidor.

<sup>4</sup> <https://github.com/gabrieldev6/tensorflow-para-tensorflow.js>.

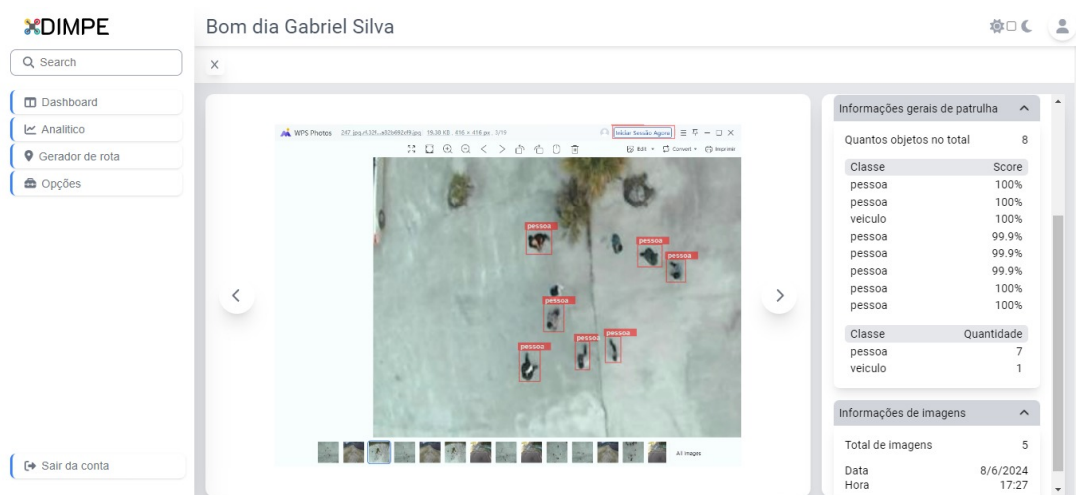
Figura 14 – Lista de relatórios.



Fonte: Autor.

A Figura 14 apresenta uma lista dos momentos em que novas detecções foram registradas. Cada entrada inclui uma prévia da detecção, o nome do usuário e informações sobre a data e a hora da criação. Essas informações são úteis para identificar quem estava manuseando o equipamento no momento da detecção e o horário exato. Em casos de invasão, esses dados são valiosos para a elaboração do boletim de ocorrência.

Figura 15 – Tela de listagem de relatórios, o usuário poderá qual relatório quer .



Fonte: Autor.

A Figura 15 exibe todas as fotos capturadas durante a identificação, mostrando os *bounding boxes* na imagem e fornecendo informações detalhadas sobre cada detecção, como a quantidade de instâncias, a hora, a classe e a confiança. Além disso, as imagens podem ser baixadas para possível divulgação do evento de invasão ou furto.

O sistema inclui um recurso avançado de *web worker*, onde o modelo e os recursos visuais são processados em *threads* separadas. Isso reduz a sobrecarga de processamento em

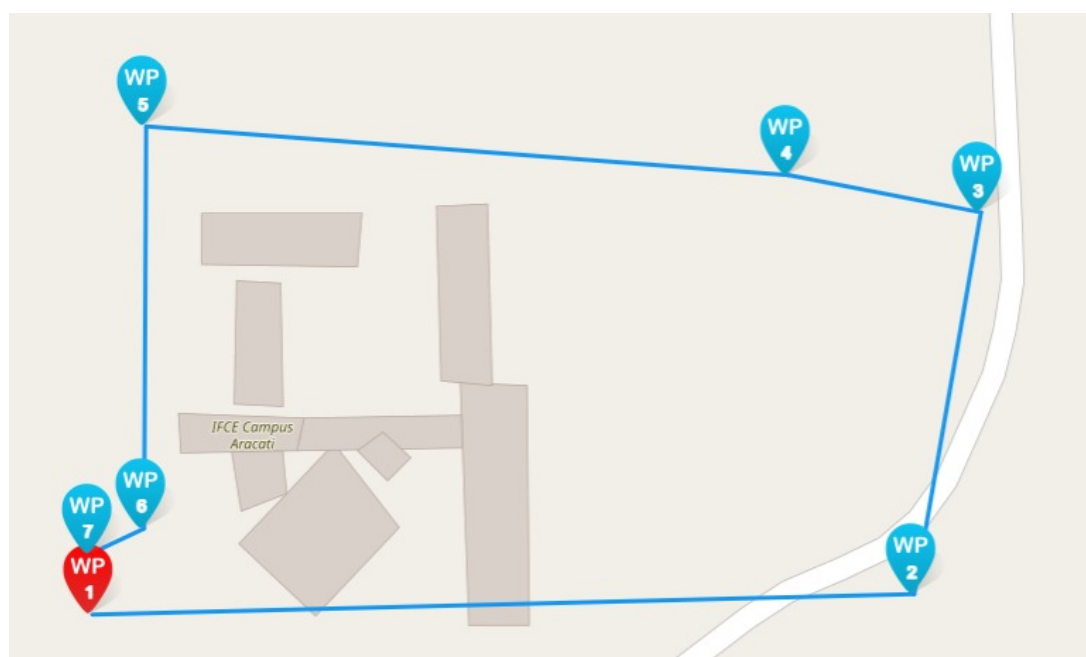
*desktops* com *hardware* mais limitado, garantindo um bom desempenho mesmo em máquinas menos potentes.

