International Journal of Digital Crime and Forensics
Volume 16 • Issue 1 • January-December 2024

Dangerous Objects Detection Using Deep Learning and First Responder Drone

Zeyad AlJundi
https://orcid.org/0009-0009-5158-4249
Naif Arab University for Security Sciences, Saudi Arabia

Saad Alsubaie
Naif Arab University for Security Sciences, Saudi Arabia

Muhammad H. Faheem
https://orcid.org/0000-0002-1643-6728
Naif Arab University for Security Sciences, Saudi Arabia

Raha Mosleh Almarashi
Naif Arab University for Security Sciences, Saudi Arabia

Emad-ul-Haq Qazi
https://orcid.org/0000-0003-1448-3632
Naif Arab University for Security Sciences, Saudi Arabia

Jong Hyuk Kim
https://orcid.org/0000-0003-4505-1103
Naif Arab University for Security Science, Saudi Arabia

ABSTRACT

Detecting dangerous objects, such as firearms or knives, is crucial for public safety or accurate situational assessment in crime scenes in law enforcement applications. Drones as first responders have been actively utilized for this purpose, showing significant benefits in law enforcement with fast and early detection of such objects. However, automated detection is still challenging, particularly with low-quality drone cameras that operate in low illumination conditions. We evaluate the performance of four popular AI deep learning models to automate the detection of dangerous objects recorded from low-quality drone cameras. The results show that the YOLOv5s model achieves the best detection performance, yielding mAP50 results of 0.964 for color and 0.949 for infrared videos, which are excellent performances considering the low-quality and low-resolution dataset. The trained network model is further implemented as an online web application where law enforcement officers can upload videos taken from drones or CCTV.

KEYWORDS

Drone as a First Responder (DFR), Dangerous Object Detection, Deep Learning, Security and Law Enforcement

INTRODUCTION

Drone as a first responder (DFR) has emerged as a new technological tool in security and law enforcement, in which drones are deployed to respond to an emergency call in police departments, arriving at the scenes before the ground officers while streaming live footage to the officers en route. This system enables the ground responders to prepare for what they might encounter at the scene, such as the presence of firearms. For example, the Chula Vista Police Department in the United States has adopted this technology since 2018, deploying DFR from the rooftop for over 20 thousand emergency calls, arriving at the scene within 93 seconds on average while assisting in arrests of over 28 thousand suspects (Chula Vista Police Department, 2024). Since deploying drones is typically less expensive than ground patrols or helicopters, police can allocate resources more effectively for their budgets. Although DFRs are still in their infancy, they can be utilized for crime scene investigation, disaster response, critical infrastructure protection, crowd safety, and so on.

DOI: 10.4018/IJDCF.367034

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creative-commons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Processing videos captured from the drone is also crucial for accurate situational assessment and decision-making in law enforcement. Most security systems have relied on camera operators' bare-eye inspection of the videos. However, this kind of task is typically very tedious and dull, as it requires processing a large volume of live or recorded footage, thus reducing the work performance. In recent years, artificial intelligence (AI) technologies have made significant progress in understanding visual data, such as object detection and scene understanding (Soori et al., 2023; Zhu et al., 2021a). Therefore, integrating this AI capability into drones can significantly enhance the performance of security systems.

Fast and robust detection of dangerous objects, like firearms and knives, is critical in the DFR systems to support the decision-makers in taking the necessary security measures. Although many datasets and AI models are available for general object detection, firearm and dangerous object datasets collected from drones are very limited. For example, gun detection datasets (Delong et al., 2021) collected gun images from internet movie databases aiming for embedded applications. Closed-circuit television (CCTV) footage is also utilized for weapon detection (Hnoohom et al., 2021), in which various deep-learning modules are evaluated. VisDrone-DET2021 releases a dataset aiming at drone object detection (Delong et al., 2021), which contains videos collected from drones over various urban areas with vehicles and pedestrians and applies deep learning models.

