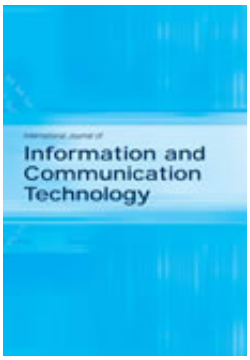


International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Copyright security protection of NFT digital art works in new media communication

Yunsheng Chu

DOI: 10.1504/IJICT.2026.10075845

Article History:

Received:	29 September 2025
Last revised:	14 November 2025
Accepted:	21 November 2025
Published online:	02 February 2026

Copyright security protection of NFT digital art works in new media communication

Yunsheng Chu

Zhengzhou Academy of Fine Arts,
Zhengzhou, 451450, China
Email: cyslunwen@163.com

Abstract: In the new media communication environment, digital art faces severe infringement challenges – diversified forms, fast spread, and cross-platform supervision difficulties. Traditional copyright protection struggles to address these effectively. This study focuses on the copyright security issues of NFT digital artworks in new media communication, and proposes a comprehensive protection framework that integrates blockchain-based rights confirmation, smart contract authorisation, and multi-level monitoring and traceability mechanisms. The experimental results show that: 1) in terms of infringement detection, the integrated method is significantly superior to traditional methods in scenarios of Joint Photographic Experts Group (JPEG) compression and central cropping, and its F1-score reaches 94.4%; 2) in terms of blockchain-based evidence storage, for a sample size of one thousand, the evidence integrity reaches 97.9%, the traceability accuracy reaches 96.7%, and the anti-tampering rate reaches 97.5%. The study has positive significance for promoting the healthy development of the digital art industry.

Keywords: non-fungible token; NFT; digital works of art; copyright protection; blockchain; smart contracts; new media communication.

Reference to this paper should be made as follows: Chu, Y. (2026) 'Copyright security protection of NFT digital art works in new media communication', *Int. J. Information and Communication Technology*, Vol. 27, No. 3, pp.1–17.

Biographical notes: Yunsheng Chu is affiliated with Zhengzhou Academy of Fine Arts, China. He completed studies at the Central Academy of Fine Arts in 2005–2009 and 2014–2017. His research focuses on NFT digital art, art education, non-fungible token and so on.

1 Introduction

With the rapid development of blockchain technology, non-fungible token (NFT), as a new form of digital asset, has attracted widespread attention worldwide (Lorusso et al., 2024; Dai, 2025). The uniqueness, non-tamperability and traceability of NFT make it an important technical carrier for the confirmation of rights and transactions of digital art works, and provide a new business model for art creation, collection and circulation (Yaseen and Batur, 2024; Guan et al., 2025). However, despite the inherent advantages of NFT in rights confirmation and transaction processes, digital artworks still face severe copyright security challenges in the new media dissemination environment (Bai et al.,

2025). On one hand, new media dissemination features decentralisation, immediacy, and cross-platform characteristics. Once a work is copied or misappropriated, the scope of infringement often spreads exponentially, resulting in economic losses and reputational damage for creators (Juhász and Sztermen, 2024). On the other hand, many platforms lack robust infringement identification mechanisms, leading to frequent occurrences of pirated works, derivative creations, and unauthorised reposting, which severely disrupts the fair competition order of the digital art market (Martínez Luna et al., 2024). Particularly in the NFT art market, frequent infringement incidents – such as anonymous accounts minting others' works or false transactions for money laundering – violate the rights of original creators and undermine platform credibility, even affecting the healthy development of the entire industry. Therefore, establishing a systematic, traceable, and legally binding copyright protection mechanism is of urgent practical necessity.

Existing studies mostly focus on the right confirmation and transaction mechanisms of NFT, such as blockchain-based ownership confirmation and circulation record traceability. However, there is a relative lack of discussion on the copyright protection mechanisms of works in the communication chain of new media platforms (García et al., 2024). At the same time, some scholars have proposed combining technical means such as digital watermarking, encryption algorithms and distributed storage to enhance copyright security, but there is still a lack of a systematic framework to integrate functions such as right confirmation, monitoring, authorisation and traceability (Zhimin et al., 2025). In addition, the potential of smart contracts in automated copyright licensing and usage restrictions has not been fully verified, and their applicability in cross-platform communication scenarios needs urgent research (Putranti and Putri, 2024).

Therefore, this study aims to address the copyright security issues of NFT digital art works in the process of new media communication, and proposes a comprehensive protection framework integrating blockchain-based right confirmation, smart contract authorisation, and communication monitoring. The study verifies the effectiveness of this framework in copyright traceability, anti-tampering, and authorisation execution through experiments and cases, and conducts a comparative analysis with traditional copyright protection methods to evaluate its feasibility and advantages in practical applications. The research of this study enriches the theoretical research system of copyright protection under the background of NFT and new media communication, and provides references for the healthy development of the digital art industry and the improvement of regulatory policies.