Na próxima seção, serão discutidos os resultados e a validação da solução apresentada. A acurácia do modelo em situações reais será detalhada conforme descrito na seção 7.1.

## 6 VALIDAÇÃO DA SOLUÇÃO

Para o início dos testes, foi criado um plano de voo no INAV que cobre a área acima dos blocos. A altura definida para o voo foi de 5 metros acima do nível do mar, pois a baixa resolução da transmissão de imagem do drone limita a capacidade do modelo de identificar uma pessoa a partir de altitudes maiores. A Figura 16 mostra a rota percorrida pelo drone. A região ao redor dos *waypoints* 2, 3 e 4 é a mais crítica, pois inclui tanques de larvicultura, uma quadra, muita vegetação e a presença de animais peçonhentos. Já nos *waypoints* 5, 6 e 7, estão localizados o estacionamento e os portões de entrada e saída.

Figura 16 – Plano de voo que o drone deve percorrer.

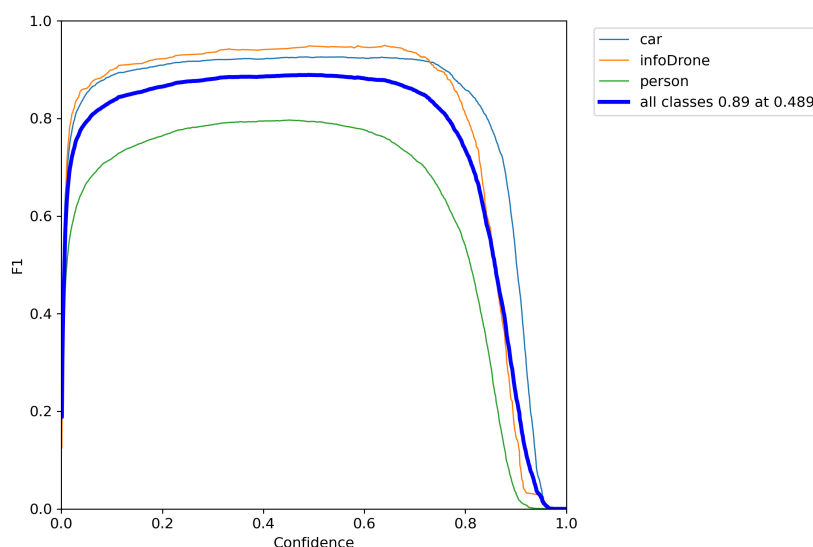


Fonte: Autor.

