ENHANCING COPYRIGHT PROTECTION AND PROVENANCE IN NFTS WITH BLOCKCHAIN-INTEGRATED FREQUENCY-DOMAIN WATERMARKING

Tien Luong Trinh[1], *Minh Thanh Ta*[2,*]

Abstract

The rapid expansion of the Non-Fungible Token (NFT) market has underscored significant challenges in copyright protection and ownership authentication. While blockchain technology ensures the immutability and transparency of token transactions, the off-chain storage of metadata and original content remains a critical vulnerability, exposing NFTs to risks such as data loss, manipulation, and copyright disputes. In response to these challenges, this study proposes a blockchain-integrated watermarking framework that embeds resilient copyright information into digital assets via a general frequency-domain approach. The watermark is stored off-chain within the InterPlanetary File System (IPFS), while its associated Content Identifier (CID) is anchored in a smart contract, ensuring traceability of provenance and verification of authenticity. Comparative experiments with the Least Significant Bit (LSB) method demonstrate the superior robustness of the proposed frequency-domain technique against various attacks, including compression, noise, and image manipulation. The proposed framework significantly enhances copyright protection, facilitates transparent NFT provenance, and provides a scalable foundation for secure digital asset management within blockchain-based ecosystems.

Index terms

Blockchain; NFT; copyright protection; provenance; digital watermarking; IPFS.

1. Introduction

1.1. Overview

Recent studies highlight the explosive growth of the NFT market while also underscoring persistent challenges related to copyright and intellectual property rights. For example, Darshan *et al.* [1] reported that the NFT market exceeded

[1]Institute of Information Technolory and Electronics, Academy of Military Science and Technology
[2]Institute of Information and Communication Technology, Le Quy Don Technical University
[*]Corresponding author, email: thanhtm@lqdtu.edu.vn DOI: 10.56651/lqdtu.jst.v14.n02.1109.ict

40 billion USD during 2021–2024; however, this boom also revealed widespread confusion between token ownership and the copyright of the underlying content. To address this, researchers have proposed leveraging the immutability of blockchain to ensure authenticity of digital assets. Specifically, Ramirez López and Morillo Ledezma [2] emphasized that each NFT generates a unique "digital signature" that records provenance, authorship, and ownership in a tamper-proof manner. Supported by the transparency of public blockchains, any user can trace the full transaction history of an NFT. Similarly, Bhujel and Rahulamathavan [3] noted that this traceability enables buyers to verify ownership of the original work from its creator. Bhandare and Kandi [4] further observed that every transfer of NFT ownership is publicly logged, allowing validation of authenticity through wallet address comparisons with the original creator. Collectively, these studies demonstrate that blockchain-enabled provenance tracking not only improves transactional transparency but also protects creators' rights. Moreover, [1] proposed embedding smart contracts and licensing standards to balance copyright protection with innovation in the emerging NFT ecosystem.

Despite these advances, practical deployment of NFTs continues to face significant limitations at the data and metadata layers, as recent scholarship highlights persistent controversies over the legal nature of NFT minting and trading, as well as unresolved issues regarding copyright ownership, platform liability, and metadata integrity in the metaverse [5]. Ali *et al.* [6] reported that high Ethereum gas fees—sometimes reaching 60–100 USD per transaction—have driven many NFT projects to store only hashes or metadata on-chain, while the original content and copyright information remain off-chain [7]. Although cost-efficient, this approach introduces vulnerabilities: original files may be lost or inaccessible if the external storage fails, and metadata can be altered or redirected due to insufficient integrity safeguards. Risks increase further when metadata is stored on centralized servers, leading to censorship, unauthorized modification, or permanent data loss [8]. As a result, even though blockchain immutably records NFT transactions, provenance verification and copyright validation remain incomplete because they depend on fragile off-chain records.

Most NFT marketplaces, such as OpenSea, Foundation, SuperRare, and Rarible, currently lack an automated mechanism to embed copyright information into the content (images, videos, audio) prior to minting it into NFTs. This claim is substantiated by the absence of any references to such copyright embedding systems in the official documentation [9]–[12] and research conducted on these platforms' services. Furthermore, NFT ownership solely signifies possession of the token or a specific digital copy, without conferring copyright to the underlying work [13], see also [14], p. 23. As such, NFTs cannot substitute traditional copyright registration and necessitate supplementary mechanisms to ensure the protection of creators' rights. Recent proposals suggest the integration of decentralized storage and cryptographic techniques—such as digital signatures and hashing—into NFT metadata to enhance integrity and provenance verification. However, these methods still face considerable challenges, including high transaction costs and technical complexity when scaled. In conclusion, while NFTs contribute to improving traceability and transparency, the

existing mechanisms are inadequate for comprehensive copyright protection, particularly when essential data is stored off-chain.

Given the rapid growth and rising economic value of the NFT market, the demand for robust copyright protection and ownership verification has become increasingly urgent. The surge in NFT adoption also exposes the ecosystem to fraud, forgery, and opacity in transactions. Without effective verification mechanisms, trust among stakeholders risks deterioration, undermining overall market value. The study proposes an integrated solution leveraging advanced technologies to reinforce copyright protection while ensuring integrity and transparency of NFT ownership history. The framework enables both creators and owners to publicly and reliably authenticate provenance, while mitigating risks of data loss or metadata tampering from off-chain storage. Additionally, it considers cost-optimization strategies for blockchain transactions, thereby enhancing real-world applicability. The integration of these digital mechanisms establishes a sustainable framework for NFT copyright protection, reinforces market trust, and fosters innovation within the digital economy.

1.2. Our contributions

The paper makes three primary contributions:

- *A blockchain-integrated watermarking solution:* By adopting an established frequency-domain watermarking approach, the proposed method enhances the robustness of embedded watermark information within digital NFT assets, ensuring resistance against distortion during processing, transmission, or storage.
- *A provenance-tracking mechanism for NFTs on blockchain networks:* The scheme stores watermarks off-chain on the IPFS and utilizes CID codes to enable reliable provenance verification of NFTs, strengthening copyright protection and ownership authentication of digital assets.
- *A comparative evaluation with less robust methods:* The proposed frequency-domain watermarking technique, based on existing research, is benchmarked against conventional methods like LSB embedding, demonstrating superior robustness in preserving copyright information.

1.3. Roadmap

The paper is structured into four main stages. First, a comprehensive overview of existing information-embedding techniques is provided. Second, the adopted method from previous research is described, including the integration of frequency-domain transformations within a blockchain framework. Third, experimental results and a comparative analysis against the LSB approach are presented. Finally, conclusions are drawn and recommendations for future research directions are outlined.

2. Related work

In the field of digital image copyright management, blockchain has emerged as a promising infrastructure for ensuring transparency, immutability, and decentralization in the handling of ownership records, transfers, and provenance of NFTs. Meanwhile, the IPFS provides a decentralized off-chain storage solution, addressing the limitations

of storing large digital assets directly on-chain. Through content addressing with unique CIDs, IPFS allows efficient retrieval of digital assets while significantly reducing blockchain data load and associated gas costs. The integration of IPFS with blockchain ensures metadata persistence, overcoming the risks posed by centralized links in NFT infrastructures. In particular, linking the CID to smart contracts strengthens integrity and prevents metadata manipulation, thereby reinforcing trust in NFT ecosystems [8], [13], [14]. Numerous studies and prototypes have demonstrated the effectiveness of NFT–IPFS integration for managing digital content, utilizing CIDs for asset identification and smart contracts for authenticity verification [15].