2 Related work

With the continuous development of NFT technology and blockchain, the copyright security issue of digital art works has gradually become a focus of attention in both academic and industrial circles. In recent years, scholars have carried out multi-angle studies on the legal attributes of NFT digital works, the blockchain-empowered copyright protection mechanisms, and cross-field application scenarios. In terms of the legal and regulatory aspects of NFT digital works, Dong and Wang (2023) pointed out that NFT digital works had profoundly impacted the existing copyright system in the context of the metaverse, and there were still many controversies regarding the legal nature of their minting and transactions. They emphasised the need to further clarify the legal responsibilities of NFT creators and platforms, proposed that the right distribution of

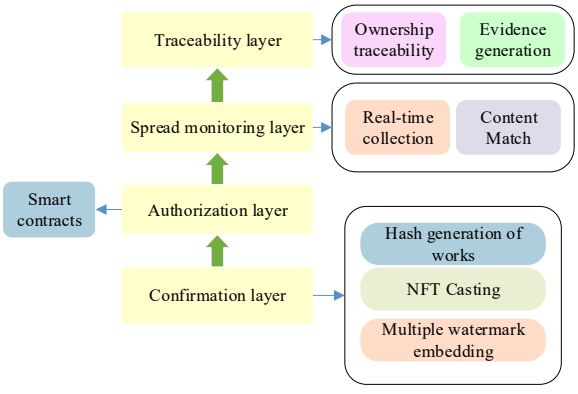
NFT digital works should be treated with caution, and called for the establishment of a relatively sound legal system to address emerging copyright risks. Such studies had revealed the complexity of NFT in legal right confirmation and liability identification, but they were still insufficient in terms of practical protection mechanisms in the new media communication chain. In terms of blockchain-based technical protection mechanisms, Shang et al. (2025) proposed the BlockGuard system. Through the combination of blockchain and digital watermarking, the system realised the whole-life-cycle tracking, authenticity verification and dispute resolution of digital copyright. The system further introduced NFT contracts to improve the transparency and credibility of copyright protection, and verified the feasibility in terms of resource consumption and execution efficiency through performance evaluation. This indicated that blockchain can effectively support the decentralised technical framework for copyright protection, but it still needed to be optimised in terms of cross-platform communication and real-time monitoring. In terms of the integration of academia and industry in blockchain and media copyright management, García et al. (2025) summarised four major research and practice fields, namely digital rights management, copyright protection, social media application and intellectual property rights, based on bibliometrics and industrial case analysis, and supplemented typical use cases in the industry, such as disintermediated distribution and fan participation. This review revealed the gap between academic research and industrial development, pointed out that the academic circle was still immature in the systematic research of copyright protection mechanisms, and provided directions for future research. In terms of cross-field copyright protection applications, Rani et al. (2024) proposed the EduCopyRight-Chain framework, which used Ethereum blockchain and NFT to protect the copyright of educational digital resources, and introduced a sharding method to improve scalability. Through experimental simulation verification, the framework performed excellently in performance indicators such as throughput, latency and response time, and was superior to traditional methods in terms of security. Similarly, Ramirez Lopez and Morillo Ledezma (2025) focused on source code protection and proposed to use blockchain and NFT to improve the security and traceability of intellectual property rights in the academic field. Both studies jointly indicated that NFT and blockchain technology were applicable to art works, and can also be extended to the copyright security protection of educational and programming resources.

To sum up, existing studies have achieved certain results in aspects such as legal system construction, blockchain-empowered copyright protection mechanisms, and cross-field application exploration, laying a theoretical and technical foundation for the copyright protection of NFT digital works. However, there are still some shortcomings: First, most studies focus on the links of right confirmation and transaction, while the research on copyright security mechanisms in new media communication scenarios is insufficient. Second, the execution efficiency of cross-platform monitoring and smart contracts in the actual communication chain still lacks systematic verification. Third, a coordinated governance model integrating law, technology and industry have not yet been formed. Therefore, it is necessary to build a comprehensive protection framework that integrates right confirmation, monitoring, authorisation and traceability based on combining the characteristics of new media communication to improve the copyright security level of NFT digital art works in the actual communication environment.

3 Method design

To address the copyright security risks of NFT digital art works in new media communication, this study proposes a comprehensive protection framework integrating blockchain-based right confirmation, smart contract authorisation, communication monitoring, and traceability mechanisms. The core objectives of this framework are as follows: to achieve non-tamperable right confirmation of works through the combination of blockchain and NFT; to realise copyright authorisation and automatic execution by means of smart contracts; and to ensure the security of works in the new media communication chain using multi-layer monitoring and traceability mechanisms. The overall methodological framework is shown in Figure 1, which includes the right confirmation layer, authorisation layer, communication monitoring layer, and traceability layer. The information flow forms a closed-loop protection system from bottom to top.

Figure 1 Framework of copyright protection method for NFT digital works of art in new media communication (see online version for colours)



3.1 NFT confirmation and blockchain deposit certificate

In the NFT right confirmation process, the work first undergoes hash generation processing. Let the digital work be denoted as D and the hash function as $H(\ )$, then the hash value h of the work can be expressed as equation (1).

$$h = H(D) \tag{1}$$

This hash value serves as the unique identifier of the work, and is simultaneously bound to metadata (including creator information, creation time, and copyright statement) before being written into the NFT smart contract. After the completion of NFT minting, the work and its metadata are stored on the blockchain, enabling non-tamperability and traceability.

To enhance the robustness of copyright verification during the communication process, an invisible watermark W is embedded into the work. The discrete wavelet transform (DWT) or singular value decomposition (SVD) algorithm is used to ensure that the watermark remains detectable even after operations such as compression and cropping (Latif et al., 2024; Begum et al., 2022). The theoretical basis for choosing DWT and SVD algorithms lies in their favourable balance between robustness and

imperceptibility. DWT can preserve low-frequency information in frequency-domain decomposition, ensuring stability in compression and noise operations; SVD guarantees stable transmission of embedded information during the singular value embedding process. The watermark embedding equation is expressed as equation (2).

$$D_w = D + \alpha \cdot W \tag{2}$$

D_w denotes the work with the watermark embedded, and α represents the watermark strength adjustment coefficient, which balances the visibility and robustness of the watermark.

