Chapter 5
AI and ML Approaches in Adaptive Watermarking

Neha Yadav
https://orcid.org/0000-0002-7793-2063
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Mayank Singh
https://orcid.org/0000-0002-8393-3652
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Vipin Tyagi
https://orcid.org/0000-0003-4994-3686
Jaypee University of Engineering and Technology, Guna, India

ABSTRACT

Digital watermarking is a crucial method for addressing the threats of data piracy and illegal content distribution in cloud environments and copyright protection systems. This chapter looks at Artificial Intelligence (AI) and Machine Learning (ML) methods of adaptive watermarking, and we will pay close attention to how intelligent systems can make such watermarking solutions more robust, imperceptible, and payload-dense. In addition, this chapter will review the various neural network architectures, deep learning frameworks, reinforcement learning approaches, and hybrid AI system structures that can be utilised in watermarking applications, particularly in cloud computing settings. We will conduct a review of current state-of-the-art AI/ML methods and models for embedding and detecting watermarks. This review will provide a taxonomy of methods, compare these methods, and present case studies and experimental setups.

DOI: 10.4018/979-8-3373-3785-2.ch005

1 INTRODUCTION

1.1 Background and Motivation

As the growth of digital content creation and sharing has advanced rapidly, particularly with the rise of cloud platforms, copyright infringement and data misuse have similarly risen. Today, images, videos, and other forms of multimedia are being shared, stored, and accessed widely on distributed systems. With the relative ease of duplicating and sharing these types of multimedia in cloud environments, users are more susceptible to copyright infringement, piracy, unauthorised conveyance or interpretation, and loss of ownership identity. Digital watermarking, specifically, will be an essential technique in the development of copyright processing schemes designed to address copyright issues. Digital watermarking methodologies enable the embedding of copyright or ownership information directly into multimedia content, making it potentially undetectable by users while still being detectable for authentication, provenance, and forensic purposes. Most traditional watermarking approaches are practical in controlled environments (e.g., image or video data formats); however, their performance is often compromised in terms of robustness, adaptability, and perceptual quality when executed in dynamic and adversarial cloud environments. The rapid, even rampant, growth of digital content in tamper-free environments has resulted in immense and unique challenges for copyright protection processes and their enforcement mechanisms (Amrit & Singh, 2022). Traditional watermarking techniques may be paramount in protecting ownership strategies. Still, they are usually adversarial and fail to achieve optimal outcomes across multiple content types, variable network conditions, and attacks that typically occur in cloud systems. The emergence of AI and ML techniques marks a shift in watermarking technology, offering adaptive systems able to learn from patterns in data, predict practical embedding approaches, and dynamically adapt to changing conditions (Liu & Nematollahi, 2024). An adaptive AI/ML watermarking system will have unique and essential benefits over traditional methods. Adaptive systems will automatically optimise watermark strength based on content and predict and counteract potential attacks while still performing consistently across heterogeneous cloud environments. AI solutions can quickly process large amounts of multimedia content, making them attractive in instances of large-scale cloud applications where manual tuning of parameters is impractical (Dandooh, El-Fishawy, & Hemdan, 2025).

AI and ML make watermarking systems transformative. Previous embedding techniques are altered with adaptable learning, meaning embedding systems can respond to new content types, random attacks, and environmental variability. AI systems can make intelligent decisions related to the strength, location, and method of embedding. Intelligent adaptive watermarking maximises both security and trans-