Chapter 7
Adaptive Watermarking Algorithms for Multi-User Cloud Environments

Birendra Kumar Saraswat
https://orcid.org/0000-0003-0628-6823
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Prakash Joshi
Raj Kumar Goel Institute of Technology, Ghaziabad, India

Ritika
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

Satya Prakash Yadav
https://orcid.org/0000-0002-2634-5600
Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur, U.P. , India

Harshit Munjal
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

ABSTRACT

Secure and robust ownership authentication of media content assets in large-scale multi-user (public/private) cloud environments is an important and challenging issue. Due to the fact that many cloud systems support the work of many individuals at the same time, the digital assets will be easily accessible, copied, and modified. The classical static-pattern-based traditional watermarking is sometimes insufficient to cope with dynamic threats and variant user demands. A for cloud data Adaptive watermarking algorithms use online data analysis, user behavior profiling, and

DOI: 10.4018/979-8-3373-3785-2.ch007

adaptable embedding techniques to dynamically adjust watermark parameters such as the strength, the embedding domain and the location according to different user profiles and usage patterns on the cloud. We leverage the technique of machine learning and context-aware policies for detecting watermark strength and adapting imperceptibility and robustness in order to achieve reinforcement against various attacks (e.g., collusion, forgery, and removal).

I. INTRODUCTION

In the age of ubiquitous cloud computing, data security and IP protection are growing concerns, especially in multi-user cloud settings where data is often shared, manipulated, and included by various parties (Jiang, Zhang, Dong, Jiang, & Di, 2024). A large amount of work has been done in this direction, and watermarking algorithms that are able to adapt themselves to the structure of the data have emerged as a potential solution for these refinements by embedding identifiers and robust identification marks throughout digital assets. These algorithms are based on sophisticated algorithms from the field of machine learning and signal processing such that they are able to adapt their watermarking parameters on the fly with regard to the properties of the host media signal and the context of the user interaction (Slocum et al., 2024). This flexibility makes the embedded watermark nearly invisible to users, thus keeping the original data quality and application value, and also robust to common attacks, including compression, cropping, and collusion, which are very common in the distributed and collaboration cloud. Adaptive Watermarking to Cloud: An Introduction In the last decade, we have seen the concept of multiple owners' data sharing stored over the cloud, but with the introduction of watermarking, this is indeed possible (Murala & Thammireddy, 2024). In a cloud-based scenario, ownership can be fractionalized among multiple users accessing different versions or collaboratively editing the same digital documents (or multimedia content) (Harini & Chakkaravarthy, 2024). Such vulnerabilities can be attacked using some static watermark techniques (with a global fixed watermark). It is widely admitted that such algorithms are not robust if one considers arbitrary collusion (subsets of pirates), which are not necessarily disjoint, see (Aljameel & Rahman, 2023). Most existing DWM has to be designed for very specific applications, whereas adaptive DWM can use adaptive watermarking techniques that can customize watermarking strength, location, and encoding strategy based on user privilege level, document confidentiality level, access frequency and use pattern. For instance, a document opened by a manager and an intern will have different stego-codes reflecting their positions, providing finer granularity for traceability and responsibility when security leaks happen, and data spreads beyond the supplementary channels. Artificial