These public datasets are helpful but need to reflect the realistic DFR scenarios in the context of law enforcement. DFRs are typically equipped with low-cost cameras and operate from a distance for public safety. In addition, other factors, such as low-light or night-time conditions, affect the detection performance. This study collects new datasets from a realistic DFR scenario under low-light conditions to fill these gaps and evaluate AI models for detecting dangerous objects. The key contributions of this work are:

- Collection of new dangerous objects dataset (firearms, knives) from a realistic DFR scenario.
- Evaluation of four different AI models ("You Only Look Once" version 8 [YOLOv8], small "You Only Look Once" version 5 [YOLOv5s], faster region-based convolutional neural network [Faster R-CNN], and a visual geometry group 19 layers deep [VGG19]).
- Development of an online application that can process uploaded videos to detect firearms and knives, aiming to support law enforcement agencies in the future in automating the evaluation of videos in security.

This is the first study on dangerous object detection from a DFR in the security field.

RELATED WORK

Lightweight convolutional neural network architecture for efficient aerial image classification on unmanned aerial vehicles (UAVs) is proposed by Kyrkou and Theocharides (2020), in which EmergencyNet allows the network to process multiresolution features without increasing the number of parameters. A "You Only Look Once" version 5 (YOLOv5)-based algorithm is also proposed by Zhang et al. (2023), which is tailored for small object detection in UAV images, with potential applications in tasks like traffic monitoring, search and rescue, and environmental surveillance. This algorithm enhances the original YOLOv5 architecture, incorporating a space-to-depth convolution module, various attention mechanisms, and an improved multiscale detection module. Sun et al. (2022) introduce a novel network UA-CMDet (University at Albany Detection and tracking), for detecting vehicles in aerial images by harnessing the capabilities of both RGB (red, green, and blue) and IR (infrared) cameras, leveraging uncertainty-aware learning to extract complementary insights from these two imaging modalities. TPH-YOLOv5 (transformer prediction head) is an enhanced version of the YOLOv5 object detection model introduced by Zhu et al. (2021b), which explicitly addresses two critical challenges: the variations in object scale and the presence of motion blur in

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/dangerous-objects-detection-using-deep-learning-and-first-responder-drone/367034

Related Content

Assurance of Network Communication Information Security Based on Cyber-Physical Fusion and Deep Learning
Shi Cheng, Yan Qu, Chuyue Wangand Jie Wan (2023). *International Journal of Digital Crime and Forensics (pp. 1-18).*
www.irma-international.org/article/assurance-of-network-communication-information-security-based-on-cyber-physical-fusion-and-deep-learning/332858

Mitigate DoS and DDoS Attack in Mobile Ad Hoc Networks
Antonis Michalas, Nikos Komninosand Neeli R. Prasad (2011). *International Journal of Digital Crime and Forensics (pp. 14-36).*
www.irma-international.org/article/mitigate-dos-ddos-attack-mobile/52776

Malevolent Node Detection Based on Network Parameters Mining in Wireless Sensor Networks
Sunitha R.and Chandrika J. (2021). *International Journal of Digital Crime and Forensics (pp. 130-144).*
www.irma-international.org/article/malevolent-node-detection-based-on-network-parameters-mining-in-wireless-sensor-networks/283131

The State-of-the-Art Technology of Currency Identification: A Comparative Study
Guangyu Wang, Xiaotian Wuand WeiQi Yan (2017). *International Journal of Digital Crime and Forensics (pp. 58-72).*
www.irma-international.org/article/the-state-of-the-art-technology-of-currency-identification/182465

Measuring Crime in and around Public Housing Using GIS
Harold R. Holzman, Robert A. Hyattand Tarl Roger Kudrick (2005). *Geographic Information Systems and Crime Analysis (pp. 311-329).*
www.irma-international.org/chapter/measuring-crime-around-public-housing/18831