RADemics

Multi Scale Feature Extraction in Computer Vision Systems for Robust Digital Forensics in Cybersecurity

A. S. Nisha, T.Dhivya
ST. JOSEPH'S COLLEGE OF ENGINEERING, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY.

9. Multi Scale Feature Extraction in Computer Vision Systems for Robust Digital Forensics in Cybersecurity

1A. S. Nisha, Assistant Professor, Department of Artificial Intelligence and Data Science, St. Joseph's College of Engineering, Chennai, Tamil Nadu - 600043, India. as.nisha.cse@gmail.com

2T.Dhivya, Assistant Professor, Department of Artificial Intelligence and Data Science, Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu, India. tdhivya23@gmail.com

Abstract

This chapter explores the critical intersection of multi-scale feature extraction in computer vision systems and its application to robust digital forensics within cybersecurity. As cyber threats continue to evolve, digital forensics plays a pivotal role in identifying, analyzing, and mitigating cybercrimes. Leveraging advanced computer vision techniques, multi-scale feature extraction enhances the accuracy and efficiency of digital forensic investigations by capturing intricate patterns and details across varying data resolutions. The chapter examines emerging challenges, including the integration of Internet of Things (IoT) devices, the detection of synthetic media such as deepfakes, and the importance of maintaining data integrity throughout forensic processes. It also discusses the role of machine learning and AI in advancing forensic capabilities, as well as the ethical and legal considerations involved in the collection and analysis of digital evidence. The chapter serves as a comprehensive resource for researchers and practitioners addressing modern challenges in cybersecurity forensics.

Keywords:

Multi-scale feature extraction, computer vision, digital forensics, cybersecurity, IoT integration, deepfake detection.

Introduction

The landscape of cybersecurity has evolved significantly over the past few decades, with an increasing reliance on digital systems for personal, corporate, and governmental operations [1]. As the digital world grows, so do the threats it faces [2]. Cybercrimes have become more sophisticated, exploiting vulnerabilities in both software and hardware systems [3]. Digital forensics has emerged as a critical field in combating these threats, focusing on the identification, preservation, and analysis of digital evidence [4]. This discipline was crucial for law enforcement, private investigators, and cybersecurity professionals, as it helps uncover the origins and mechanisms of cyberattacks, aiding in both criminal prosecution and the development of stronger security protocols [5,6]. As cybercrimes diversify, traditional forensic methods are being supplemented with advanced technologies like multi-scale feature extraction in computer vision systems, which enhances the ability to analyze complex data and recognize intricate patterns across

various scales [7,8]. The use of these methods was becoming increasingly vital for ensuring the integrity and accuracy of forensic investigations [9].

In recent years, computer vision has emerged as a pivotal tool in digital forensics, particularly in the analysis of large volumes of visual data such as images, videos, and surveillance footage [10-12]. Computer vision techniques allow investigators to extract meaningful features from digital media thatotherwise be too complex or subtle for traditional analysis [13]. By employing multi-scale feature extraction, these systems can capture details across various resolutions and scales, providing a more comprehensive view of the evidence [14,15]. This approach enables forensic professionals to identify key visual elements that could be crucial in solving cybercrimes, such as faces, objects, or hidden patterns within digital files [16,17]. The continuous advancements in machine learning and AI have significantly improved the accuracy and efficiency of these systems, making them invaluable tools in modern digital forensic investigations [18,19]. The integration of computer vision techniques with digital forensics has already proven successful in a variety of domains, from fraud detection to analyzing cyber-attack footprints [20,21].

The integration of Internet of Things (IoT) devices into everyday life has introduced new challenges and opportunities in the field of digital forensics [22]. IoT devices, ranging from smart home systems to industrial sensors, collect vast amounts of data that can serve as valuable evidence in cybercrime investigations [23-25]. However, these devices also present unique challenges due to their diversity, security vulnerabilities, and the large volume of data they generate. In digital forensics, extracting and analyzing data from IoT devices requires advanced methodologies to handle diverse data formats, ensure data integrity, and overcome potential tampering. Multi-scale feature extraction techniques applied to data from IoT devices enable investigators to focus on both high-level patterns and fine-grained details, improving the ability to reconstruct events, detect anomalies, and trace the origins of cyberattacks. As the IoT ecosystem expands, developing more robust forensic tools and strategies be essential for handling the complexities of this growing network of connected devices and ensuring the effective use of IoT data in investigations.