Beyond provenance tracking and storage optimization, researchers have also explored combining blockchain with watermarking and digital signatures to enhance copyright protection. Cong *et al.* [16] introduced a system that integrates blockchain with invisible watermarking and digital signatures, where blockchain secured provenance information and watermarking embedded copyright details directly into digital images. Similarly, Sri Lakshmi Madapati *et al.* [17] developed a decentralized verification framework that compared hash values stored on-chain with those of digital assets, enabling reliable verification without intermediaries. Expanding on these directions, Ranjbar Alvar *et al.* [18] proposed embedding ownership and buyer information into the asset itself, while simultaneously managing these assets as NFTs, thus guaranteeing verifiable ownership and transparent transaction history within blockchain networks.

The Blockmarking framework, first introduced by Thanh *et al.* in 2022 [19], exemplifies an early integration of watermarking and blockchain by embedding author metadata into digital images and recording their hashes on-chain, thereby ensuring a tamper-resistant and transparent provenance record. Building upon this foundation, Thanh *et al.* further extended the framework in 2024 [20] by incorporating IPFS-based decentralized storage and adopting multi-layer watermarking techniques. This advancement not only strengthened ownership verification and improved the detection of unauthorized copies but also enhanced the scalability and robustness of the original system. Collectively, these two works illustrate a coherent research trajectory, showcasing the evolution of Blockmarking from a conceptual prototype into a more sophisticated and practical solution for decentralized copyright protection. Additionally, these systems employed smart contract–based licensing mechanisms, enabling automated copyright enforcement and reducing the reliance on centralized authorities. Collectively, these hybrid models illustrate the potential of integrating blockchain, IPFS, and watermarking to create transparent, decentralized, and enforceable digital copyright management systems [21]–[23].

Parallel to blockchain integration, watermarking techniques themselves have evolved significantly, reflecting different trade-offs between robustness and imperceptibility. Spatial-domain methods such as the LSB embedding are widely recognized for their simplicity and high embedding capacity; however, they are vulnerable to compression, filtering, and format conversion [24], [25]. In contrast, transform-domain methods, notably the Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT), provide greater resilience to common image processing attacks. For instance,

pure DWT watermarking has been shown to achieve higher correlation coefficients under distortion compared to LSB [25], while approaches based on the Discrete Cosine Transform (DCT) are particularly compatible with JPEG compression. Araghi *et al.* [26] examine the impact of applying deeper levels of SVD within hybrid DWT–SVD watermarking schemes, with a particular emphasis on imperceptibility and robustness. Their results indicate that the proposed two-level SVD approach achieves superior performance compared to the conventional method, especially under diverse signal processing and geometric attacks. Hybrid technology approaches have also demonstrated promising results: Wu *et al.* [27] propose a semiblind watermarking scheme that combines DWT–SVD with a chaotic map to enhance both imperceptibility and robustness. Their method achieves high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) values while maintaining strong resistance against common signal processing and geometric attacks, while Soundrapandiyan *et al.* [28] employed a hybrid DWT–DCT approach for medical images, their study demonstrated an effective balance between imperceptibility and resilience.

Despite significant advancements in blockchain, NFT, and IPFS technologies, existing literature primarily focuses on asset storage, provenance tracking, and metadata integrity, with limited attention to ensuring watermark persistence within a blockchain-based smart contract environment. While blockchain and NFTs provide immutability and ownership tracking, and IPFS offers decentralized storage, these systems alone cannot fully guarantee the authenticity and copyright protection of digital assets. Without watermarking, there is no robust mechanism to safeguard against unauthorized replication or tampering. By integrating watermarking, the proposed approach adds a critical layer of protection, embedding a unique, traceable identifier directly into the asset. This ensures the digital asset's copyright is verifiable and persistent throughout its lifecycle, enhancing the system's ability to effectively manage and protect digital copyright.

3. The proposed method

3.1. System architecture overview

The proposed solution authenticates digital images and safeguards copyrights by integrating digital watermarking with blockchain technology, while storing metadata on IPFS. This approach harnesses the strengths of blockchain, watermarking, and decentralized storage to effectively manage digital assets. Although previous research has examined the combination of blockchain and watermarking [29], and the computational challenges associated with performing these tasks on-chain [30], existing public blockchains, such as Ethereum, face limitations in directly processing watermarking due to high computational costs and gas fees. These systems typically store image hashes or metadata on-chain, with watermarking often handled off-chain. The constraints of current blockchain systems render them impractical for watermarking, which requires the efficient processing of large image files and complex algorithms.

Consequently, in this study, the watermark extraction and embedding processes are carried out off-chain. Future work will involve developing a private blockchain system optimized for the computational demands of digital asset copyright management. The proposed architecture is conceptualized as a three-layer framework designed to provide end-to-end security and authenticity for digital images. The layers are:

- *Watermarking engine*: The hybrid frequency-domain watermarking technique, integrating DWT, the decomposition into an orthogonal matrix Q and an upper-triangular matrix R (QR) , and SVD, embeds imperceptible and robust data directly into the image, providing resilient in-band authentication data.
- *Decentralized storage layer*: IPFS provides a permanent, content-addressed repository for the asset, acting as a "digital vault".
- *Provenance layer*: Blockchain creates an unforgeable record of ownership and authenticity, while a NFT on a public blockchain serves as an immutable, universally accessible “digital birth certificate”, cryptographically linking the creator, the asset, and its watermark.

The innovation of the proposed approach lies not in the individual components, but in their integrated synergy. The resulting three-part cryptographic link—connecting the identity to the image data, the image data to a persistent address, and that address to a public ledger—establishes a more robust framework for verifying authenticity than any single technology could achieve on its own. This model represents a paradigm shift from traditional centralized Digital Rights Management systems, which depend on restrictive controls, to verifiable digital provenance. The proposed approach enables independent, trustless authentication of a digital asset’s origin and integrity. The system operates through two primary protocols, which are outlined in detail below.

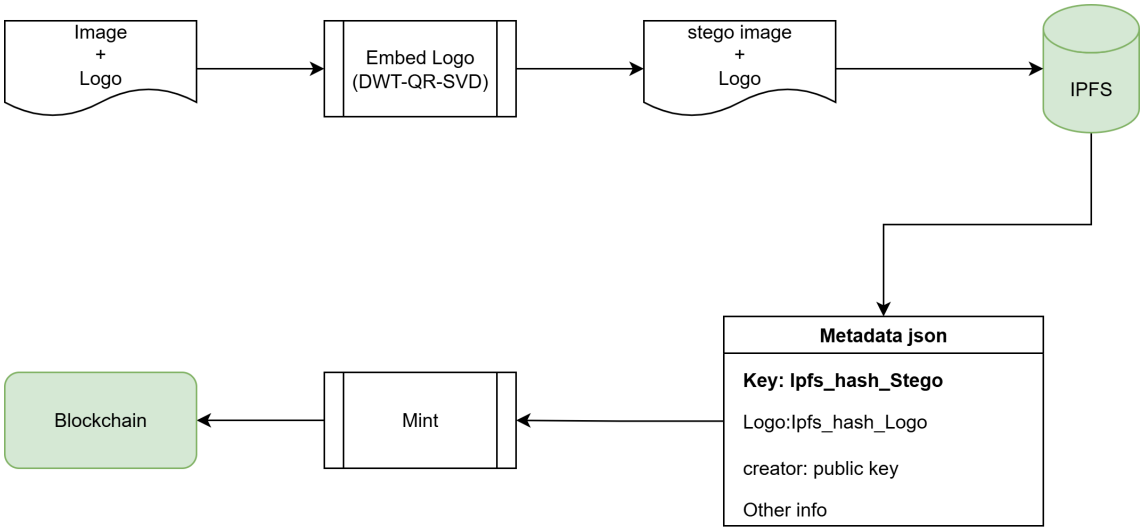

Fig. 1. Embedding and Minting.

