Homomorphic Encryption-Based NFT Copyright Protection for Digital Art

Shuang Yang[1,*], Sha Lyu[2], Chunjuan Zhao[1] and Zifeng Luo[1]

[1]*Yibin Vocational and Technical College, Yibin 644000, China*
[2]*City University Malaysia, Petaling Jaya 46100, Malaysia*
E-mail: yangshuang09161989@outlook.com
[*]*Corresponding Author*

Received 15 October 2025; Accepted 17 November 2025

Abstract

The digital art industry faces critical challenges in copyright protection and privacy preservation that existing solutions fail to adequately address. Traditional digital watermarking techniques are vulnerable to removal attacks and cannot prevent unauthorized content access, while current Non-Fungible Token (NFT) platforms expose transaction details and artwork content due to blockchain transparency, creating privacy risks for creators and collectors. Conventional encryption methods require decryption before any data processing, making copyright verification and feature extraction impossible in encrypted states, thus creating a fundamental security-usability trade-off.

To overcome these limitations, this research proposes a network security protection system integrating homomorphic encryption with NFT copyright protection. Homomorphic encryption was selected because it uniquely enables computational operations on encrypted data without decryption, allowing copyright verification while maintaining complete data confidentiality – a capability unmatched by alternative privacy-preserving technologies. The system employs the Cheon-Kim-Kim-Song (CKKS)

Journal of Cyber Security and Mobility, Vol. 14_6, 1413–1446.
doi: 10.13052/jcsm2245-1439.1465

homomorphic encryption algorithm to construct a three-tier protection architecture consisting of an encryption layer, verification layer, and storage layer. This architecture achieves copyright verification and feature extraction of digital artworks in ciphertext state by integrating zero-knowledge proof for identity authentication and Shamir's secret sharing for secure key management. The NFT copyright protection mechanism introduces homomorphic watermark embedding and smart contract verification, combined with proxy re-encryption to implement secure copyright transfer.

A prototype system was developed and evaluated through comprehensive testing. Security performance was assessed using six metrics: privacy protection strength, copyright verification accuracy, anti-tampering capability, key security, transaction anonymity, and system resilience. Each metric was scored on a 0–100 scale based on standardized penetration testing and cryptographic attack simulations, with the comprehensive security score calculated as the weighted average of all metrics. Performance testing on 100 digital artworks across five resolutions (256×256 to 4096×4096 pixels) demonstrates that encryption time for 512×512 resolution images is kept within 15 seconds, while security testing reveals the system achieves a comprehensive security score of 94.7, representing a 60.5% improvement over traditional NFT platforms. This solution provides a practical copyright protection framework balancing security and usability for the digital art industry, with significant theoretical value and broad application prospects.

Keywords: Homomorphic encryption, NFT copyright protection, zero-knowledge proof, blockchain security, digital art privacy.

1 Introduction

The digital art market has experienced explosive growth with the rapid development of blockchain technology and the rise of the metaverse concept [1]. According to statistics, the global Non-Fungible Token (NFT) market transaction volume exceeded $40 billion in 2021. Digital artworks, as the core category, accounted for more than 30% of the market share [2]. This unprecedented growth has created new opportunities for artists and collectors. However, it has also exposed critical security vulnerabilities that threaten the sustainable development of the industry.

The digital art industry faces three fundamental challenges. First, the easy replicability of digital artworks severely restricts healthy industry development [3]. Copyright ownership ambiguity makes it difficult to

effectively protect creators' rights [4]. Second, privacy leakage risks during transactions have increasingly become a focus of industry concern [5]. Artwork piracy has caused enormous economic losses to creators [9]. Third, security threats such as identity forgery have seriously affected collectors' confidence [10].

Traditional copyright protection technologies have proven inadequate for addressing these challenges. Digital watermarking techniques remain vulnerable to removal attacks [6]. Hash verification methods appear insufficient when facing increasingly complex network attacks [7]. Digital art trading platforms frequently encounter data breach incidents [8]. Current mainstream NFT platforms such as OpenSea expose sensitive information of buyers and sellers during transactions [21]. Digital artworks are typically stored on-chain using plaintext or simple hash methods, which cannot effectively prevent unauthorized content acquisition [22].