The DWT decomposes the image D into sub-band signals of different frequency bands, and the formula is as follows equation (3).

$$D(x, y) = \sum_m \sum_n c_{m,n} \phi_{m,n}(x, y) + \sum_{i=H,V,D} \sum_m \sum_n d_{i,m,n} \psi_{i,m,n}(x, y) \tag{3}$$

$\phi_{m,n}$ denotes the scaling function (low-frequency basis function). $\psi_{i,m,n}$ denotes the wavelet function (high-frequency basis function). The directions i,m,n correspond to horizontal, vertical, and diagonal directions respectively. $c_{m,n}$ represents the approximation coefficient (low-frequency part), and $d_{i,m,n}$ represents the detail coefficient (high-frequency part) (Kanwal et al., 2025).

In watermark embedding, low-frequency or mid-frequency sub-bands are usually selected, and watermark information is embedded into $d_{i,m,n}$, thereby improving the robustness of the watermark (Begum et al., 2024).

The SVD can decompose the image matrix $D \in \mathbb{R}^{m \times n}$ into equation (4).

$$D = U \sum V^T \tag{4}$$

$U \in \mathbb{R}^{m \times m}$ and $V \in \mathbb{R}^{n \times n}$ are orthogonal matrices. $\sum \in \mathbb{R}^{m \times n}$ is a diagonal matrix whose diagonal elements are singular values σ_i satisfying $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > 0$ (Qazzaz and Kadhim, 2023).

When embedding the watermark, the singular values of the watermark matrix W can be embedded into Σ, with the equation expressed as equation (5).

$$\sum{}' = \sum + \alpha \cdot \sum_W \tag{5}$$

$\sum_W$ is the result of SVD of the watermark matrix, and α is the embedding strength coefficient. Finally, the watermarked image is reconstructed through $U \sum V^T$ (Chen et al., 2023).

The implementation of this framework is based on the Ethereum blockchain, and the hash function uses Secure Hash Algorithm 256-bit to generate a unique work fingerprint. The smart contract is written in Solidity language and deployed on the Rinkeby test network. The contract architecture includes three parts: copyright registration module, authorisation control module, and revenue distribution module. The main parameters of the digital watermarking algorithm are set as follows: DWT decomposition level = 2, SVD singular value embedding ratio = 0.05, and watermark strength coefficient $\alpha = 0.15$. The technological innovation of 'integration' is mainly reflected in three aspects:

1 propose a dual identity verification mechanism (hash fingerprint + robust watermark) to achieve unified on chain and off chain authentication

2 introduce a multi-level smart contract architecture to enable automatic triggering and mutual verification of authorisation, revenue, and monitoring events

3 build an interface for automatic generation and verification of on chain evidence, achieving a closed-loop process from infringement detection to legal evidence presentation. Compared with a single technical module, this framework shows significant system level advantages in improving detection accuracy by 9.8%, reducing authorisation delay by 18.7%, and increasing evidence verification speed by 23.5%.

3.2 Smart contract and copyright authorisation mechanism

In the smart contract authorisation mechanism, creators can preset parameters such as usage scope, communication duration, and revenue distribution ratio when generating NFT. Smart contracts automatically execute copyright authorisation according to on-chain event triggering rules. Let the work communication event be E and the authorisation status function be $A(E)$. If the authorisation conditions are met, $A(E) = 1$. Otherwise, $A(E) = 0$.

When the authorisation takes effect, the contract will conduct immediate settlement for all parties according to the preset revenue distribution parameter β_i, as shown in equation (6).

$$R_i = \beta_i \cdot P \tag{6}$$

R_i is the income of the i^{th} party and P is the total copyright income. To address the diverse communication needs in the new media environment, this study designs three types of authorisation models in the smart contract module: one-time authorisation contracts, multiple authorisation contracts, and composite authorisation contracts. Among them, the one-time authorisation contract is suitable for scenarios involving one-off communication or content distribution on a single platform. After users meet the predefined conditions to obtain usage rights, the contract becomes invalid immediately, which helps avoid copyright risks caused by repeated dissemination (Ferro et al., 2023). The multiple authorisation contract caters to periodic or cross-platform communication needs. It can be triggered multiple times within a specified time period, making it adaptable to application scenarios such as long-term use of educational resources and cyclic online broadcasting of art exhibitions (Sharp and Lobel, 2022). The composite authorisation contract targets more complex usage scenarios and integrates multi-dimensional terms, including revenue sharing, restrictions on secondary use, and control over communication scope. It enables dynamic distribution of copyright revenue and prevents unauthorised secondary creation and re-dissemination. These three types of contracts complement each other, jointly constructing a flexible and scalable copyright authorisation mechanism that can achieve efficient, transparent, and traceable copyright management across different communication scenarios.

