Chapter 8
Blockchain-Enhanced Watermarking for Cloud-Based Content Authentication

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

Prem Chand Vashist
G.L. Bajaj Institute of Technology and Management, Greater Noida, India

ABSTRACT

In this chapter, the problem of content authentication in cloud computing is addressed, and a Blockchain-Enhanced Watermarking (BEW) system is proposed. With digital assets now stored in the cloud, access and sharing become even more challenging. With content no longer sitting on a server on your premises, how do you ensure that it has come from a trusted source and that it hasn't been altered? Conventional watermark methods safeguard ownership but have an insufficient ability to trace back, are impossible to prevent distortion, and lack an encryptable digital proof for the data in open networks. The BEW utilizes resilient digital watermarking techniques, along with permissioned blockchain, to maintain an indelible, decentralized record of watermark data.

DOI: 10.4018/979-8-3373-3785-2.ch008

I. INTRODUCTION

Blockchain-driven watermarking for Cloud-Based Content Authentication is an amalgamation of two cutting-edge technologies, blockchain and digital watermarking, for securing digital assets in the cloud (Raghu, Bhat, Nambiar, Shetty, & DB, 2025). We will inevitably see a significant shift towards cloud-based storage and distribution of documents, images, videos, and other digital assets. This shift will lead to growing risks of unwanted access to this data and attempts to impersonate another user and steal intellectual property. (Hou, Ou, Peng, & Long, 2024) As a fundamental recordable digital object, digital assets have played a crucial supporting role in various fields and have provided a solid foundation for watermarking, particularly in the fields of image and video watermarking. Traditional watermarking, which invisibly embeds identifying information into the host content, has been widely used as a tool for tracing ownership and verifying authenticity. However, it is not immune to easy tampering, removable attacks, or the necessity of establishing the time-stamped originality or legitimate ownership of a digital asset (Alshuraify, Yassin, Abduljabbar, & Nyangaresi, 2024). The blockchain), which is a decentralized and tamper-evident ledger technology, serves as a new layer of security and trust: any transaction (such as a piece of content creation, modification and redistribution) can be recorded transparently and be cryptographically protected in such a way that it is almost impossible to tamper with it. By including watermarking operations within the blockchain's structure, the watermark itself can be securely generated and registered, together with its associated metadata (e.g., ownership data, creation times, and distribution occurrences), which can be forever implicated (Bhat, 2025). When digital assets are accessed through the cloud or shared, the embedded watermark can be used to retrieve records on the blockchain, thus instantly authenticating, copyrighting, and even revealing the life story of the asset. This cooperation removes the necessity of trust in one single authority (centralized), thereby minimizing mono points of failure or wrongdoers in the cloud service structure (Vanmathi, Farouk, Alhammad, Bhattacharya, & Kasyapa, 2024). Imagine a photographer uploads a high-resolution original photo to a cloud platform: it will re-embed a cryptographically strong watermark and register the hash of the image, the signature of the watermark, the credentials of the locker, and the uploading time onto a blockchain ledger. Assume that such an image is then shared, transferred, or modified later (Nithyashree & Pawankumar, 2025). In this situation, any user or automatic process can check the current watermark and the image hash against the blockchain. In a few seconds, the system can automatically detect if the photo has been tampered with or not or if it has been misattributed or not. This strategy strengthens content verification and simplifies the enforcement of the law against illegal exploitation of copyright, as an immutable, time-stamped ledger is legally