### 6.1 Acurácia do treinamento

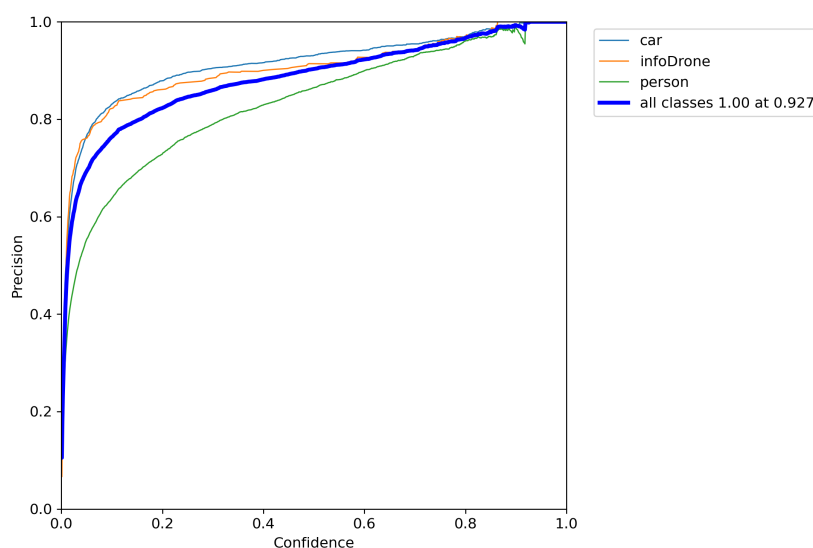
O treinamento foi conduzido ao longo de 250 épocas. A cada 10 épocas, os gráficos gerados eram avaliados para determinar se era necessário ajustar o *dataset* e melhorar a precisão na identificação de casos positivos. Durante o treinamento, observou-se que as informações relativas ao drone eram frequentemente incorretamente identificadas como pessoas. Para mitigar esses falsos positivos, foi criada uma nova classe chamada "infoDrone".

Figura 17 – Gráficos representando os resultado das métricas de F1-score.



No gráfico da Figura 17, observa-se um platô na faixa de confiança entre 10% e 70%, o que ocorre devido ao maior número de instâncias com confiança dentro desse intervalo. A quantidade de detecções com confiança superior a 70% diminui gradualmente até atingir 95%, ponto em que não há mais instâncias com confiança acima desse valor.

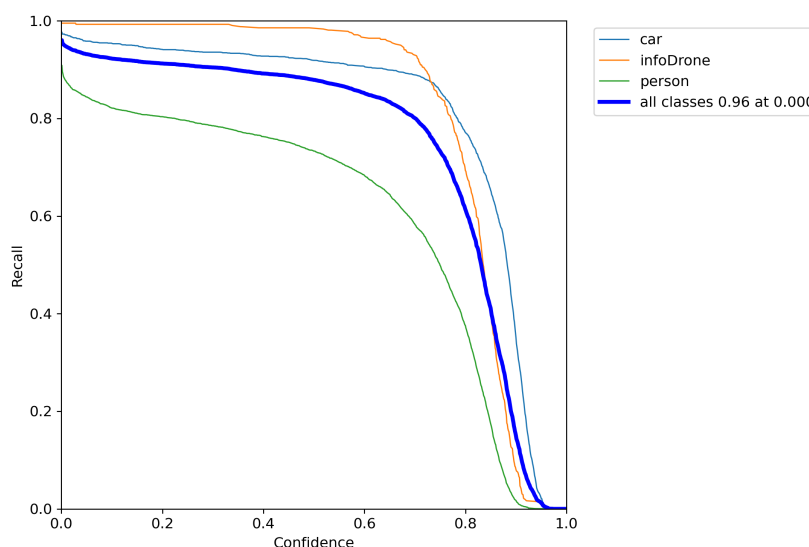
Figura 18 – Gráficos representando os resultado das métricas de precisão.



O gráfico da Figura 18 demonstra a precisão em função da confiança. É notável que, à medida que a confiança aumenta, o modelo se torna mais preciso. Mesmo com uma confiança de 20%, a média da precisão se mantém acima de 80% e continua a crescer com o aumento da confiança, indicando uma redução significativa nos falsos positivos em relação aos verdadeiros positivos.

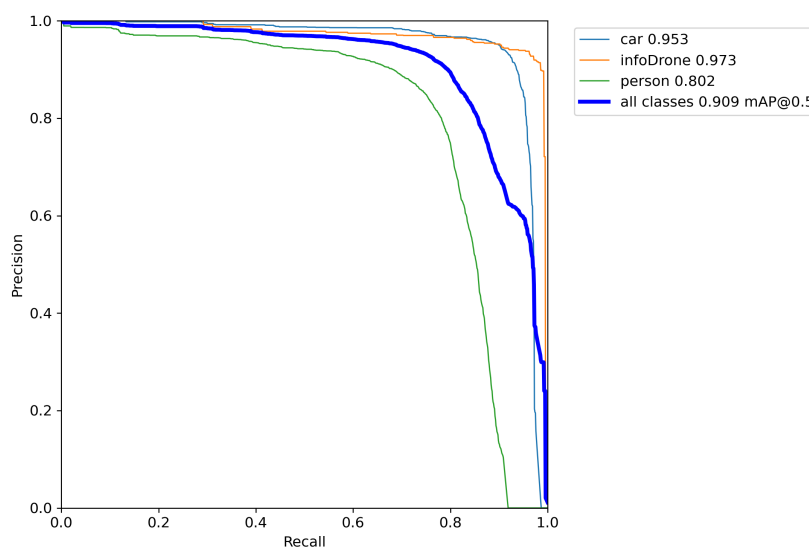


Figura 19 – Gráficos representando os resultado das métricas de recall.