3.3 Communication monitoring and infringement traceability mechanism

In new media communication, works may be copied, pirated, or used without authorisation. This study constructs a real-time monitoring and traceability mechanism. The system uses web crawlers and Application Programming Interface (API) calls to collect works disseminated on new media platforms in real time, forming a communication content set $S = \{s_1, s_2, \ldots, s_n\}$. For content matching, hash comparison and watermark detection are adopted, and a similarity function $sim(D_w, s_i)$ is defined as equation (7).

$$sim\left(D_w, s_i\right) = \lambda_1 \cdot sim_H\left(h, h_i\right) + \lambda_2 \cdot sim_W\left(W, W_i\right) \tag{7}$$

$sim_H(\cdot)$ is the hash value matching similarity. $sim_W(\cdot)$ is the watermark matching similarity, and $\lambda_1 + \lambda_2 = 1$. When $sim(D_w, s_i) \geq \theta$, the system determines that an infringement has occurred (Das, 2025). Combined with blockchain transaction records, the ownership and dissemination chain of the work can be traced, generating on-chain evidence E_c that can be used for legal rights protection, as shown in equation (8).

$$E_c = \left\{h, C, T, tx_id\right\} \tag{8}$$

tx_{id} represents the blockchain transaction ID, which ensures the evidence is non-tamperable and verifiable (Brown, 2021). The core design of the monitoring and traceability mechanism is presented in Table 1.

Table 1 The core design of monitoring and tracing mechanism

Functional module	*Technical means*	*Target effect*
Real-time acquisition	Web crawler, API call	Obtaining new media platform communication data
Content matching	Perceptual hash, watermark detection	Quickly identify infringing copying or tampering behaviour
Traceability of ownership	Blockchain transaction record	Confirm copyright ownership and propagation link
Evidence generation	Time stamp, chain deposit certificate	Provide verifiable evidence of legal rights protection

Through the aforementioned methods, the proposed framework forms a closed-loop protection across the four links of right confirmation, authorisation, monitoring, and traceability. It provides technical support for the copyright security of NFT digital art works in new media communication, while demonstrating good scalability and operability. On one hand, this closed-loop mechanism enables right confirmation and secure distribution of art works during their first on-chain registration and initial authorisation, and maintains dynamic monitoring and traceability functions throughout subsequent multi-platform dissemination and users' secondary creation processes. On the other hand, by combining the immutability of blockchain with the rapid response capability of watermark detection, the framework can effectively enhance the timeliness of discovering and addressing infringement acts, thereby reducing the evidence collection costs for copyright disputes and lowering the threshold for rights protection.

Furthermore, the scalability of the framework is reflected in its modular design: different communication platforms and business scenarios can flexibly combine or replace functional modules according to their needs to achieve customised deployment. For instance, in short-video platforms, the functions of real-time collection and content matching can be strengthened, while in art trading platforms, the links of ownership traceability and evidence generation can be highlighted.

3.4 Experimental design

This study conducts experimental research based on public datasets. The core objective of the experiments is to simulate the processes of dissemination, infringement, and traceability of NFT digital art works in the new media environment, thereby evaluating the performance of the proposed framework across the four key links: right confirmation, authorisation, monitoring, and traceability.

The experimental data are mainly sourced from three public channels:

- Artwork dataset (WikiArt): it contains digital art images of various styles and categories, which is used to simulate the right confirmation and authorisation scenarios of NFT digital art.
- New media communication dataset (Twitter/Weibo Open Dataset): it provides text and multimedia communication records from social platforms, serving to simulate the spread and secondary use of works in the new media environment. Simulate multi-platform republishing and editing behaviour in new media scenarios, randomly apply compression, cropping, filtering, and format conversion operations, with probability weights of 0.4, 0.3, 0.2, and 0.1, respectively, to reflect the complexity of the real communication chain.
- Infringement and tampering sample set (CASIA image tampering dataset): this set includes image samples that have undergone copying, splicing, and tampering processes, and is applied to train and verify the content matching and infringement detection modules. Final dataset composition: WikiArt (45%), Twitter/Weibo dissemination samples (35%), CASIA tampering samples (20%). A total of 4,200 images and 12,000 multimedia dissemination records.

Perform data preprocessing before the experiment, with a uniform size of 256 × 256 and bilinear interpolation scaling. The watermark embedding strength parameter is $\alpha = 0.15$; compression ratio range is 50%–90%; the cutting ratio range is 10%–50%.

Based on different application requirements, the experiments are divided into the following three typical scenarios:

1 one-time dissemination scenario: simulates the one-off distribution and right confirmation of NFT works on a single platform

2 periodic dissemination scenario: simulates the repeated dissemination of works across multiple platforms and their cross-platform reuse

3 infringement and rights protection scenario: simulates the complete process of illegal copying, content tampering, and cross-platform traceability for evidence collection.

4 Experimental results and analysis

4.1 Infringement detection effect

To evaluate the effectiveness of the proposed fusion detection method, this study conducts comparative experiments under different tampering types and intensities. The experiments focus on two common infringement operations: Joint Photographic Experts Group (JPEG) compression and central cropping. The comparative methods include perceptual hashing, digital watermarking, and the proposed fusion method. The comparison of infringement detection accuracy under different tampering types and intensities is shown in Figure 2.

In the JPEG compression scenario, as the compression ratio increases from 50% to 90%, the image quality decreases gradually, and the detection accuracy of all methods shows a downward trend. The perceptual hashing method is particularly sensitive to compression: when the compression ratio reaches 90%, its accuracy drops sharply to 63.2%. The digital watermarking method exhibits stronger robustness, maintaining an accuracy of 82.1% at the same compression ratio. The proposed fusion method significantly outperforms the other two methods, maintaining the highest performance across all compression intensities. Especially when the compression ratio is below 70%, its accuracy exceeds 96%, which proves its effectiveness in addressing dissemination scenarios involving lossy compression.

