Chapter 9
Anomaly Detection in Behavioral Surveillance Using Deep Learning Techniques

Arun Agrawal
http://orcid.org/0000-0001-7233-6660
Institute of Technology and Management, Gwalior, India

Rashmi S. Bhaskar
BNMIT Bengaluru, India

Sanjay Badhe
D.Y. Patil International University, Akurdi, India

Suvarna Kisan Thakur
http://orcid.org/0009-0000-6720-2705
Dr. Babasaheb Ambedkar Technological University, India

Anika Bhandari
Chandigarh University, India

Kajal Jain
http://orcid.org/0009-0004-1440-3860
Maharishi Markandeshwar University, Mullana, India

Deepak Gupta
http://orcid.org/0000-0003-3929-1362
Institute of Technology and Management, Gwalior, India

ABSTRACT

This chapter explores techniques for detecting abnormal behavior in surveillance systems using deep learning. Modern surveillance relies on advanced models to identify suspicious activities crucial for safety and monitoring. The discussion traces the evolution from traditional rule-based methods to deep models such as convolutional and recurrent neural networks, autoencoders, and transformers. It highlights challenges in defining normality, managing temporal variations, handling large-

DOI: 10.4018/979-8-3373-4202-3.ch009

scale data, and ensuring privacy. The chapter examines temporal behavior models, including LSTM encoders, 3D CNNs, and attention-based architectures. Real-world applications in video surveillance, crowd monitoring, and human activity analysis are reviewed. Issues like data imbalance, real-time inference, model explainability, and ethics are discussed. Finally, performance metrics, evaluation protocols, and model comparisons are outlined to guide readers in designing effective anomaly detection frameworks for practical use.

INTRODUCTION

Overview of Behavioral Surveillance Systems

Behavioral surveillance systems are now an essential part of the contemporary security monitoring. They track human movement at airports, transportation centers, workplaces, hospitals, and even in the internet (Verma et al., 2022). Their main aim is to identify abnormal or hazardous conduct at initial stages so as to eliminate security breaches, accidents or any other forms of inauspicious occurrences. The common systems make use of the hardware that includes cameras, motion sensors, and wearable devices, and computer programs that can analyze extensive amounts of data. These systems in the physical space monitor movements, posture, gestures, and interactions of people. They use digital space to analyze patterns of online usage to identify anomaly like suspicious transactions or unusual logins. To access these systems, the improvements in computing strength, storage space and speed of data transmission now allow them to handle high-quality video, a quantity of sensors input, and past records in real-time (Dávila-Montero et al., 2021). These developments have made them useful in the fields of public safety, healthcare, industrial monitoring and in smart city developments.

Evolution of Anomaly Detection Approaches

The notion of anomaly detection is an old one. The first systems used rule-based methods when experts defined the static conditions on which to be able to identify unusual activity (Li et al., 2023). As an illustration, the initial video surveillance systems would trigger a warning signal when one entered a restricted zone or stayed in the same place too long. These systems were successful in simple situations but failed in the cases of changeable behavior or complex environments.

Subsequently, there came statistical and classical approaches to machine learning. Numbers Numerical patterns of behavior can be analyzed using such models as Gaussian mixture models, support vector machines, and clustering algorithms.

A Novel Distributed QoS Control Scheme for Multi-Homed Vehicular Networks