Chapter 14
Dynamic Watermarking for Multi-Tenant SaaS Applications

Reshu Tyagi
https://orcid.org/0009-0001-4610-6834
ABES Institute of Technology, India

Swati Singh
https://orcid.org/0000-0002-0932-7363
IMS Engineering College, Ghaziabad, India

Arun Kumar Takuli
Graphic Era Hill University, Haldwani, India

Ahimsa Bhardwaj
IMS, Ghaziabad, India

ABSTRACT

Dynamic watermarking is a paramount tool for protecting intellectual property and sensitive data in multi-tenant SaaS (Software-as-a-Service) environments. In this paper, we present a new dynamic watermarking model designed for multi-tenant SaaS applications where various clients share resources and infrastructure. Compared to static watermarking, dynamic watermarking enables the application of individual, tenant-related watermarks at runtime without compromising performance or user experience for data streams, reports, or application content. The framework utilizes tenant-aware contextual metadata to create, embed, and trace watermarks, enabling the detection of traceable data leakage, unauthorized data

DOI: 10.4018/979-8-3373-3785-2.ch014

sharing, and audit approaches. Strong cryptographic techniques are used to protect against tampering, watermark removal, or collusion attacks, thereby upholding the integrity and non-repudiation of the watermarking procedure.

I. INTRODUCTION

Dynamic watermarking for multi-tenant SaaS (Software-as-a-Service) applications is a crucial step toward digital content protection, security, and accountability, especially when multiple tenants access sensitive and private information co-located on the same infrastructure with shared software (Vasconcelos Soares dos Santos, 2024). In the era of cloud-centric computing, enterprises are increasingly shifting their focus toward SaaS solutions due to their cost-effectiveness. Ease of implementation, leaving behind the monolithic approach of implementing an application on a legacy OS, but not without its share of pitfalls, especially in data leakage, IP theft, tampering & unauthorized sharing. Dynamic watermarking is not just about defending against these threats but also about providing a preemptive defensive line by embedding traceable and, in many cases, user-specific identifying marks into documents, reports, or media files created by the application at the point of access or download. (Charanarur & Gundu, 2025) Unlike fixed watermarking, where a non-eradicable standard overlay or notation is applied, dynamic watermarking adorns content-series or user-specific embellishments (such as usernames, timestamps, IP addresses, session IDs, or even tokens cryptographic unique to each rendering or export event), which makes instances traceable to an individual user action (Liu, 2024). This fine granularity and flexibility around context and awareness provide many benefits: it discourages leaks by increasing accountability, facilitates easy forensic tracking (post-incident), and satisfies regulatory or contractual obligations to provide auditing and non-repudiation. (Haryanto et al., 2024) If a SaaS service requires multi-tenant functionality, dynamic watermarking must be designed to support tenant isolation and customization, allowing each tenant to define personalized and custom watermarking rules, visibility, format, and operation triggers. Certain tenants may prefer visible watermakers in the open as a deterrent to misuse. On the other hand, some may use secret watermarks in metadata or steganographic embedding for stealth and, presumably, the same degree of evidence. (Asad & Farooqui, 2025) Furthermore, the technology implementation of these capabilities must prevent the intermingling of data across tenants and maintain the rigid perimeters required by multi-tenant compliance standards, e.g., SOC 2, GDPR, or HIPAA. Dynamic watermarking systems often rely on a robust back-end that intercepts data before it leaves the SaaS provider's realm, modifying PDFs, images, documents, or streaming data dynamically and injecting user and session data into the payload. (Rahdari et