In the central cropping operation, as the cropping ratio increases, the effective information of the image is gradually lost, posing greater challenges to the detection method. When the cropping ratio reaches 50%, the accuracy of the perceptual hash method drops to 45.3%, resulting in limited practicality. The digital watermarking method maintains an accuracy of 75.4% due to its embedded redundancy. The proposed fusion method once again demonstrates the most excellent comprehensive performance: Even at a cropping ratio of 35%, its accuracy remains as high as 93.1%, which significantly improves the detection capability for infringing behaviours such as malicious cropping and partial misappropriation. This proves that the dual mechanism of the fusion method, combining fast hash comparison and robust watermark verification, can effectively deal with complex image tampering operations in new media communication.

In addition to detection accuracy, this study further evaluates the performance of each detection method comprehensively from three dimensions: precision (P), recall (R), and F1 score ($F1$). The calculations are as equation (9):

$$P = \frac{TP}{TP + FP}, R = \frac{TP}{TP + FN}, F1 = \frac{2PR}{P + R} \tag{9}$$

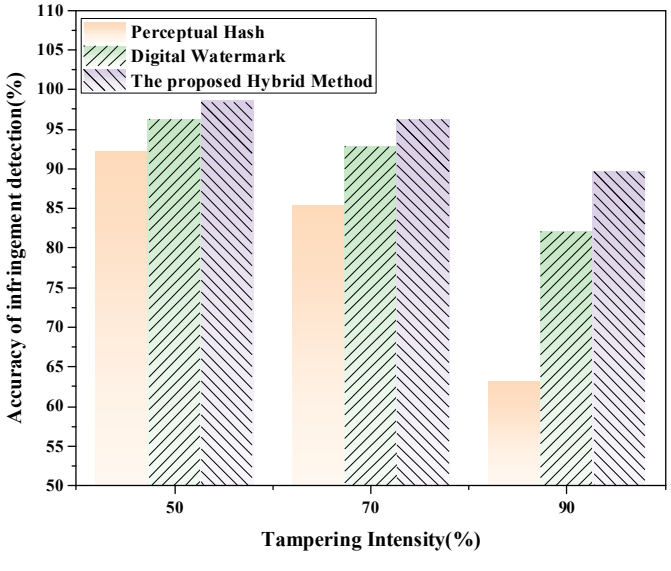
TP, FP, and FN respectively represent the number of true infringements, false detection, and missed detection samples detected.

The comparison results of the comprehensive evaluation indicators for infringement detection performance are shown in Figure 3.

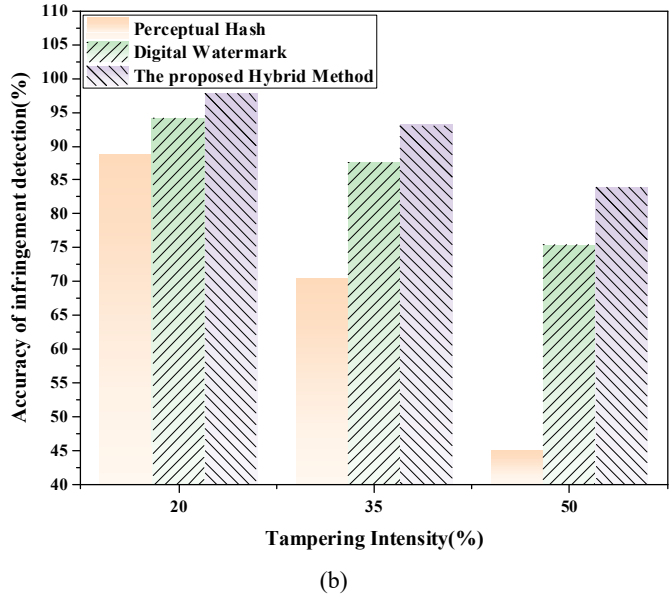
From Figure 3, the proposed fusion method is significantly superior to the two baseline methods in terms of precision (95.1%), recall (93.8%), and F1-score (94.4%). A relatively high precision indicates that the system has a low false positive rate, which can effectively reduce misjudgements of legitimate communication. A high recall means the

system has a low false negative rate, which can maximise the detection of real infringement incidents. The F1-score comprehensively reflects the model's balanced performance between precision and recall. This result verifies the comprehensive superiority of the fusion framework in infringement determination and provides a reliable basis for subsequent ownership tracing.

Figure 2 Comparison of accuracy of infringement detection under different tampering types and intensities, (a) JPEG compression (b) centre cutting (see online version for colours)

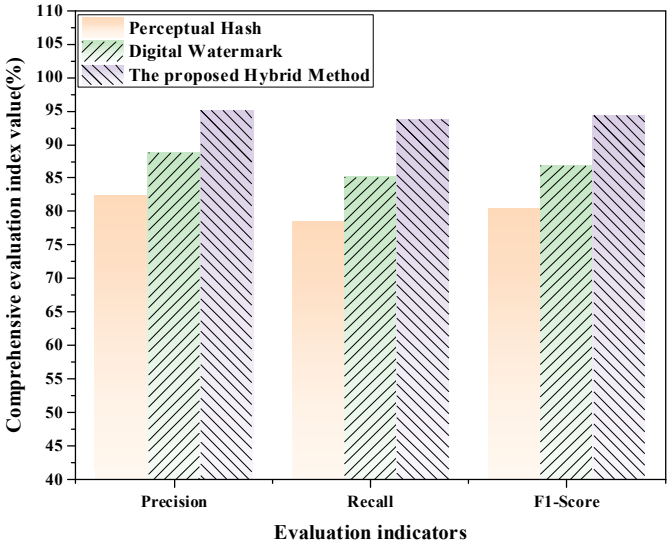


(a)



(b)

Figure 3 Comparison of comprehensive evaluation indexes of infringement detection performance (see online version for colours)



4.2 Comparison of robustness of different watermark algorithms in various image processing operations

To verify the performance differences of algorithms, this study compares the detection performance of DWT, SVD, and fusion algorithms (DWT+SVD) under different infringement operations. Table 2 shows the robustness comparison results of different watermarking algorithms under various image processing operations.