No gráfico da Figura 19, são exibidos os valores de *recall* em função da confiança atribuída pelo modelo às classes. A curva azul escura representa a média entre todas as classes. O gráfico mostra que o valor de *recall* diminui abruptamente a partir de 75%, o que pode ser explicado pela escassez de instâncias identificadas como falsos negativos com confiança acima de 75%.

Figura 20 – Gráficos representando os resultado das métricas de mAP.



O gráfico da Figura 20 ilustra o mAP@0.5, uma métrica abrangente que avalia tanto a precisão quanto a localização das detecções em um modelo de detecção de objetos. O valor médio de mAP@0.5 foi de 90,9%. No entanto, a classe "pessoa" obteve um desempenho de 80,2%, significativamente inferior ao das outras classes. Isso se deve à grande quantidade e variedade de instâncias da classe "pessoa", o que dificultou a inferência do modelo durante a validação.

## 6.2 Resultado na identificação em campo

Os testes foram conduzidos variando a altitude entre 3 e 5 metros, tanto durante a noite quanto no final da tarde. Para avaliar o desempenho em campo, foi considerado o tempo desde o momento em que a altitude atingia 3 metros até o instante em que o modelo identificava o objeto corretamente. Falsos positivos não foram incluídos na análise. Foram realizados dois voos orbitais ao redor de uma pessoa.

À noite, em locais com iluminação intensa, a visão do drone foi prejudicada, tornando necessário o uso de LEDs infravermelhos para minimizar o efeito de superexposição quando o modo noturno estava ativado. O modelo encontrou dificuldades para identificar os objetos à noite devido à superexposição causada pelos refletores presentes no local.

Figura 21 – imagens representando os teste durante o dia e a noite respectivamente.



Fonte: Autor

Figura 22 – imagens representando os teste durante o dia e a noite respectivamente.



Fonte: Autor

Na Figura 21, o vídeo tem duração de 1 minuto. A partir de 3 metros, a pessoa aparece por 10 segundos. O tempo de identificação é de 6 segundos, e durante esse período, os valores de confiança variam entre 12% e 76%. A Figura 22 representa o vídeo feito à noite, com duração de 48 segundos. A partir de 3 metros, a pessoa aparece por 10 segundos, mas em nenhum momento o modelo conseguiu identificar a pessoa na imagem.

Não foi possível realizar testes em campo para avaliar a capacidade do modelo em identificar várias pessoas simultaneamente, devido à falta de voluntários dispostos a participar. No entanto, para essa fase de teste foram utilizadas imagens do *dataset* pertencentes ao conjunto de teste que possuía as características necessárias para avaliar as identificações simultâneas. Na Figura 24, é perceptível que o modelo identificou erroneamente uma planta como uma pessoa, indicando que, mesmo em condições de boa iluminação, ainda pode haver casos de falsos positivos. Por outro lado, na Figura 23, o modelo apresentou um bom desempenho, identificando corretamente todas as pessoas.

Figura 23 – Imagens do conjunto de teste.



Fonte: Autor

Figura 24 – Imagens do conjunto de teste.



Fonte: Autor

Na seção seguinte serão discutidos os desafios enfrentados para construção do protótipo

desde a construção do drone até ao desenvolvimento do sistema que foi desenvolvido para web, esse fato tornou limitado a disponibilidade de ferramentas para construção do algoritmo.

## 7 DESAFIOS ENFRENTADOS

Um dos grandes desafios iniciais foi encontrar informações relevantes relacionadas à construção, montagem, configuração e manejo de drones. Muitas informações estão descentralizadas e, em grande parte, disponíveis apenas em fóruns desatualizados ou em canais estrangeiros no YouTube dedicados à montagem e *reviews* de drones. Dúvidas específicas sobre dimensionamento, escolha de componentes e montagem foram resolvidas com a ajuda de uma comunidade criada por um canal brasileiro chamado "Mundo Drone", onde várias pessoas com experiência no assunto se reuniram e contribuíram para a construção do equipamento.