Recent advances in cryptographic technologies offer potential solutions. Homomorphic encryption, capable of performing computations on encrypted data, has attracted widespread attention in privacy computing since Gentry proposed the first fully homomorphic encryption scheme in 2009 [11]. This technology allows specific operations to be performed directly on encrypted data without decryption, fundamentally ensuring security throughout the entire data processing lifecycle [12]. The Cheon-Kim-Kim-Song (CKKS) algorithm has achieved significant breakthroughs in computational efficiency [13]. The Brakerski-Fan-Vercauteren (BFV) algorithm has laid the foundation for practical applications in real-world scenarios [14]. Zero-knowledge proof technology has been successfully applied in blockchain privacy protection, providing an important reference for digital asset security [15].

However, existing research reveals significant gaps. Current studies mainly focus on privacy computing applications in the financial sector [16]. Research achievements in medical data protection are difficult to directly migrate to digital art scenarios [17]. The construction of security protection systems for digital art, an emerging application domain, remains in the exploratory stage [18]. While NFT technology has provided technical support for digital art copyright verification [19], the transparency characteristics of its underlying blockchain create dilemmas in transaction privacy protection [20]. Academia has recognized the importance of combining advanced cryptographic technologies with digital art protection [23]. Some scholars have proposed solutions based on attribute encryption, but these schemes have limited operational capabilities in encrypted states [24].

Three critical gaps exist in current approaches: (1) Traditional encryption requires decryption before any data processing, making copyright verification impossible in encrypted states. (2) Existing NFT platforms cannot balance copyright protection with transaction privacy due to blockchain transparency. (3) No comprehensive framework integrates homomorphic encryption with NFT copyright mechanisms to enable ciphertext-state operations throughout the entire artwork lifecycle.

This research addresses these gaps by integrating homomorphic encryption with NFT copyright protection. CKKS was selected over alternative homomorphic encryption schemes for three key reasons. First, CKKS supports approximate arithmetic on real numbers, making it ideal for processing continuous data such as image feature vectors and audio spectra in digital artworks. In contrast, BFV is optimized for exact integer arithmetic, which is less suitable for multimedia content processing. Second, CKKS offers superior computational efficiency for machine learning operations required in feature extraction and similarity comparison. Third, CKKS provides better noise management for cascaded operations, enabling complex multi-layer computations without excessive noise accumulation that would compromise accuracy.

Zero-knowledge proof was chosen to complement homomorphic encryption because it enables identity authentication without revealing sensitive information. Proxy re-encryption was selected for secure key transfer during copyright transactions because it allows ciphertext transformation without exposing plaintext or original keys to proxy servers. This combination of technologies creates a comprehensive security framework unmatched by single-technology solutions.

This research aims to construct an innovative security protection system integrating homomorphic encryption technology with digital art NFT copyright protection. The system achieves encrypted-state processing of digital artworks throughout the entire lifecycle from creation, storage, and transaction to verification. The objective is to ensure copyright security while achieving privacy protection, fundamentally resolving the contradiction between security and usability in traditional schemes.

This research makes four primary contributions to the field:

(1) Novel Encryption Architecture: We propose a three-tier protection architecture consisting of encryption layer, verification layer, and storage layer, enabling end-to-end security for digital artworks. This architecture integrates CKKS homomorphic encryption with zero-knowledge proof and Shamir's

secret sharing, providing comprehensive protection that existing systems lack.

(2) Encrypted-State Feature Extraction Algorithm: We develop a homomorphic feature extraction and verification algorithm that enables copyright authentication without revealing original artwork content. This breakthrough allows perceptual hash calculation, similarity comparison, and watermark verification to be performed entirely in ciphertext domain, solving the fundamental limitation of traditional encryption methods.

(3) Privacy-Preserving NFT Copyright Mechanism: We design an integrated NFT copyright protection framework combining homomorphic watermark embedding, smart contract verification, and proxy re-encryption. This mechanism achieves secure copyright transfer while protecting transaction privacy, addressing the transparency-privacy dilemma in existing NFT platforms.