- *Embedding and Minting protocol*: As depicted in Fig. 1, a creator first embeds an identifying logo into a host image using the DWT-QR-SVD engine. The resulting

stego-image and the original logo are then uploaded to the IPFS network. Finally, an NFT is minted on a public blockchain, with its metadata containing the CIDs for both assets, along with the creator's public key.

- *Verification and Authentication protocol*: As depicted in Fig. 2, a verifier uses the public information stored in the NFT to retrieve the stego-image and the original logo from IPFS. The embedded logo is then extracted from the stego-image using the inverse watermarking algorithm. Finally, the extracted logo is quantitatively compared against the original logo to confirm authenticity, resulting in a definitive "Success" or "Reject" outcome.

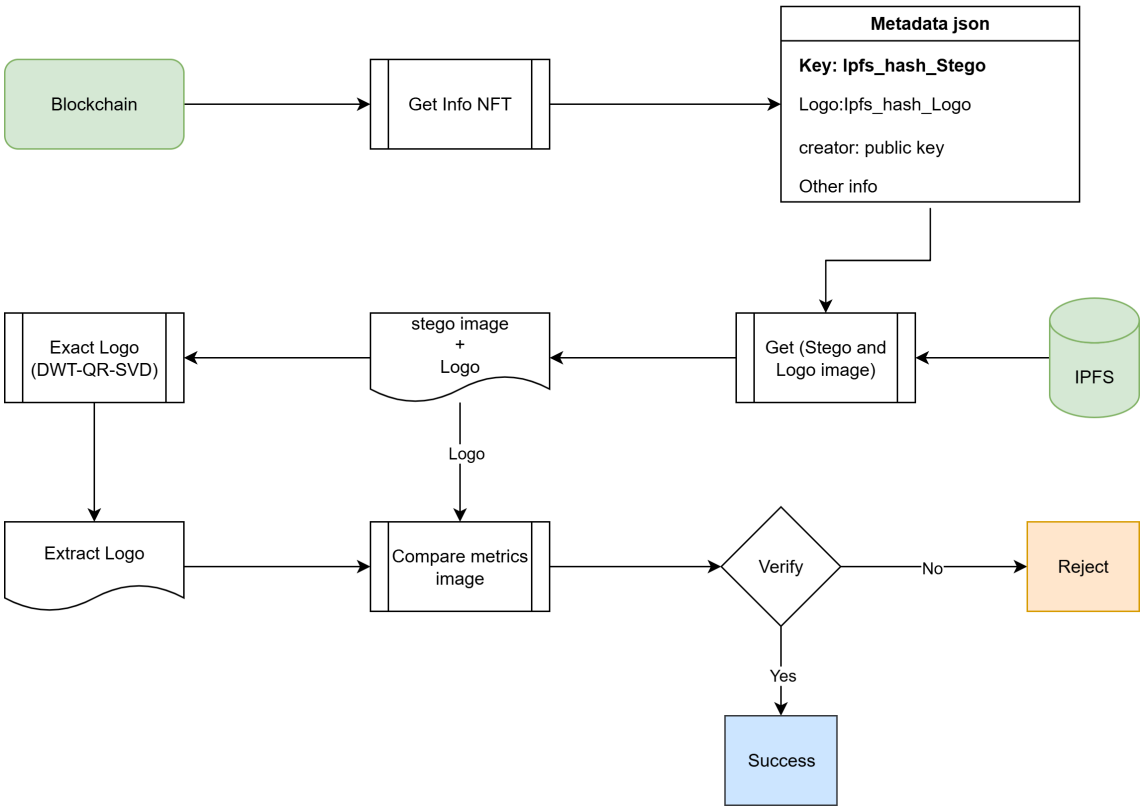

Fig. 2. Verification and Authentication.

3.2. Watermarking scheme

The core of the system's security lies in its hybrid watermarking engine. The selection of a combined DWT, QR, and SVD approach is a strategic decision designed to achieve a superior balance between the three cardinal properties of digital watermarking: imperceptibility, robustness, and capacity. The algorithmic parameters and notations used in this process are summarized in Table 1.

Building upon these definitions, Algorithm 1 illustrates the embedding procedure. This algorithm leverages the decomposition power of DWT and QR to localize the embedding domain, followed by the singular value manipulation offered by SVD. By

modifying the singular values of the transformed host image with those of the watermark, the method ensures that the embedded information is both stable and imperceptible.

Table 1. Algorithmic parameters and notations

Symbol	Description	Type / Example / Value
I	Original cover image	Color image matrix (M×N×3), uint8
B, G, R	Blue, Green, Red channels	Color matrix (M×N) for each channel
W	Watermark image	Grayscale image matrix (m×n), uint8
R	DWT decomposition level	Integer 1–3
LL, HL, LH, HH	Sub-bands from DWT	Sub-matrices (half-size per level)
$Q, R1$	QR decomposition of LL_R	Orthogonal Q and upper triangular $R1$
HU_w, HS_w, HV_w	SVD of $R1$	Orthogonal matrices and singular values
U_w, S_w, V_w	SVD of watermark W	Orthogonal matrices and singular values
α	Embedding strength factor	Positive float (e.g. 0.05–0.2)
HS_w^{hat}	Singular values after embedding	$HS_w^{hat} = HS_w + \alpha S_w$
H_{hat}	Reconstructed matrix with watermark	$HU_w \cdot diag(HS_w^{hat}) \cdot HV_w$
LL_{hat}	LL band after watermarking	$LL_{hat} = Q \cdot H_{hat}$
I_{wm}	Watermarked image	Color image matrix (M×N×3), uint8
Hw	R matrix from QR of watermarked LL	Output of QR(LLw_R)
$HSbw_{hat}$	Singular values of Hw	Vector from SVD(Hw)
S_w^{hat}	Estimated singular values of W	$(HSbw_{hat} - HS_w)/\alpha$
W_{ext}	Extracted watermark	Grayscale image matrix (m×n), uint8

Algorithm 1: DWT–QR–SVD Watermark Embedding

Require: Cover image I (with channels B, G, R), watermark W, embedding strength α, DWT level R

Ensure: Watermarked image I_{wm} and keys $\{HS_w, U_w, V_w, R, \alpha\}$

1: Split $I \to (B, G, R)$
2: Apply R-level DWT (Haar) on B to obtain lowband LL_R and subband stack $\mathcal{S}$
3: QR-decompose $LL_R \Rightarrow (Q, R1)$
4: SVD of $R1$: $R1 = HU_w \cdot \mathrm{diag}(HS_w) \cdot HV_w$
5: SVD of W: $W = U_w \cdot \mathrm{diag}(S_w) \cdot V_w$
6: Embed on singular values: $\hat{HS_w} \leftarrow HS_w + \alpha\, S_w$
7: Rebuild $\hat{H} \leftarrow HU_w \cdot \mathrm{diag}(\hat{HS_w}) \cdot HV_w$
8: Reconstruct lowband: $\hat{LL} \leftarrow Q \cdot \hat{H}$
9: Inverse R-level DWT with $\hat{LL}$ and $\mathcal{S}$ to get watermarked blue channel $\tilde{B}$
10: Merge channels: $I_{wm} \leftarrow \mathrm{Merge}(\tilde{B}, G, R)$
11: **return** I_{wm}, keys $\{HS_w, U_w, V_w, R, \alpha\}$

In a complementary manner, Algorithm 2 outlines the extraction phase. Using the same decomposition path, the algorithm isolates the modified singular values from the attacked or altered watermarked image. These values are then compared with the original host singular values to reconstruct an estimate of the embedded watermark.