A busca por um *dataset* dedicado a essa finalidade foi bastante desafiadora, uma vez que a altitude, a posição da câmera e a qualidade da imagem influenciam significativamente os resultados do modelo. Outra condição relevante, mas ausente no *dataset* encontrado, foi a presença de imagens noturnas. Para mitigar essa limitação, foram adicionadas imagens com filtro preto e branco, na tentativa de simular condições noturnas e aproximar o modelo da realidade o máximo possível. A escolha das classes para o *dataset* partiu da necessidade de identificar invasores ou veículos suspeitos, outras classes como cães ou gatos não foi possível encontrar imagens que pudessem ser usadas para o contexto desse trabalho.

## 8 LIMITAÇÕES E TRABALHOS FUTUROS

Como trabalho futuro, propõe-se a aplicação da mesma solução em outros contextos, como o monitoramento de plantações e pastagens de gado. Além disso, há a possibilidade de otimizar o processo de identificação em tempo real, reduzindo travamentos e atrasos que podem ocorrer durante a detecção. A implementação de uma câmera com maior resolução é essencial para diminuir o número de identificações incorretas, aprimorando a precisão e a confiabilidade do sistema.

## 9 CONSIDERAÇÕES FINAIS

As aplicações de visão computacional agregado ao uso de drones têm mostrado grande potencial na área de segurança patrimonial. Os testes realizados em diferentes condições de luminosidade e altitude revelaram tanto as capacidades quanto as limitações do sistema. Apesar dos desafios enfrentados, como a superexposição causada por fontes de luz intensa durante a noite, as adaptações realizadas, como a adição de LEDs infravermelhos, demonstraram ser eficazes em melhorar a visibilidade e a precisão da detecção de objetos. Esses resultados indicam que, com ajustes e aprimoramentos contínuos, a tecnologia pode se tornar uma ferramenta essencial para monitoramento e proteção de propriedades, proporcionando uma vigilância mais eficiente e abrangente.

A solução foi projetada para mitigar a necessidade de treinamento no uso de drones, embora ainda seja necessário um conhecimento básico para criar rotas no *mission control* e operar o sistema que recebe e classifica as imagens. Entre as capacidades da solução, a identificação durante o dia é bastante consistente, tornando o projeto adequado para uso em ambientes externos durante o período diurno.

Além disso, o uso de drones equipados com visão computacional pode revolucionar os protocolos de segurança ao permitir uma cobertura mais ampla e detalhada de grandes áreas, o que seria inviável com métodos tradicionais. A flexibilidade e a capacidade de resposta rápida dos drones permitem uma vigilância constante e em tempo real, aumentando significativamente a eficácia na prevenção de incidentes e na resposta a possíveis ameaças. O desempenho razoável observado nos cenários testados sugere que, com investimentos adicionais em pesquisa e desenvolvimento, essa tecnologia pode superar suas limitações atuais e oferecer soluções robustas para a segurança patrimonial.

## REFERÊNCIAS

- AHMED, F. Recent advances in unmanned aerial vehicles: a review. **Arabian Journal for Science and Engineering**, v. 47, p. 7963–7984, 2022. <https://doi.org/10.1007/s13369-022-06738-0>.
- CINNAMON, I.; TEPPER, F.; KADRI, R. S. **DIY Drones for the Evil Genius: Design, Build, and Customize Your Own Drones**. [S.l.]: McGraw-Hill Education, 20216. ISBN 9781259861468.
- CORTURATO, R. T. Sky mapping: sistema baseado em drone para vigilância patrimonial. **VII Simpósio de Tecnologia da Fatec Jales – SITEF**, n. 171, 2023. Disponível em: <<https://ric.cps.sp.gov.br/handle/123456789/16588>>.
- COSTA, R. D. Análise da atuação dos drones na segurança de um país. **dronethusiast**, 2019. Disponível em: <http://hdl.handle.net/10362/91298>.
- CUNHA, W.; CAMARGO, V. Uma investigação da aplicação de aprendizado de máquina para detecção de smells arquiteturas. In: . [S.l.: s.n.], 2019. p. 78–85.
- FORSYTH, D. A.; PONCE, J. **Computer Vision: A Modern Approach (2nd ed.)**. [S.l.]: prentice hall professional technical reference, 2012.
- GHAMARI, M. Unmanned aerial vehicle communications for civil applications: a review. **IEEE access**, v. 10, p. 102492–10253, 2022. 10.1109/ACCESS.2022.3208571.
- GROUP, I. F. W. **A Complete Guide to Setting Up INAV 3.0**. 2021. Acesso em: 11 set. 2024. Disponível em: <<https://inavfixedwinggroup.com/guides/getting-started/a-complete-guide-to-setting-up-inav-3-0/>>.
- INAVFLIGHT. **INAV Wiki**. 2021. Acesso em: 11 set. 2024. Disponível em: <<https://github.com/iNavFlight/inav/wiki>>.
- JORGE, H. V. N. Aeronaves remotamente pilotadas (drones) e enfrentamento da criminalidade no brasil. **Revista Eletrônica Direito TI**, v. 1, n. 9, p. 5–5, 2018. Disponível em: <https://direitoeti.com.br/direitoeti/article/view/107>.

