


Chapter 6


Security Analysis: Attacks and Countermeasures in Watermarking Systems

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

In the rapidly evolving digital media landscape, watermarking technology has become a crucial component of comprehensive content protection strategies. Despite its potential, the security of watermarking systems remains a primary concern, primarily due to the increasing sophistication of attack methods designed to damage, erase, or manipulate a watermark detector. This chapter explores the security challenges associated with watermarking and the countermeasures available. For each potential attack, it discusses the impact, detection difficulty, and possible damage. Additionally, the chapter outlines defensive architectures and algorithms, including robust embedding techniques, adversarial training in watermarking systems, tampering localisation, and cryptographic reinforcement. It is illustrated with case studies, simulation research and results, diagrams, and a benchmarking framework to help readers understand how to design, evaluate, and secure watermarking against modern threats.

DOI: 10.4018/979-8-3373-3785-2.ch006

1. INTRODUCTION TO WATERMARKING SECURITY

Digital watermarking refers to the process of embedding inaudible information into media assets (such as audio, video, or image files) for their secure assertion, authenticity verification, and distribution monitoring, among other tasks. The primary objective of watermarking is to embed an imperceptible yet robust signal within digital assets. As the use of watermarking systems has increased across multimedia content distribution platforms, the security surrounding these signals is becoming increasingly tenuous. As watermarking systems become more valuable and visible, they become susceptible to threat model adversaries who may attempt to either change or remove the watermark without affecting the perceptual quality of the visible media (Madala et al., 2023). Watermarking security can be thought of as referring to the global question, “How secure is a watermarking system to unauthorised changes or removal?” To address this question, potential threats should be studied, system robustness should be evaluated under defined attack conditions, and countermeasures employed in the watermarking system design that defend against these security threats (Tauhid, Xu, Rahman, & Tomai, 2023). A secure watermarking system should ensure that the conduit watermark remains thorough and detectable despite being subjected to compression, geometric distortion, filtering, or malicious adversarial efforts.

1.1 Importance of Security in Modern Watermarking

As digital content is rapidly disseminated through cloud storage, streaming sites, and social media, the need for watermarking security is more crucial than ever. The attack vectors against watermarking systems include:

- Removing owner identifiers to make piracy easier
- Replacing a watermark with a fake watermark
- Altering watermark information to fool forensics or tracking
- Using adversarial methods to fool AI-based detectors

We observe that security threats evolve in tandem with advancements in watermarking algorithms, particularly those that utilise AI and ML. Therefore, we will require multi-layer and dynamic security.

1.2 Key Components of a Secure Watermarking System

A robust and secure watermarking system is built upon the following key components:

32 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/chapter/security-analysis/388659

Related Content

Performance Evaluation of Data Intensive Computing In the Cloud

Sanjay P. Ahuja and Bhagavathi Kaza (2014). *International Journal of Cloud Applications and Computing* (pp. 34-47).

www.irma-international.org/article/performance-evaluation-of-data-intensive-computing-in-the-cloud/113806

Multiple Perspective of Cloud Computing Adoption Determinants in Higher Education a Systematic Review

Mohammed Banu Ali (2019). *International Journal of Cloud Applications and Computing* (pp. 89-109).

www.irma-international.org/article/multiple-perspective-of-cloud-computing-adoption-determinants-in-higher-education-a-systematic-review/228918

Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment

Mouhib Ibtihal, El Ouadghiri Driss and Naanani Hassan (2017). *International Journal of Cloud Applications and Computing* (pp. 27-40).

www.irma-international.org/article/homomorphic-encryption-as-a-service-for-outsourced-images-in-mobile-cloud-computing-environment/179536

Integration of Cognitive Radio Sensor Networks and Cloud Computing: A Recent Trend

Yasir Saleem, Farrukh Salim and Mubashir Husain Rehmani (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1025-1048).

www.irma-international.org/chapter/integration-of-cognitive-radio-sensor-networks-and-cloud-computing/119895

Artificial Intelligence in Cyber Security

MohanaKrishnan M., A.V. Senthil Kumar, Veera Talukdar, Omar S. Saleh, Indrarini Dyah Irawati, Rohaya Latip and Gaganpreet Kaur (2023). *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT* (pp. 366-385).

www.irma-international.org/chapter/artificial-intelligence-in-cyber-security/325953