Algorithm 2: DWT–QR–SVD Watermark Extraction

Require: Watermarked image (or its blue channel) $\tilde{B}$, keys $\{HS_w, U_w, V_w, R, \alpha\}$
Ensure: Extracted watermark W_{ext}
1: Apply R-level DWT (Haar) on $\tilde{B}$ to obtain $LL_{w,R}$ and subband stack $\mathcal{S}_w$
2: QR-decompose $LL_{w,R} \Rightarrow (Q_w, H_w)$ ▷ H_w is the R-factor
3: SVD of H_w: $H_w = \hat{HU_w} \cdot \mathrm{diag}(HSbw) \cdot \hat{HV_w}$
4: Recover watermark singular values: $\hat{S_w} \leftarrow \dfrac{HSbw - HS_w}{\alpha}$
5: Rebuild watermark: $W_{ext} \leftarrow U_w \cdot \mathrm{diag}(\hat{S_w}) \cdot V_w$
6: **return** W_{ext}

3.3. Integration with decentralized technologies for immutable provenance

While a robust watermark provides authenticity, it does not inherently ensure a permanent, publicly verifiable record. To address this gap, the proposed method integrates the watermarking engine with decentralized technologies, combining the IPFS for storage and a blockchain-based NFT for provenance. This integration establishes an immutable chain of custody for the digital asset.

After obtaining the CIDs of the stego image (CID_{stego}) and the original logo (CID_{logo}) from IPFS, a smart contract transaction mints an NFT on a public blockchain. The NFT functions as an on-chain certificate of authenticity and ownership, secured by blockchain properties of decentralization, transparency, and tamper-resistance. The associated metadata—a structured JSON object—links the token to the off-chain assets and contains the IPFS hashes, the creator's public key, and optional copyright information (Fig. 1). This ensures verifiable provenance through the persistent storage of files on IPFS and the irreversible commitment of their CIDs on the blockchain.

4. Results and comparison

In this section, the paper will experiment with methods including the DWT, QR analysis, and SVD, based on the framework proposed by Nguyen Thanh Hai *et al.* [31]. The approach incorporates the use of the IPFS for decentralized off-chain storage and CIDs for provenance tracking. The paper will then compare the results of this approach with other techniques, such as DWT-SVD [32] and the basic LSB method. Finally, the study highlights the advantages of frequency domain watermarking in improving copyright protection for NFTs and other digital assets.

4.1. Experimental environment

All experiments were conducted on a client workstation running Ubuntu (version 22.04 LTS). The system is equipped with an Intel Core i5 (11^{th} generation) CPU, 16 GB of RAM, and a 512 GB NVMe SSD. Experimental evaluation shows that this configuration is sufficient for efficiently executing DWT, DCT, watermark embedding, and IPFS pinning tasks.

After watermark embedding, the resultant stego-image is exported to the IPFS by uploading through Pinata, a pinning service offering reliable IPFS gateway functionality. The obtained CID is embedded into the tokenURI field of an ERC-721 [33] compliant NFT metadata JSON. The metadata follows typical NFT standards, where the image or tokenURI field references the IPFS-stored resource via the content-addressed CID.

The smart contract implementing the ERC-721 standard was then deployed and tested on the Sepolia Ethereum testnet [34], [35]. Sepolia is currently the preferred Ethereum test network for developers, offering a lightweight, proof-of-stake environment that closely simulates mainnet behavior but uses valueless test ETH - a form of Ethereum used for testing purposes with no real-world value.

To interact with Sepolia, standard Ethereum development tools (e.g., Remix, Hardhat, Truffle) were configured to point to the appropriate RPC endpoint and network chain identifier and to recognize Sepolia block explorer services for transaction tracking.

4.2. Evaluate the functionality of copyright protection systems

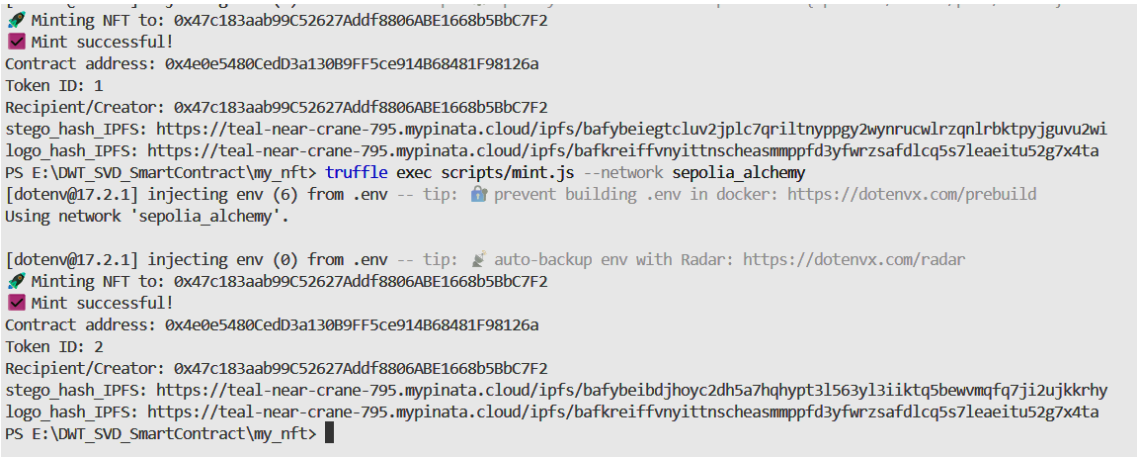

Fig. 3. Mint NFTs.

- *Mint NFTs:* Fig. 3 presents the experimental results of minting an NFT on the Sepolia Ethereum testnet through a Truffle script. The output confirms the successful minting process, providing details such as the contract address, token identifier (token ID), recipient/creator address, as well as the IPFS hashes of both the stego image and the original logo. These results demonstrate that the proposed watermarking system is tightly integrated with decentralized infrastructures (IPFS and blockchain), thereby establishing an immutable and publicly verifiable proof of authenticity. Users can independently verify this provenance record by inspecting the corresponding transaction on the blockchain.[1]
- *Authored NFT set*: Fig. 4 illustrates the interaction between our client software and the blockchain to retrieve data on the NFTs minted by a specific wallet address. The query result shows that the wallet has created three NFTs, each with

