Chapter 13 Real-World Security Applications Through Computer Vision

Asish Kumar Dalai https://orcid.org/0000-0003-0613-175X *VIT-AP University, India*

Hitesh Mohapatra

(D) https://orcid.org/0000-0001-8100-4860

School of Computer Engineering, Kalinga Institute of Industrial Technology (Deemed), Bhubaneswar, India

ABSTRACT

The model is trained on a diverse dataset that includes various scenarios of violent interactions, allowing it to perform consistently across different surveillance environments and adapt to changing conditions. The chapter details the training process, including the data augmentation techniques employed to improve the model's generalization. Additionally, the system incorporates behavioral analysis to minimize false positives, helping to differentiate between brief aggressive actions and normal behavior. Extensive testing using real-world surveillance footage demonstrates the system's accuracy in detecting and classifying violent events. Comparative analysis shows that the solution outperforms existing methods in terms of both precision and recall. The chapter also explores the practical implications of deploying such a system, including its scalability for large monitoring networks and its potential integration with existing security infrastructures.

DOI: 10.4018/979-8-3693-9405-2.ch013

Copyright © 2025, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

I. INTRODUCTION

In the field of computer vision, object detection and classification have emerged as essential tasks, with applications spanning from self-driving cars to security systems. One of the leading deep learning models in this area is the "You Only Look Once" (YOLO) framework, which has shown impressive results in real-time object detection (Redmon et al., 2015). The YOLO series, from its initial version to the latest YOLOv8, has continuously advanced object detection by optimizing network designs and enhancing backbone architectures. As these models progress, researchers are increasingly focused on improving their effectiveness, especially for small object detection-vital for tasks like autonomous driving. Recent studies have explored integrating YOLO architectures with other deep learning models to boost the detection of small vehicles (Mokayed et al., 2023). Moreover, investigations into the role of anchor box selection and loss function adjustments have further refined YOLO's vehicle detection performance (Sang et al., 2018). This paper provides an in-depth evaluation of the performance of various YOLO-based models for vehicle detection in traffic scenes, with a particular emphasis on the unique challenges within Bangladesh (Alamgir et al., 2022).

In an era where public safety and security are paramount, the development of advanced technologies for rapid identification and prevention of violent acts has become crucial. Surveillance systems play a pivotal role in this domain, and leveraging cutting-edge deep learning techniques has proven to significantly enhance the accuracy and efficiency of violence detection (Arun Akash et al., 2022). This research introduces an innovative approach utilizing the latest You Only Look Once (YOLO) version 7 architecture to improve human violence detection. The goal is to harness YOLO V7's real-time processing capabilities to swiftly analyse video feeds from security cameras. By extensively training the model on diverse datasets, it can accurately detect and classify instances of aggressive behaviour (Chidambaram & Chandrasekaran, 2023). The proposed method not only pushes the boundaries of violence detection technology but also holds practical applications for real-world surveillance, providing stronger public safety measures as the demand for robust security solutions grows. Ultimately, this study offers a novel and efficient strategy for detecting human violence in video surveillance, advancing both technological innovation and public safety through the scalable and adaptable nature of the system (Corovic et al., 2018).

22 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: <u>www.igi-</u> <u>global.com/chapter/real-world-security-applications-through-</u> <u>computer-vision/371345</u>

Related Content

Evidentiary Implications of Potential Security Weaknesses in Forensic Software

Chris K. Ridder (2009). International Journal of Digital Crime and Forensics (pp. 80-91).

www.irma-international.org/article/evidentiary-implications-potential-security-weaknesses/3910

Geometrically Invariant Image Watermarking Using Histogram Adjustment

Zhuoqian Liang, Bingwen Feng, Xuba Xu, Xiaotian Wuand Tao Yang (2018). International Journal of Digital Crime and Forensics (pp. 54-66). www.irma-international.org/article/geometrically-invariant-image-watermarking-using-histogramadjustment/193020

Secure Robust Hash Functions and Their Applications in Non-interactive Communications

Qiming Liand Sujoy Roy (2010). *International Journal of Digital Crime and Forensics* (pp. 51-62).

www.irma-international.org/article/secure-robust-hash-functions-their/47071

Application of Tracking Signals to Detect Time Series Pattern Changes in Crime Mapping Systems

Wilpen L. Gorrand Shannon A. McKay (2005). *Geographic Information Systems and Crime Analysis (pp. 171-182).*

www.irma-international.org/chapter/application-tracking-signals-detect-time/18823

Indirect Attribution in Cyberspace

Robert Laytonand Paul A. Watters (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance (pp. 246-262).* www.irma-international.org/chapter/indirect-attribution-in-cyberspace/115761