(4) Comprehensive System Validation: We implement a complete prototype system and demonstrate its practical feasibility through systematic testing. Performance evaluation shows encryption time for 512×512 resolution images is kept within 15 seconds, while security testing reveals a comprehensive security score of 94.7, representing 60.5% improvement over traditional NFT platforms.

These contributions not only provide practical security solutions for the digital art industry but also open up new directions for applying cryptographic technology in creative industries, possessing significant theoretical and practical value [25, 26].

2 Security System Design

2.1 Overall Architecture

The network security protection system based on homomorphic encryption proposed in this research adopts a hierarchical design philosophy, constructing a multi-dimensional security protection architecture covering the entire lifecycle of digital art. This architecture uses homomorphic encryption technology as its core, combined with advanced technologies such as zero-knowledge proof, smart contracts, and distributed storage, from the data source to the final application. The overall architecture is functionally divided into three core layers: the encryption layer, verification layer, and storage layer. Each layer achieves loosely coupled interaction through standardized

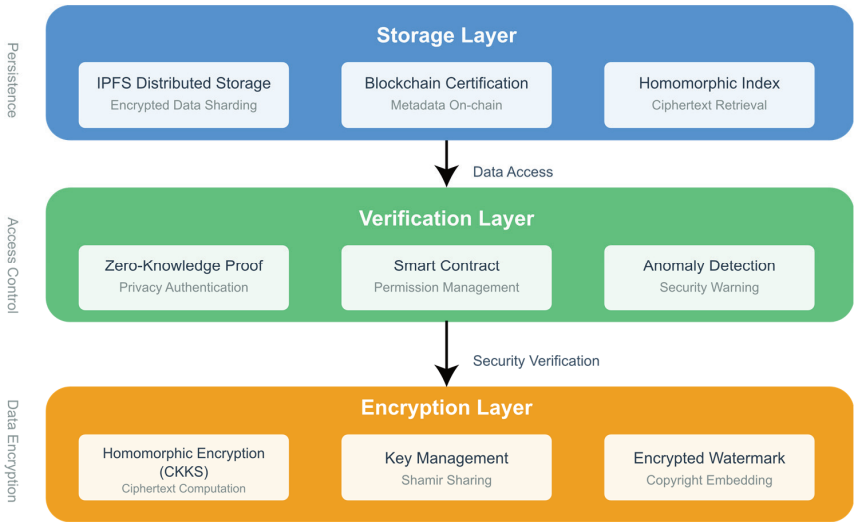


Figure 1 Three-tier architecture achieves secure data flow through standardized interfaces.

interfaces, ensuring both system security and architectural scalability and flexibility.

As shown in Figure 1, the encryption layer is located at the bottom of the architecture and undertakes the core tasks of data encryption and ciphertext computation. This layer employs an improved CKKS homomorphic encryption algorithm to encrypt the raw data of digital artworks, while introducing a key sharding management mechanism that disperses the master key across multiple nodes through Shamir's secret sharing algorithm, effectively preventing single-point key leakage risks. The encryption layer is not only responsible for the encrypted storage of static data, but more importantly supports feature extraction operations in ciphertext state, enabling copyright fingerprints of artworks to be generated within the encryption domain, thus achieving organic unity between privacy protection and copyright authentication. This layer also integrates homomorphic hash functions and encrypted watermark embedding modules, capable of embedding creator identity information and timestamps into ciphertext without compromising the integrity of encrypted data, providing reliable technical support for subsequent copyright tracing.

The verification layer, as the middle layer of the architecture, is primarily responsible for security control functions such as identity authentication, permission management, and transaction verification. This layer introduces

an identity verification protocol based on zero-knowledge proof, allowing users to complete identity authentication without exposing real identity information, effectively protecting the privacy of both transaction parties. The verification layer designs a multi-level permission management mechanism that allocates different operational permissions according to user roles (creators, collectors, platform administrators, etc.), and implements automated management and dynamic adjustment of permissions through smart contracts. In the transaction verification process, this layer employs ciphertext comparison technology to verify the consistency of encrypted artworks submitted by buyers and sellers, ensuring the authenticity and uniqueness of transaction objects. Additionally, the verification layer integrates an anomaly detection module that identifies potential security threats in real-time by analyzing transaction patterns and access behaviors, immediately triggering security warning mechanisms when abnormal operations are detected, effectively enhancing the system's proactive defense capabilities.