[1]https://sepolia.etherscan.io/tx/0x10731bcd36e15be4708a80ccad0bb1b9e85ce02a2379baaa255534b02d3d7ca4

a unique token identifier, name, and description. For every NFT, the corresponding IPFS hashes of both the stego image and the original logo are provided, together with the creator's public key. These outputs confirm that the system can automatically fetch and display on-chain information, thereby enabling transparent monitoring of the minting history. Such integration between blockchain queries and IPFS metadata demonstrates the persistence of provenance records and the accessibility of verifiable evidence of ownership and authenticity.

```
NFT Contract Address: 0x4e0e5480CedD3a130B9FF5ce914B68481F98126a
Checking NFTs created by: 0x47c183aab99C52627Addf8806ABE1668b5BbC7F2
totalSupply = 3

Wallet 0x47c183aab99C52627Addf8806ABE1668b5BbC7F2 has created 3 NFTs
-------------------------------------
#Token ID: 1
  Name: Lena NFT
  Description: Lena NFT created by recipient
  stegoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafybeiegtcluv2jplc7qriltnyppgy2wynrucwlrzqnlrbktpyjguvu2wi
  logoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafkreiffvnyittnscheasmmppfd3yfwrzsafdlcq5s7leaeitu52g7x4ta
  publicKeyCreator: 0x47c183aab99c52627addf8806abe1668b5bbc7f2
-------------------------------------
#Token ID: 2
  Name: Madrill NFT
  Description: Madrill NFT created by recipient
  stegoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafybeibdjhoyc2dh5a7hqhypt3l563yl3iiktq5bewvmqfq7ji2ujkkrhy
  logoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafkreiffvnyittnscheasmmppfd3yfwrzsafdlcq5s7leaeitu52g7x4ta
  publicKeyCreator: 0x47c183aab99c52627addf8806abe1668b5bbc7f2
-------------------------------------
#Token ID: 3
  Name: Pepper NFT
  Description: Pepper NFT created by recipient
  stegoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafybeid2ip2ah5z42u6k63tggyut63vbnebdkhldkvd6lmnnqm3yyhz7tq
  logoHashIPFS: https://teal-near-crane-795.mypinata.cloud/ipfs/bafkreiffvnyittnscheasmmppfd3yfwrzsafdlcq5s7leaeitu52g7x4ta
  publicKeyCreator: 0x47c183aab99c52627addf8806abe1668b5bbc7f2
-------------------------------------
```

Fig. 4. Authored NFT set.

- *NFT transfer history*: Fig. 5 demonstrates the transfer of ownership of an NFT, distinct from its initial creation. The system retrieves data directly from the blockchain, displaying the full transaction history of Token ID = 2. The record shows the original mint event, where the creator became the first owner, followed by subsequent transfer transactions to other wallet addresses. Each event is presented with block number, timestamp, transaction hash, sender and recipient addresses, thereby enabling transparent and verifiable tracking of asset ownership. Users can independently confirm this provenance history through the corresponding on-chain record.[2]
- *Owned NFT set*: Fig. 6 illustrates the current state of NFT ownership after user-to-user transfers have been executed. The highlighted yellow address represents the present owner of Token ID 2 and Token ID 3, while the metadata of each NFT continues to preserve the information about the original creator. The system distinguishes clearly between creation rights and ownership rights, this separation allows ownership and provenance to be reliably tracked on the blockchain.

[2]https://sepolia.etherscan.io/token/0x4e0e5480cedd3a130b9ff5ce914b68481f98126a?a=2

Fig. 5. NFT transfer history.

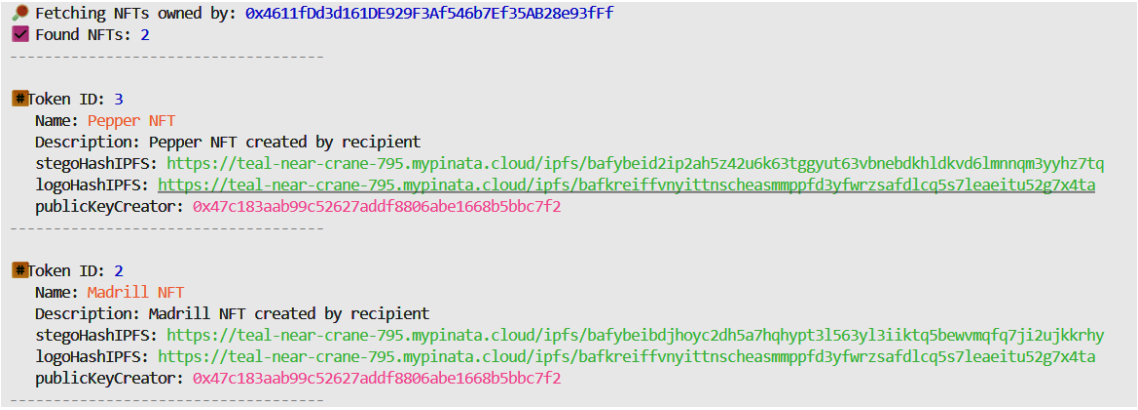

Fig. 6. Owned NFT set.

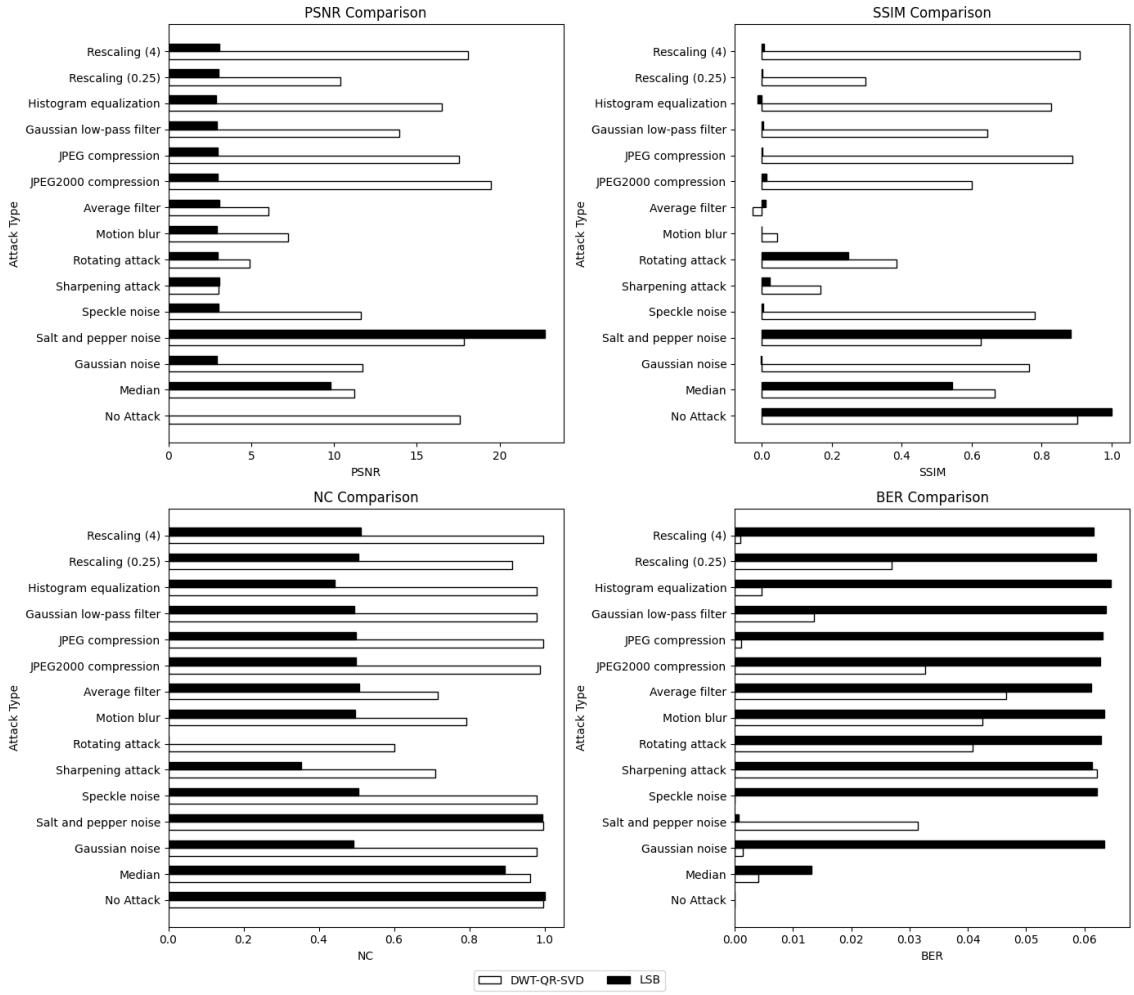

Fig. 7. Comparison of DWT-QR-SVD and LSB watermarking techniques.

