Chapter 10
Quantum-Resistant Digital Watermarking-Preparing for Post-Quantum Cryptography

Neha Varshney
https://orcid.org/0009-0005-0398-736X
ABESIT Ghaziabad, India

Jhalak Saxena
HRIT University, India

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

Shilpi Gupta
Meerut Institute of Technology, Meerut, India

ABSTRACT

Quantum computers pose existential threats to classical cryptographic systems, including those used to secure digital watermarking—the embedding of robust, imperceptible information into multimedia for copyright protection and authentication. As Shor's and Grover's algorithms undermine the security of RSA, ECC, and symmetric key schemes, respectively, watermarking techniques reliant on these cryptosystems are at risk of attack once practical quantum computers emerge. This paper reviews the state-of-the-art in quantum-resistant, or post-quantum, digital watermarking. We examine approaches that leverage post-quantum public-key primitives, such as lattice-based, hash-based, and code-based cryptography, to

DOI: 10.4018/979-8-3373-3785-2.ch010

establish secure embedding and verification protocols that are immune to quantum decryption. Additionally, we analyze the computational trade-offs of integrating quantum-safe algorithms into watermarking pipelines—in terms of embedding transparency, capacity, computational cost, and resilience against attacks.

I. INTRODUCTION

With the dawning of the era of quantum computing, digital security, and especially the security of current cryptographic schemes, has become one of the paramount urgent issues. Digital watermarking – as an important method of defending against intellectual property rights and data authenticity - is confronted with the novelty and enormous attacking challenge of quantum computers (Chawla & Mehra, 2023). These devices, which exploit features such as superposition and entanglement, can break many classical cryptographic protocols used in current digital watermarking systems (Aydeger et al., 2024). As with all symmetric and public key cryptosystems, digital watermarking algorithms are threatened by Shor's quantum algorithm, necessitating the consideration of quantum-safe digital watermarking schemes to protect digital content in the future post-quantum world. Digital watermarking is an information technology that refers to imperceptibly modifying digital media (such as images, audio, video, or documents) to embed a watermark, which may carry information. The information is often used to identify its owners or producers for Copyright protection, authentication, and tracking, among other purposes. (Bishwas & Sen, 2024) These watermarking schemes are typically based on secret keys, symbols, or encryption procedures from classical cryptography (e.g., RSA or Elliptic Curve Cryptography (ECC)). Yet, quantum algorithms, such as Shor's, are able to factor large numbers and compute discrete logarithms exponentially faster than classical computers, thereby breaking the aforementioned classic cryptosystems (Li et al., 2023). It would be easy for an opponent with a sufficiently powerful quantum computer to recover keys or forge signatures, thereby breaking the trust, integrity, and legal enforceability of watermarked contents (Ren et al., 2025). Post-quantum cryptography involves developing new types of protocols and algorithms that remain secure even in the presence of an adversarial advantage and quantum attacks. Post-quantum cryptographic primitives are based on mathematical problems that are expected to be infeasible even for quantum computers, such as lattice-based, hash-based, code-based, multivariate polynomial, and isogeny-based schemes (Sahoo et al., 2024). Incorporating these primitives into the architecture of digital watermarking presents a multilayered problem: the schemes must provide quantum-proof security while preserving the invisibility of the embedded watermark, its robustness against typical attacks, and its efficiency in terms of computation and data