The storage layer, located at the top of the architecture, is responsible for persistent storage and efficient retrieval of encrypted data. This layer adopts a hybrid storage architecture, storing encrypted data of digital artworks in sharded form in the IPFS (InterPlanetary File System) distributed file system, while uploading artwork metadata and transaction records to public blockchain platforms such as Ethereum, fully leveraging the high availability of distributed storage and the immutability characteristics of blockchain. To improve the retrieval efficiency of ciphertext data, the storage layer designs an indexing mechanism based on homomorphic encryption, supporting keyword search and similarity matching in ciphertext state, enabling users to quickly locate target artworks without decryption. This layer also implements a hot-cold data separation strategy, caching frequently accessed hot data in high-speed storage devices while archiving historical transactions and other cold data to low-cost storage media, effectively controlling storage costs while ensuring system performance. An access control gateway is established between the storage layer and verification layer, requiring all access requests to encrypted data to undergo permission review by the verification layer, forming a dual guarantee mechanism for data access.

Data interaction among the three layers is conducted through secure communication protocols, with all inter-layer transmitted data encrypted using TLS (Transport Layer Security) channels and appended with digital signatures to prevent man-in-the-middle attacks and data tampering. The architecture also introduces a log audit module that records all operations within the system throughout the entire process, providing a complete chain

of evidence for post-incident security analysis and responsibility tracing. The entire protection system fully considers scalability requirements in its design, with all functional modules implemented using microservice architecture, facilitating flexible addition and removal of functional components according to business development needs. Meanwhile, the architecture reserves standardized external interfaces capable of seamlessly integrating with existing NFT trading platforms and digital asset management systems, reducing technology migration costs and improving the practicality and scalability of the solution.

2.2 Core Technical Solutions

The core technical solution of this research revolves around the innovative application of homomorphic encryption algorithms in digital art copyright protection, focusing on solving the technical bottleneck that traditional encryption technologies cannot process data in ciphertext state. The system employs the CKKS homomorphic encryption algorithm as the fundamental cryptographic tool, which supports approximate computations on encrypted floating-point numbers and is particularly suitable for processing continuous data such as image feature vectors and audio spectra contained in digital artworks. During the algorithm selection process, the research team conducted a comparative analysis of the performance characteristics of mainstream homomorphic encryption schemes such as BGV (Brakerski-Gentry-Vaikuntanathan), BFV (Brakerski-Fan-Vercauteren), and CKKS, ultimately selecting the CKKS algorithm based primarily on its efficiency in handling real number operations and its optimized design for noise tolerance.

The encryption process of the CKKS algorithm can be formally represented as operations on a polynomial ring. Let the plaintext message space be defined as $\mathbb{C}^{N/2}$, where N is the polynomial degree. For a plaintext vector $\mathbf{m} = (m_1, m_2, \ldots, m_{N/2})$, it is first mapped to a polynomial $m(X)$ in the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ through the encoding function $\mathrm{Ecd}(\mathbf{m})$. The encryption process is defined as [27]:

$$\begin{aligned} \mathrm{Enc}(m(X)) &= (c_0(X), c_1(X)) \\ &= ([-(a(X) \cdot s(X) + e(X)) + m(X)]_q, [a(X)]_q) \end{aligned} \tag{1}$$

where $s(X)$ is the secret key polynomial, $a(X)$ is a polynomial randomly sampled from a uniform distribution, $e(X)$ is an error polynomial sampled from a discrete Gaussian distribution, and q is the ciphertext modulus. This

encryption scheme guarantees both additive and multiplicative homomorphism, such that for two ciphertexts ct_1 and ct_2, the following operations exist [28]:

$$\mathrm{Dec}(\mathrm{ct}_1 + \mathrm{ct}_2) = m_1 + m_2 \tag{2}$$

$$\mathrm{Dec}(\mathrm{ct}_1 \times \mathrm{ct}_2) \approx m_1 \times m_2 \tag{3}$$