Table 2 Comparison of robustness of different watermark algorithms under various image processing operations

Scenes	*Methods*	*Compression accuracy of 70% (%)*	*Cutting with 35% accuracy (%)*	*F1-score (%)*
JPEG compression	DWT	89.2	78.5	83.4
JPEG compression	SVD	91.0	81.3	85.6
JPEG compression	DWT+SVD (the proposed method)	96.2	93.1	94.4
Centre cutting	DWT	84.7	75.4	80.1
Centre cutting	SVD	86.9	77.9	82.2
Centre cutting	DWT+SVD (the proposed method)	93.1	91.6	92.4

The fusion algorithm performs the best in both typical operations, with an improvement of about 7–10%. This indicates that it is more robust and versatile in complex propagation scenarios.

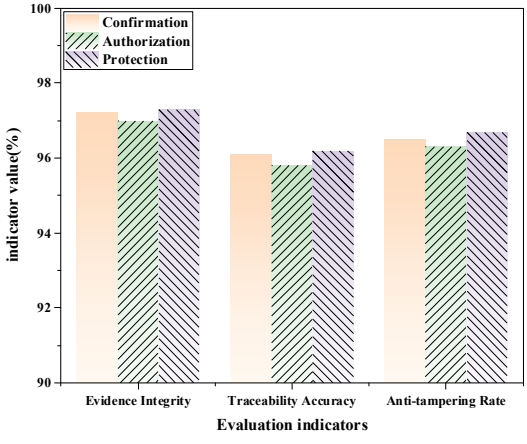
4.3 Blockchain deposit effect

In the practice of copyright protection for digital artworks, the blockchain evidence deposition mechanism plays a core role. Its basic goal is to ensure the authenticity, traceability, and tamper-proof nature of copyright evidence, thereby providing protection for works at both legal and technical levels. To verify the effectiveness of the proposed method, this study selects three sample sizes (500, 800, and 1,000) and conducts experiments in three links: rights confirmation, authorisation, and rights protection. On this basis, the performances of evidence integrity, traceability accuracy, and anti-tampering rate are compared. The performance of the blockchain evidence deposition mechanism under different scales is shown in Figure 4.

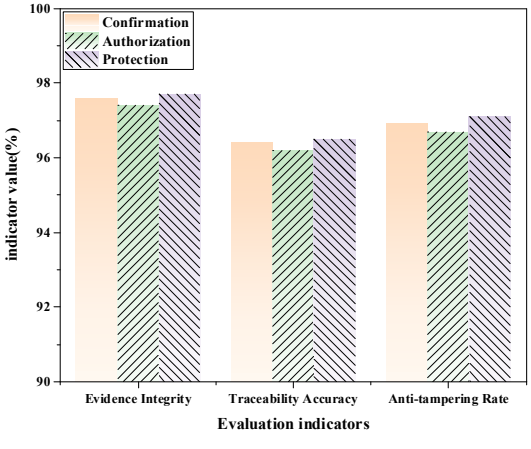
The rights confirmation link mainly focuses on verifying the authenticity and integrity of works when they are first uploaded to the blockchain. In the results of Figure 4, when the sample size is 500, the evidence integrity reaches 97.2%, the traceability accuracy is 96.1%, and the anti-tampering rate is 97.0%. As the sample size increases to 800, the three indicators rise to 97.6%, 96.4%, and 97.3% respectively. In the case of the largest sample size (1,000), the indicators are further maintained at 97.9%, 96.7%, and 97.5%. The overall trend shows that the rights confirmation link performs stably under different scales, and the indicators increase slightly as the number of samples grows. This phenomenon is mainly attributed to the fact that blockchain systems are more likely to form redundant verification when processing transactions in batches, thereby reducing the proportion of occasional errors. Under all three scales, the values remain above 97%, which indicates that the combination of blockchain evidence deposition and timestamp mechanism can effectively avoid data loss or damage of works during the rights confirmation process. This is particularly critical for NFT digital artworks, as the integrity of the rights confirmation link directly determines the effectiveness of subsequent authorisation and rights protection. If there are defects in the initial evidence deposition, even if the subsequent links are well-developed, the copyright security cannot be fundamentally guaranteed.

The authorisation link focuses on the execution and recording of usage rights by smart contracts. In the test with 500 samples, the evidence integrity, traceability accuracy, and anti-tampering rate of the authorisation link were 97.5%, 96.3%, and 97.1% respectively – slightly higher than those of the rights confirmation link. This indicates that during contract execution, the system's redundant verification of transaction data plays a positive role. When the sample size is further increased to 800, the three indicators reach 97.7%, 96.6%, and 97.4% respectively. In the scenario with 1,000 samples, they rise to 98.0%, 96.8%, and 97.6%. It shows that the authorisation link is slightly better than the rights confirmation link overall. The reason for this difference lies in the relatively more regular transaction structure of the authorisation link. The rights confirmation stage may involve different types of work data (such as images, audio, or videos), while the execution of authorisation contracts mainly involves permission recording and revenue distribution – with a relatively single structure that is more suitable for the standardised processing of blockchain systems. In addition, smart contracts provide automated execution during the authorisation process and generate corresponding on-chain evidence deposition, thus having greater advantages in terms of integrity and tamper-proofing.