4.3. Performance evaluation of watermarking robustness

This section evaluates the robustness and indiscernibility of the proposed watermarking system under various signal processing and geometric attacks, using 14 different attack methods. The performance of DWT-QR-SVD, DWT-SVD, and LSB was assessed based on four metrics: PSNR, SSIM, Normalized Correlation (NC), and Bit Error Rate (BER), across different attack scenarios, including compression, filtering, noise injection, and geometric transformations.

In the Fig. 7, DWT-QR-SVD (no color) outperforms LSB (black) in all metrics, demonstrating superior robustness against attacks such as JPEG compression and Gaussian noise. LSB, on the other hand, shows poor performance, with significant degradation in watermark quality and durability after extraction. This highlights that frequency domain methods like DWT-QR-SVD are more robust and sustainable than spatial domain methods like LSB.

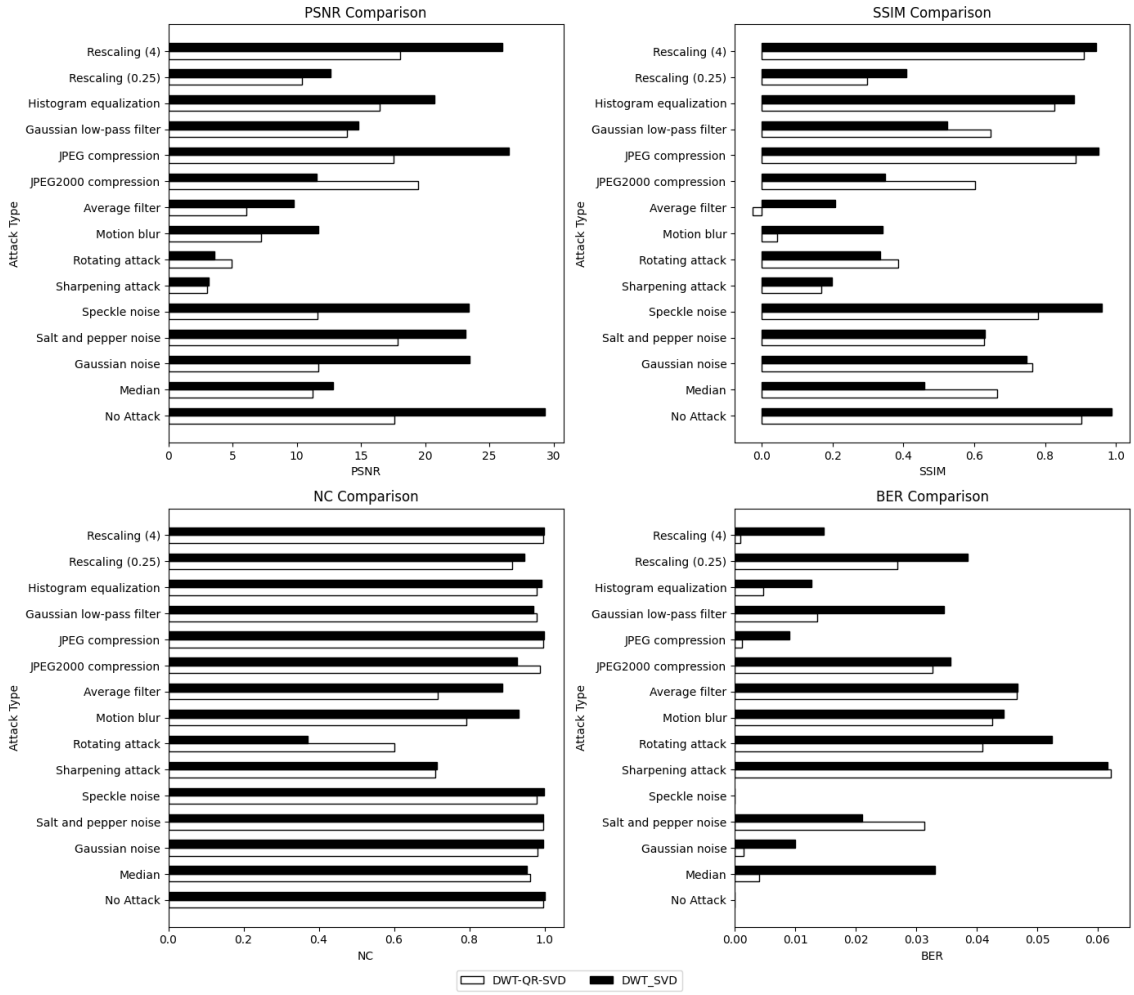

Fig. 8. Comparison of DWT-QR-SVD and DWT-SVD watermarking techniques.

In the Fig. 8, DWT-QR-SVD (no color) performs better than DWT-SVD (black) in NC and BER, indicating better watermark retention and resistance to bit error attacks. However, DWT-SVD slightly excels in PSNR and SSIM, with only minor differences between the two methods. Both DWT-QR-SVD and DWT-SVD show similar robustness.

Fig. 9 illustrates the visual results for each method, showing the extracted watermark after the attack. The left column displays results for DWT-QR-SVD, while the right column represents results for LSB. Among 15 different image attack techniques, the DWT-QR-SVD method successfully identifies 13 out of 15 logo images, whereas the LSB method recognizes only 3 out of 15.

Frequency domain methods, such as DWT-QR-SVD and DWT-SVD, demonstrate clear advantages over spatial domain methods like LSB, particularly in terms of robustness against compression and noise attacks. These methods consistently achieve higher PSNR and SSIM values, ensuring better image quality preservation. The NC values for DWT-QR-SVD are close to 1, indicating strong watermark extraction