KUMAR, A. K. K. **Improving Train Track Safety using Drones, Computer Vision and Machine Learning**. 2020.

LIANG, O. **What is PID and How to Tune it**. 2023. Acesso em: 11 set. 2024. Disponível em: <<https://oscarliang.com/pid/>>.

LINHARES, F. Drones começam a ser usados pela polícia militar em operações no es. **G1**, 2018. Disponível em: <https://g1.globo.com/es/espírito-santo/noticia/drones-comecam-a-ser-usados-pela-polícia-militar-em-operacoes-no-es.ghtml>.

MARTINEZ, K. The history of drones: A comprehensive timeline. **dronethusiast**, 2018. Disponível em: <http://www.dronethusiast.com/history-of-drones/>. Acesso em: 10 Nov. 2023.

MICROSOFT. **Modelos do ONNX: otimizar a inferência - Azure Machine Learning**. 2024. Acesso em: 11 set. 2024. Disponível em: <<https://learn.microsoft.com/pt-br/azure/machine-learning/concept-onnx?view=azureml-api-2>>.

MUNAWAR, H. S. et al. Inspecting buildings using drones and computer vision: A machine learning approach to detect cracks and damages. **Drones**, v. 6, n. 1, 2022. ISSN 2504-446X. Disponível em: <<https://www.mdpi.com/2504-446X/6/1/5>>.

NAYEEM, M. J.; RANA, S.; ISLAM, M. R. Prediction of heart disease using machine learning algorithms. **European Journal of Artificial Intelligence and Machine Learning**, 2022. Disponível em: <<https://api.semanticscholar.org/CorpusID:254344012>>.

OLIVO, R. Y. Uma abordagem neural na identificação de objetos em imagens para auxílio na manutenção de rede elétrica. **Porto Alegre: Sociedade Brasileira de Computação.**, n. 33, p. 179–182, 2020. DOI: <https://doi.org/10.5753/sibgrapi.est.2020.13006>.

PÚBLICA, S. Anuario brasileiro de segurança publica. **São Paulo: Forum Brasileiro de Segurança Pública**, p. 50–57, 2023. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-02-as-mortes-de-policiais-em-2022.pdf?data=160124>.

REDMON, J. et al. **You Only Look Once: Unified, Real-Time Object Detection**. 2016.

SANTOS, C. Voando alto: registro de drones cresce 11,3%. **Estado de Minas.**, 2022. Disponível em: [https://www.em.com.br/app/noticia/economia/2022/02/21/internas\\_economia,1346547/voando-alto-registro-de-drones-cresce-11-3-no-brasil-e-18-8-em-minas.shtml](https://www.em.com.br/app/noticia/economia/2022/02/21/internas_economia,1346547/voando-alto-registro-de-drones-cresce-11-3-no-brasil-e-18-8-em-minas.shtml).

SANTOS, R.; BEKO, M.; LEITHARDT, V. Modelo de machine learning em tempo real para agricultura de precisão. In: . [S.l.: s.n.], 2022. p. 69–70.

SOLAWETZ, J. N. J. **How to Train YOLOv5 on a Custom Dataset**. 2020. Acesso em: 11 set. 2024. Disponível em: <<https://blog.roboflow.com/how-to-train-yolov5-on-a-custom-dataset/>>.

SZELISKI, R. **Computer Vision: Algorithms and Applications 2nd Edition**. [S.l.]: Springer Science Business Media, 2021. ISBN 978-1-84882-934-3.

WANG, C.-Y.; BOCHKOVSKIY, A.; LIAO, H.-Y. M. **YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors**. 2022.