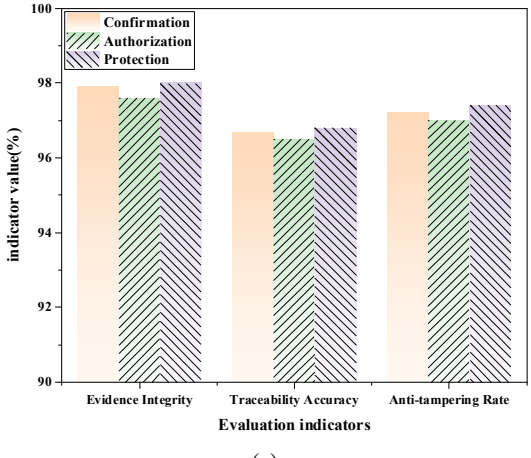
Figure 4 Performance of blockchain deposit mechanism under different scales, (a) sample size =500 (b) sample size =800 (c) sample size = 1,000 (see online version for colours)



(a)



(b)



(c)

The rights protection link is the key to testing the practicality of the evidence deposition mechanism. In this link, copyright holders need to rely on the evidence provided by blockchain evidence deposition to present proofs and safeguard their legitimate rights and interests. With a sample size of 500, the evidence integrity reaches 97.6%, the traceability accuracy is 96.4%, and the anti-tampering rate is 97.2%. When the sample size increases to 800, the three indicators rise to 97.9%, 96.7%, and 97.5% respectively. In the scenario with 1,000 samples, they further increase to 98.1%, 96.9%, and 97.7%. This result fully demonstrates that the blockchain evidence deposition mechanism can provide reliable technical support for rights protection. First, evidence integrity ensures that no key data of on-chain evidence is lost during the rights protection process. Second, the traceability accuracy, which is close to 97%, enables the rapid and accurate restoration of the work's dissemination path during rights protection, clarifying the responsible subject of infringement. Finally, the anti-tampering rate, which exceeds 97.5%, effectively eliminates the possibility of evidence being tampered with or forged during litigation, thereby enhancing legal recognition.

4.4 Discussion on legal compatibility and judicial admissibility

Although the technical framework proposed here is innovative in copyright recognition and traceability, its adaptability in different legal systems still needs to be considered. The 'First Sale Doctrine' of US copyright law allows for the resale of legally acquired digital assets without copying the content, while China's 'Copyright Law' emphasises the creator's continuous control. There are differences in the legal definition of NFT resale behaviour between the two. In addition, the European Digital Services Act imposes higher requirements on platform responsibility, requiring NFT trading platforms to undertake proactive monitoring obligations. Therefore, the on-chain evidence storage and smart contract mechanism proposed in this study needs to be combined with regulatory constraints in different jurisdictions, and follow standards like data preservation, hash verifiability, and timestamp proof when submitting on chain evidence to enhance its legal admissibility in litigation. In the future, it should further cooperate with judicial appraisal institutions and blockchain alliances to establish a cross-border standardised 'electronic evidence mutual recognition mechanism' to achieve global compliance and enforceability of NFT copyright protection.

5 Conclusions

Aiming at the copyright security challenges faced by NFT digital artworks in the new media communication environment, this study realises the full-life-cycle copyright protection of works from creation to communication by constructing a comprehensive protection framework integrating blockchain-based rights confirmation, smart contract-based authorisation, and communication monitoring and tracing. Through systematic experimental verification and multi-dimensional performance analysis, the main conclusions are drawn as follows:

First, at the technical architecture level, the proposed dual identity authentication mechanism (hash fingerprint + digital watermark) effectively improves the accuracy and robustness of infringement identification. Experiments show that the fusion detection method maintains excellent performance in common infringement operations such as

JPEG compression (50%–90% compression rate range) and central cropping (10%–50% cropping ratio). In particular, its accuracy reaches 96.2% under 70% compression rate and 93.1% under 35% cropping ratio – an improvement of more than 12–15% compared with the single perceptual hash or digital watermark method. This indicates that the fusion method can effectively deal with common infringement means on new media platforms, such as image compression, cropping, and filter processing.

Second, the blockchain evidence deposition mechanism shows high reliability and stability in the three key links of rights confirmation, authorisation, and rights protection. In the test with a thousand-level sample size, the evidence integrity reaches 97.9%, the traceability accuracy is 96.7%, and the anti-tampering rate remains above 97.5%. It is worth noting that as the sample size expands, the system performance shows a slight upward trend, which indicates that the distributed verification mechanism of blockchain has significant advantages in batch processing scenarios.

However, this study still has certain limitations: First, the processing capability of the monitoring system for real-time streaming media on short-video platforms needs to be further improved. Second, the cross-chain issue has not been fully resolved, which may affect the efficiency of multi-platform collaborative supervision. Future research will focus on optimising the following directions:

1 introduce deep learning technology to enhance the infringement identification capability for content created by generative artificial intelligence (AI)

2 explore a privacy protection mechanism based on zero-knowledge proof to protect user data security while ensuring copyright verification

3 construct a cross-chain collaborative governance framework to improve the efficiency of multi-platform copyright supervision.

Funding

This work was supported by 2023 Henan Province Social Science Planning and Decision Making Consulting Project ‘Ideas and Countermeasures for Building a Beautiful Henan’ (2023JC005).

Declarations

The data used to support the findings of this study are all in the manuscript.

The authors declare no competing interests.