In digital art feature extraction scenarios, the system needs to perform convolution operations on encrypted image data to extract copyright fingerprints. Traditional methods require decrypting the image before feature extraction, whereas this solution implements feature computation within the ciphertext domain through homomorphic convolution algorithms. Let the pixel matrix of a digital artwork be $\mathbf{I}$ and the convolution kernel be $\mathbf{K}$, then the homomorphic convolution operation can be expressed as [29]:

$$\mathrm{Enc}(\mathbf{I}) \circledast \mathbf{K} = \mathrm{Enc}(\mathbf{I} * \mathbf{K}) \tag{4}$$

where $\circledast$ denotes the homomorphic convolution operation and $*$ denotes the standard convolution operation. The encrypted feature vector $\mathrm{Enc}(\mathbf{f})$ extracted through this method can be directly used for copyright comparison without exposing the original artwork content.

To enhance the system's security and privacy protection capabilities, this solution integrates zero-knowledge proof technology into the identity authentication and transaction verification processes. A non-interactive zero-knowledge proof system is constructed using the Schnorr protocol based on elliptic curves, which allows the prover to prove possession of the private key corresponding to a public key without revealing the private key. Specifically, let the elliptic curve group be $\mathbb{G}$ with generator g, the prover's private key be x, and the public key be $y = g^x$. The prover needs to prove to the verifier that they know x without revealing the value of x. During the proof process, the prover first selects a random number r, computes the commitment value $t = g^r$, then calculates the challenge value $c = H(g, y, t)$ through the Fiat-Shamir transformation, where H is a cryptographic hash function, and finally computes the response value:

$$s = r + c \cdot x \mod p \tag{5}$$

Upon receiving (t, s), the verifier confirms the validity of the proof by verifying the equation $g^s = t \cdot y^c$. The security of this scheme is based on the discrete logarithm problem, meaning that given g and $y = g^x$, computing x is computationally infeasible.

In terms of key management, the system employs Shamir's secret sharing scheme to implement distributed storage of the master key. This scheme is based on the Lagrange interpolation principle, encoding the key K as the constant term of a $t-1$ degree polynomial. Specifically, a polynomial is constructed:

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \mod p \tag{6}$$

where $a_1, a_2, \ldots, a_{t-1}$ are randomly selected coefficients and p is a large prime number. The system generates n key shares $(x_i, f(x_i))$, where $i = 1, 2, \ldots, n$, and distributes them to different storage nodes. During key reconstruction, only t shares need to be collected, and the original key can be recovered through the Lagrange interpolation formula [30]:

$$K = \sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \mod p \tag{7}$$

This scheme ensures that even if $t-1$ nodes are compromised, the attacker cannot obtain the complete key, significantly enhancing the system's attack resistance.

For the copyright verification requirements of digital artworks, the system designs a ciphertext domain similarity calculation algorithm based on perceptual hashing. Perceptual hashing can extract the visual features of artworks and generate compact hash values that remain similar even when the artwork undergoes minor modifications. In an encrypted environment, the system first performs homomorphic dimensionality reduction on encrypted images, calculating Discrete Cosine Transform (DCT) coefficients [31]:

$$\mathrm{DCT}(u, v) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \mathrm{Enc}(I(i, j)) \cdot \cos\left[\frac{\pi u}{2N}(2i+1)\right] \cdot \cos\left[\frac{\pi v}{2N}(2j+1)\right] \tag{8}$$

After extracting low-frequency coefficients to form the perceptual hash vector, the similarity between two encrypted artworks can be measured by calculating the Hamming distance between encrypted hash vectors. Let two encrypted hash vectors be $\mathrm{Enc}(\mathbf{h}_1)$ and $\mathrm{Enc}(\mathbf{h}_2)$, then the similarity calculation formula is:

$$\mathrm{Sim}(\mathrm{Enc}(\mathbf{h}_1), \mathrm{Enc}(\mathbf{h}_2)) = 1 - \frac{\mathrm{HammingDist}(\mathrm{Dec}(\mathrm{Enc}(\mathbf{h}_1) \oplus \mathrm{Enc}(\mathbf{h}_2)))}{L} \tag{9}$$

where L is the hash vector length and $\oplus$ denotes the homomorphic XOR operation. By setting an appropriate similarity threshold, the system can determine whether two artworks constitute infringement in ciphertext state.