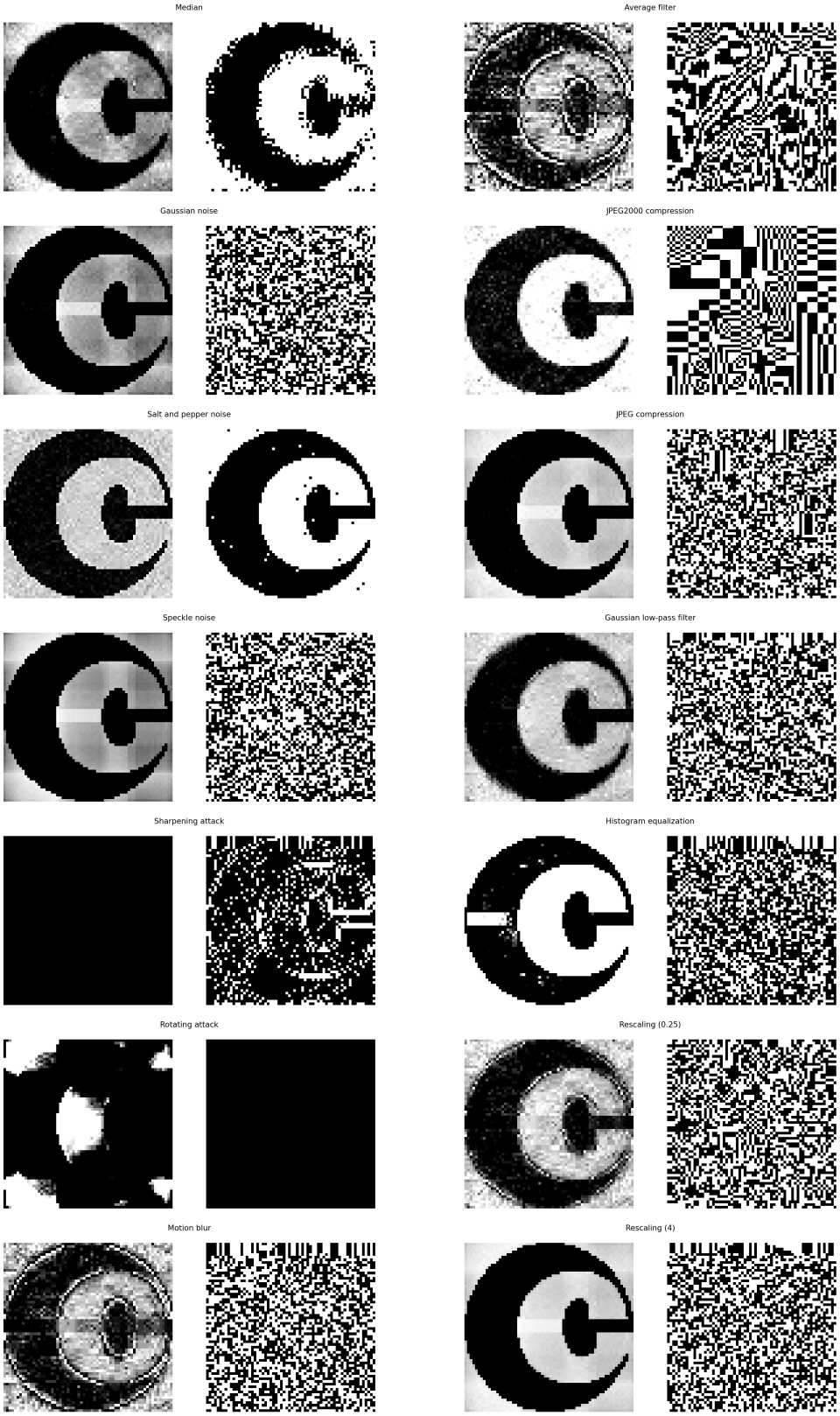

Fig. 9. Watermarking results and recovery performance after attack.

reliability, while the lower BER reflects fewer retrieval errors. In contrast, LSB shows significant degradation across all metrics under most attack conditions.

Overall, frequency domain methods offer superior resilience and effectiveness, making them a more reliable choice for copyright protection applications.

5. Conclusions

The proposed DWT-QR-SVD watermarking technique has demonstrated strong resilience against a wide spectrum of image-processing and geometric attacks. Experimental evaluations across PSNR, SSIM, NC, and BER metrics confirm that this hybrid transform-based approach achieves superior imperceptibility and robustness compared with fragile spatial-domain methods such as LSB. These results highlight its suitability for reliable digital copyright protection in real-world environments.

In parallel, the decentralized copyright management framework developed in the study integrates watermarking with IPFS and blockchain-based NFTs, offering a complete set of functionalities. The system not only embeds essential ownership and authenticity information directly into the token at the minting stage but also ensures persistent, censorship-resistant, and publicly verifiable provenance records. This combination addresses the long-standing limitations of centralized repositories and off-chain metadata storage.

Future work will aim to extend the framework by enabling watermark embedding and extraction directly on-chain, investigating more advanced and adaptive watermarking techniques, and conducting large-scale performance evaluations on high-throughput blockchains to assess scalability. By pursuing these directions, the proposed system may evolve into a comprehensive and deployable solution that further strengthens the integrity, resilience, and trustworthiness of digital copyright protection in decentralized ecosystems.

References

[1] P. Darshan, J. S. Rohan, R. Rajesh, M. Ruchitha, S. Kamath, and M. N. Manas, “Intellectual property rights and entrepreneurship in the NFT ecosystem: Legal frameworks, business models, and innovation opportunities,” *arXiv preprint arXiv:2507.00172*, 2025. DOI: 10.48550/arXiv.2507.00172

[2] L. J. Ramirez Lopez and G. G. Morillo Ledezma, “Employing blockchain, NFTs, and digital certificates for unparalleled authenticity and data protection in source code: A systematic review,” *Computers*, Vol. 14, No. 4, p. 131, 2025. DOI: 10.3390/computers14040131

[3] S. Bhujel and Y. Rahulamathavan, “A survey: Security, transparency, and scalability issues of NFTs and its marketplaces,” *Sensors*, Vol. 22, No. 22, p. 8833, 2022. DOI: 10.3390/s22228833

[4] T. Bhandare and M. A. Kandi, “Tokenization of fine arts: Revolutionizing the fine arts industry with blockchain,” in *Blockchain and Smart-Contract Technologies for Innovative Applications*, N. E. Madhoun, I. Dionysiou, and E. Bertin. Springer Nature Switzerland, 2024, pp. 167–187. DOI: 10.1007/978-3-031-50028-2_6

[5] Y. Dong and C. Wang, “Copyright protection on NFT digital works in the metaverse,” *Security and Safety*, Vol. 2, pp. 1–14, 2023. DOI: 10.1051/sands/2023013

[6] O. Ali, M. Momin, A. Shrestha, R. Das, F. Alhajj, and Y. K. Dwivedi, “A review of the key challenges of non-fungible tokens,” *Technological Forecasting and Social Change*, Vol. 187, pp. 1–13, 2023. DOI: 10.1016/j.techfore.2022.122248

[7] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, “NFTs for combating deepfakes and fake metaverse digital contents,” *Internet of Things*, Vol. 25, pp. 1–24, 2024. DOI: 10.1016/j.iot.2024.101133