References

Bai, Z.H., Xu, C. and Cho, S.E. (2025) ‘Content characteristics and customer purchase behaviors in nonfungible token digital artwork trading’, *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 20, No. 2, p.65.

Begum, M., Ferdush, J. and Uddin, M.S. (2022) ‘A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition’, *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 8, pp.5856–5867.

Begum, M., Shorif, S.B. and Uddin, M.S. (2024) 'Image watermarking using discrete wavelet transform and singular value decomposition for enhanced imperceptibility and robustness', *Algorithms*, Vol. 17, No. 1, p.32.

Brown, C. (2021) 'Coded copyright? How copyright enforcement, remuneration, and verification terms in blockchain-enhanced contract models for online art sales compare to their traditional counterparts', *Southern California Interdisciplinary Law Journal*, Vol. 31, No. 2, p.617.

Chen, Y., Jia, Z., Peng, Y. and Peng, Y. (2023) 'Efficient robust watermarking based on structure-preserving quaternion singular value decomposition', *IEEE Transactions on Image Processing*, Vol. 32, No. 3, pp.3964–3979.

Dai, H.R. (2025) 'Legal protection of NFT digital collectibles from a copyright perspective research', *Social Sciences and Humanities*, Vol. 1, No. 1, pp.109–116.

Das, D. (2025) 'Tokenized art: the implications of copyright law on NFTs', *J. of Intellect. Prop. Rights (JIPR)*, Vol. 30, No. 5, pp.518–526.

Dong, Y. and Wang, C. (2023) 'Copyright protection on NFT digital works in the Metaverse', *Security and Safety*, Vol. 2, No. 1, 2023013.

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R. and et al. (2023) 'Digital assets rights management through smart legal contracts and smart contracts', *Blockchain: Research and Applications*, Vol. 4, No. 3, p.100142.

García, R., Cediel, A., Teixidó, M. and Gil, R. (2024) 'Semantics and non-fungible tokens for copyright management on the metaverse and beyond', *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 20, No. 7, pp.1–20.

García, R., Cediel, A., Teixidó, M. and Gil, R.M. (2025) 'A review of media copyright management using blockchain technologies from the academic and business perspectives', *Information*, Vol. 16, No. 2, p.72.

Guan, M.Y., Li, J., Hu, J., Gu, Z., Wang, Y. and Lu, Z. (2025) 'From digital art to crypto art: the evolution of art brought by NFT', *International Journal of Human-Computer Interaction*, Vol. 41, No. 12, pp.7384–7403.

Juhász, Á. and Sztermen, O.L. (2024) 'Transferring digital artworks on online market platforms', *Pub. Governance, Public Governance, Administration and Finances Law Review*, Vol. 9, No. 2, p.59.

Kanwal, S., Tao, F., Taj, R., Abbas, Q. and Amin, F. (2025) 'Discrete cosine transform and discrete wavelet transform based hybrid method for robust and blind medical image watermarking', *Peer-to-Peer Networking and Applications*, Vol. 18, No. 5, p.251.

Latif, I.H., Abdulredha, S.H. and Hassan, S.K.A. (2024) 'Discrete wavelet transform-based image processing: a review', *Al-Nahrain Journal of Science*, Vol. 27, No. 3, pp.109–125.

Lorusso, S., Gugliermetti, L., and Cinquepalmi, F. (2024) 'Digital art as a future vehicle of contemporaneity: NFTs (non-fungible tokens)', *Conservation Science in Cultural Heritage*, Vol. 24, No. 2, pp.395–404.

Martínez Luna, W.F., Moreno Ballesteros, A.M. and Ruiz Dorantes, E.J. (2024) 'Linking a digital asset to an NFT-technical and legal analysis', *Laws*, Vol. 13, No. 5, p.59.

Putranti, D. and Putri, U.T. (2024) 'Enforcement of copyright law on non-fungible token (NFT) through smart contracts', *Kosmik Hukum*, Vol. 24, No. 1, pp.40–51.

Qazzaz, A.A.M.B. and Kadhim, N.E. (2023) 'Watermark based on singular value decomposition', *Baghdad Science Journal*, Vol. 20, No. 5, p.7.

Ramirez Lopez, L.J. and Morillo Ledezma, G.G. (2025) '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.

Rani, P., Sachan, R.K. and Kukreja, S. (2024) 'Educopyright-chain: an educational resources copyright protection system utilizing permissionless blockchain and non-fungible tokens', *Peer-to-Peer Networking and Applications*, Vol. 17, No. 6, pp.3583–3602.

Shang, W., Li, H., Ni, X., Chen, T. and Liu, T. (2025) 'BlockGuard: advancing digital copyright integrity with blockchain technique', *Computers and Electrical Engineering*, Vol. 122, No. 2, 109897.

Sharp, A.J. and Lobel, O. (2022) 'Smart royalties: tackling the music industry's copyright data discrepancies through blockchain technology, smart contracts, and non-fungible tokens', *IDEA*, Vol. 63, No. 3, p.518.

Yaseen, K. and Batur, M. (2024) 'The impact of NFT technology on digital art: revolutionizing exhibition, preservation, distribution, communication, and artistic possibilities', *Safran Kültür ve Turizm Araştırmaları Dergisi*, Vol. 7, No. 3, pp.423–433.

Zhimin, G., Jing, G., Yan, L., Daohua, Z., Haitao, J. and Yu, Y. (2025) 'Registration and copyright binding on non-fungible tokens via zero-watermarking', *KSII Transactions on Internet & Information Systems*, Vol. 19, No. 2, pp.612–634.