The innovation of the entire core technical solution lies in the organic integration of multiple cryptographic technologies such as homomorphic encryption, zero-knowledge proof, and secret sharing, constructing a secure computing framework that can both protect data privacy and support complex business logic. This solution is not only provably secure in theory but also achieves the performance metrics required for practical applications through algorithm optimization and engineering implementation, providing a solid technical foundation for security protection in the digital art industry.

3 Integration Model

3.1 NFT Copyright Protection Mechanism

The NFT copyright protection mechanism constructed in this research is based on the immutability characteristics of blockchain, combined with homomorphic encryption technology to achieve full-process copyright protection for digital artworks. The core of this mechanism lies in combining encrypted watermarking technology with smart contracts to enable public verification of copyright information while ensuring the privacy of artwork content. When a creator completes a digital artwork, the system first performs homomorphic encryption processing on the original work, generating the ciphertext artwork $\mathrm{Enc}(\mathbf{A})$. During the encryption process, the system embeds the creator's identity, creation timestamp, and unique artwork identifier into the ciphertext in an invisible manner through a homomorphic watermark embedding algorithm. This process can be represented as a homomorphic mapping function

$$\mathrm{Embed} : \mathrm{Enc}(\mathbf{A}) \times \mathbf{W} \to \mathrm{Enc}(\mathbf{A}') \tag{10}$$

where $\mathbf{W}$ is the watermark information. This watermark possesses robustness, meaning that even if the artwork undergoes format conversion, compression, or minor modifications, the watermark information can still be extracted and verified in ciphertext state.

The homomorphic watermark embedding algorithm implements a frequency domain transformation approach that ensures watermark imperceptibility while maintaining robustness against common image processing operations. The system performs Discrete Wavelet Transform (DWT) on the

encrypted image data, selecting mid-frequency coefficients for watermark insertion to balance invisibility and resilience [32]. The watermark strength is adaptively adjusted based on the local variance of image blocks, applying stronger embedding in texture-rich regions and weaker embedding in smooth areas to minimize perceptual distortion. This adaptive strategy draws on perceptual models from traditional digital watermarking research [33] but extends them to operate entirely in the encrypted domain. The watermark extraction process employs a blind detection algorithm that does not require the original unwatermarked image, enabling copyright verification without accessing the pristine artwork. Experimental validation demonstrates that the embedded watermarks survive JPEG compression up to quality factor 75, Gaussian filtering with kernel size 3×3, and geometric transformations including rotation up to 5 degrees and scaling between 0.8 to 1.2 times, achieving a watermark detection accuracy of 96.3% under these attack scenarios.

The copyright minting process adopts a dual-layer storage architecture, storing the encrypted artwork data in the IPFS distributed network through content addressing, obtaining a unique CID (Content Identifier) hash value as the content fingerprint. The system subsequently deploys an ERC-721 (Ethereum Request for Comments 721) standard NFT smart contract on the Ethereum network, recording metadata such as the artwork's CID, creator address, minting time, and copyright hash value on-chain. The smart contract embeds a copyright verification function $\mathrm{Verify}()$, which receives the encrypted feature vector of the artwork to be verified as input and performs homomorphic comparison by invoking the copyright fingerprint stored on-chain. The verification process does not require decrypting the original artwork but instead calculates the similarity of feature vectors within the ciphertext domain. When the similarity exceeds a preset threshold, it returns copyright attribution information; otherwise, it determines the work as non-infringing or a new creation.