[8] H. Salem, H. Salloum, M. Mazzara, N. Askarbekuly, L. Johard, and G. Succi, "Hidden risks: The centralization of NFT metadata and what it means for the market," in *Advanced Information Networking and Applications (AINA 2025)*. Springer Nature Switzerland, 2025, pp. 154–162. DOI: 10.1007/978-3-031-87775-9_13
[9] OpenSea, "Terms of service," Last updated: Sep. 14, 2025. [Online]. Available: https://opensea.io/tos.
[10] F. Labs, "Terms of service," Last updated: May 30, 2024. [Online]. Available: https://foundation.app/terms.
[11] SuperRare, "Terms of service," Last updated: April 5, 2023. [Online]. Available: https://campaigns.superrare.com/terms.
[12] Rarible, "Terms of service," Last updated: Dec 5, 2022. [Online]. Available: https://static.rarible.com/terms.pdf.
[13] Z. Wang, J. Gao, and X. Wei, "Do NFTs' owners really possess their assets? A first look at the NFT-to-asset connection fragility," in *Proceedings of the ACM Web Conference 2023*, 2023, pp. 2099–2109. DOI: 10.1145/3543507.3583281
[14] U.S. Patent and Trademark Office and U.S. Copyright Office, "Non-fungible tokens and intellectual property: A report to congress," Technical Report, 2024. [Online]. Available: https://www.uspto.gov/sites/default/files/documents/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf
[15] H. Ko, J. Oh, and S. U. Kim, "Digital content management using non-fungible tokens and the interplanetary file system," *Applied Sciences*, Vol. 14, No. 1, p. 315, 2024. DOI: 10.3390/app14010315
[16] X. Cong, L. Feng, and L. Zi, "Research on IPFS image copyright protection method based on blockchain," *Computers, Materials & Continua*, Vol. 81, No. 1, pp. 663–684, 2024. DOI: 10.32604/cmc.2024.054372
[17] S. L. Madapati and N. R. Pradhan, "Decentralizing video copyright protection: A blockchain enabled novel framework with performance evaluation," *Frontiers in Artificial Intelligence*, Vol. 8, 2025. DOI: 10.3389/frai.2025.1655709
[18] S. R. Alvar, M. Akbari, D. M. X. Yue, and Y. Zhang, "NFT-based data marketplace with digital watermarking," in *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, New York, 2023, pp. 4756–4767. DOI: 10.1145/3580305.3599876
[19] L. D. Tai, V. T. Nguyen, and M. T. Ta, "Blockmarking: Hybrid model of blockchain and watermarking technique for copyright protection," in *Proceedings of the 11th International Symposium on Information and Communication Technology (SoICT2022)*, 2022, pp. 398–404. DOI: 10.1145/3568562.3568575
[20] L. D. Tai and T. M. Thanh, "A proposal of digital contents copyright protection by using blockmarking technique," *Computer Science*, Vol. 25, No. 4, 2024. DOI: 10.7494/csci.2024.25.4.5377
[21] L. Zhao, J. Zhang, and H. Jing, "Blockchain-enabled digital rights management for museum-digital property rights," *Intelligent Automation & Soft Computing*, Vol. 34, No. 3, pp. 1785–1801, 2022. DOI: 10.32604/iasc.2022.029693
[22] R. Shi, R. Cheng, B. Han, Y. Cheng, and S. Chen, "A closer look into IPFS: Accessibility, content, and performance," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, Vol. 8, No. 2, pp. 1–31, 2024. DOI: 10.1145/3656015
[23] M. Dalla Preda and F. Masaia, "Exploring NFT validation through digital watermarking," in *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES)*, 2023, pp. 1–6. DOI: 10.1145/3600160.3605063
[24] S. Sharma, J. J. Zou, G. Fang, P. Shukla, and W. Cai, "A review of image watermarking for identity protection and verification," *Multimedia Tools and Applications*, Vol. 83, No. 11, pp. 31 829–31 891, 2024. DOI: 10.1007/s11042-023-16843-3
[25] M. S. Saini, B. Venkata Kranthi, and G. S. Kalra, "Comparative analysis of digital image watermarking techniques in frequency domain using matlab simulink," *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, No. 4, pp. 1136–1141, 2012.
[26] T. K. Araghi and D. Megías, "Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking," *Multimedia Tools and Applications*, Vol. 83, No. 2, pp. 3895–3916, 2024. DOI: 10.1007/s11042-023-15554-z
[27] W. Wu, Y. Dong, and G. Wang, "Image robust watermarking method based on DWT–SVD transform and chaotic map," *Complexity*, Vol. 2024, No. 1, 2024. DOI: 10.1155/2024/6618382
[28] R. Soundrapandiyan, K. Rajendiran, A. Gurunathan, A. Victor, and R. Selvanambi, "Analysis of DWT–DCT watermarking algorithm on digital medical imaging," *Journal of Medical Imaging*, Vol. 11, No. 1, 2024. DOI: 10.1117/1.JMI.11.1.014002
[29] O. P. Singh, K. N. Singh, A. K. Singh, and A. K. Agrawal, "Watermarking with blockchain: A survey," in *Digital Image Security*. CRC Press, 2024, pp. 200–224.
[30] E. Sariboz, K. Kolachala, G. Panwar, R. Vishwanathan, and S. Misra, "Off-chain execution and verification of computationally intensive smart contracts," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–3. DOI: 10.1109/ICBC51069.2021.9461142

[31] T. H. Nguyen and M. T. Ta, "Robust image watermarking algorithm integrating QR and singular value decomposition in the discrete wavelet transform domain," in *Proceedings of the 2nd International Conference on Cryptography and Information Security (VCRIS2025)*, 2025, pp. 1–6. DOI: 10.1109/VCRIS68011.2025.11250561

[32] R. K. Singh, D. K. Shaw, and J. Sahoo, "A secure and robust block based DWT-SVD image watermarking approach," *Journal of Information and Optimization Sciences*, Vol. 38, No. 6, pp. 911–925, 2017. DOI: 10.1080/02522667.2017.1372137

[33] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "ERC-721: Non-fungible token standard," Last updated: Jan. 24, 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721.

[34] Dune Docs, "Sepolia testnet overview," [Online]. Available: https://docs.dune.com/data-catalog/evm/sepolia/overview, Accessed: Sep. 21, 2025.

[35] Etherscan, "Supported chains," [Online]. Available: https://docs.etherscan.io/supported-chains, Accessed: Sep. 21, 2025.

Manuscript received 29-9-2025; Accepted 19-12-2025.

■

Tien Luong Trinh is a researcher at Institute of Information Technolory and Electronics. He has contributed to many projects related to the application of information technology in promoting digital transformation and developing e-government systems in military units. His research interests include digital watermarking, blockchain, information security and computer vision. E-mail: luongk237@gmail.com

Minh Thanh Ta is an Associate Professor and Vice Dean at the Institute of Information and Communication Technology, Le Quy Don Technical University, Vietnam. He is also a Postdoctoral Fellow in the Department of Mathematical and Computing Sciences at Tokyo Institute of Technology, Japan. He received his B.S. and M.S. degrees in Computer Science from the National Defense Academy, Japan, in 2005 and 2008, respectively, and his Ph.D. from Tokyo Institute of Technology, Japan, in 2015. He is a member of the Information Processing Society of Japan (IPSJ) and the Institute of Electrical and Electronics Engineers (IEEE). His research interests include digital watermarking, network security, and computer vision. Correspondence can be addressed to: thanhtm@lqdtu.edu.vn

TĂNG CƯỜNG BẢO VỆ BẢN QUYỀN VÀ TRUY VẾT NGUỒN GỐC TRONG CÁC NFT BẰNG THỦY VÂN MIỀN TẦN SỐ TÍCH HỢP BLOCKCHAIN

Trịnh Tiến Lương, *Tạ Minh Thanh*

Tóm tắt

Sự phát triển nhanh chóng của thị trường NFT đã làm nổi bật những thách thức lớn trong việc bảo vệ bản quyền và xác thực quyền sở hữu. Mặc dù công nghệ blockchain đảm bảo tính bất biến và minh bạch của các giao dịch token, nhưng việc lưu trữ dữ liệu và nội dung gốc ngoài chuỗi vẫn là một lỗ hổng quan trọng, làm cho NFT dễ bị mất dữ liệu, thao túng và tranh chấp bản quyền. Để giải quyết những vấn đề này, nghiên cứu này đề xuất một khuôn khổ thủy vân tích hợp blockchain, nhúng thông tin bản quyền bền vững vào tài sản kỹ thuật số thông qua phương pháp miền tần số tổng quát. Thủy vân được lưu trữ ngoài chuỗi trên hệ thống tệp liên hành tinh (IPFS), trong khi mã nhận dạng nội dung (CID) của nó được neo trong hợp đồng thông minh, đảm bảo khả năng truy vết nguồn gốc và xác minh tính xác thực. Các thí nghiệm so sánh với phương pháp bit ít quan trọng nhất (LSB) cho thấy tính bền vững vượt trội của kỹ thuật miền tần số được đề xuất trước các cuộc tấn công như nén, nhiễu và thao tác hình ảnh. Giải pháp được đề xuất củng cố việc bảo vệ bản quyền, nâng cao tính minh bạch trong việc truy vết nguồn gốc NFT và cung cấp nền tảng có thể mở rộng cho việc quản lý tài sản kỹ thuật số an toàn trong các hệ sinh thái dựa trên blockchain.

Từ khóa

Blockchain (chuỗi khối); NFT (token không thể thay thế); bảo vệ bản quyền; truy xuất nguồn gốc; thủy vân số; IPFS (hệ thống tệp liên hành tinh).