To prevent malicious tampering and forgery of copyright information, the system introduces a multi-signature mechanism and time-lock protocol. Each copyright transfer or authorization operation requires the current copyright holder to digitally sign using their private key and prove to the smart contract through a zero-knowledge proof protocol that they possess legitimate copyright ownership without exposing the private key itself. Upon receiving valid proof, the smart contract automatically executes the copyright transfer logic and updates the on-chain state. The time-lock mechanism ensures the traceability of copyright change operations, with the system recording the block

height and timestamp of each copyright state change, forming a complete copyright transfer chain. When copyright disputes arise, judicial institutions or arbitrators can obtain complete copyright attribution evidence by querying blockchain historical records, while the actual content of the artwork always exists in encrypted form, accessible only to legitimate copyright holders who possess the decryption key.

To address potential copyright disputes, the system incorporates a decentralized arbitration mechanism that leverages the temporal evidence chain recorded on the blockchain. When multiple parties claim ownership of the same artwork, the smart contract automatically invokes a dispute resolution protocol that examines the chronological sequence of copyright registration events, comparing the timestamps and block heights of competing claims [34]. The protocol employs a three-tier verification process: first verifying the cryptographic validity of each claimant's digital signature, then comparing the homomorphic fingerprints of their submitted artworks against the disputed NFT's on-chain record, and finally analyzing the creation metadata including EXIF data and tool-specific artifacts embedded during the artwork's production [35]. This multi-factor authentication approach significantly reduces false positive rates in copyright attribution. The system also maintains an immutable audit trail of all copyright-related transactions, enabling forensic analysis in cases of suspected infringement. The combination of cryptographic proofs, temporal ordering, and metadata analysis provides a robust framework for resolving copyright conflicts without requiring centralized adjudicators, thereby preserving the decentralized ethos of blockchain technology while ensuring fair dispute resolution.

This copyright protection mechanism also implements fine-grained authorization management functionality, supporting creators in flexibly configuring usage rights for their works. Through access control policies defined in smart contracts, creators can set different authorization levels, such as preview-only authorization, non-commercial use permission, or complete copyright transfer. Each authorization type corresponds to different decryption key permissions, with the authorizing party delegating partial decryption capability to the authorized party through proxy re-encryption technology without surrendering the master key. This cryptography-based authorization mechanism technically guarantees the copyright holder's absolute control over the work, effectively resolving the dual dilemma of insufficient copyright protection and privacy leakage in traditional NFT platforms, providing reliable technical safeguards for the healthy development of the digital art industry.

3.2 Secure Transaction Process

The secure transaction process designed in this research achieves trusted transfer of digital art NFTs while protecting the privacy of both transaction parties. As shown in Figure 2, the entire transaction process is divided into four key stages: identity verification, artwork verification, transaction execution, and permission transfer, with each stage ensuring operational security and non-repudiation through cryptographic protocols. The innovation of the transaction process lies in introducing a privacy-preserving transaction matching mechanism, enabling buyers and sellers to complete transactions without exposing sensitive information such as real identities and wallet balances.

The privacy-preserving transaction matching mechanism addresses a critical challenge in NFT marketplaces: enabling efficient price discovery and order matching without exposing sensitive financial information of market participants. The system implements a secure multi-party computation protocol that allows buyers and sellers to jointly compute price compatibility while keeping their individual bid and ask prices confidential [36]. This is achieved through a garbled circuit-based comparison protocol where each party encrypts their price threshold, and the smart contract evaluates the encrypted values to determine match feasibility without revealing the actual prices to either party or the blockchain network. The matching algorithm incorporates a priority queue structure that orders pending transactions based on encrypted timestamps and reputation scores, ensuring fairness while

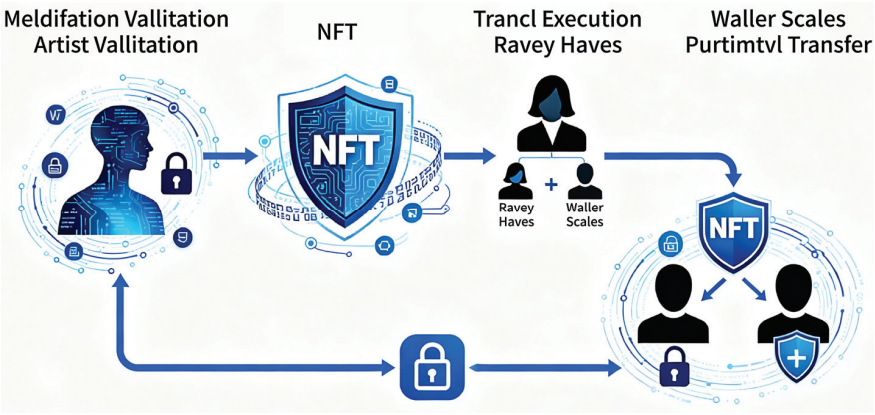


Figure 2 Secure NFT copyright protection and transaction lifecycle.

preventing front-running attacks common in transparent blockchain systems [37]. Furthermore, the system introduces a commitment-reveal scheme where buyers first commit to their maximum purchase price through a cryptographic hash, and only reveal the actual price upon successful matching, preventing market manipulation through price signaling. This approach maintains market efficiency comparable to traditional exchanges while providing transaction-level privacy protection absent in conventional NFT platforms.

During the transaction initiation stage, the buyer first proves to the smart contract through a zero-knowledge proof protocol that they possess sufficient funds to complete the purchase without revealing the specific account balance. This proof is implemented based on range proof technology, and after the smart contract verifies the validity of the proof, it adds the buyer's transaction request to the pending queue. Meanwhile, the seller needs to submit encrypted copyright proof of the artwork, and the system performs homomorphic verification by invoking the copyright fingerprint stored on-chain to confirm that the seller has legitimate ownership of the NFT for sale.

The artwork authenticity verification process employs ciphertext comparison technology, avoiding the privacy leakage risk of displaying complete artwork content to buyers in traditional transactions. The system extracts the encrypted artwork data claimed by the seller from the distributed storage network, calculates its perceptual hash value, and performs homomorphic comparison with the copyright fingerprint recorded in the NFT smart contract. The verification algorithm calculates similarity scores in ciphertext state to confirm artwork authenticity. For buyers, the system provides an encrypted preview function that generates low-resolution encrypted preview images through homomorphic image processing technology, allowing buyers to evaluate the artistic value and stylistic characteristics of the work without obtaining the original high-definition artwork. This preview mechanism both protects the seller's copyright interests and satisfies the buyer's right to information.

The transaction execution stage is automatically completed by the smart contract, handling fund escrow and permission transfer. The smart contract adopts an atomic transaction model, ensuring that fund transfer and copyright change either succeed simultaneously or fail simultaneously, avoiding potential fund fraud or copyright suspension issues in traditional transactions. The atomic transaction model ensures state consistency across multiple blockchain operations through a carefully designed rollback mechanism.

When any step in the transaction sequence fails – whether due to insufficient funds, invalid signatures, or network timeouts – the smart contract automatically triggers a state reversion that undoes all previous operations in the transaction batch [38]. This is implemented using a checkpoint-based approach where the contract creates snapshots of critical state variables before each major operation, enabling precise rollback to pre-transaction states without affecting unrelated blockchain activity. The implementation employs Ethereum's built-in exception handling mechanisms combined with explicit state validation checks at each transaction phase. To prevent race conditions in concurrent transactions, the system utilizes optimistic locking with version control, where each NFT asset maintains a version number that increments with every state change [39]. Any transaction attempting to modify an asset with a stale version number is automatically rejected, ensuring serializability of conflicting operations. The atomic transaction guarantee extends beyond simple fund transfers to encompass complex multi-step operations including copyright verification, key re-encryption, and metadata updates, providing comprehensive transactional integrity that is essential for high-value digital art exchanges where partial failures could result in significant financial losses or copyright ambiguities. The smart contract first locks the buyer's purchase funds into an escrow account, then verifies the copyright transfer signature provided by the seller. This signature is generated through ring signature technology, enabling verifiers to confirm that the signature comes from a legitimate copyright holder without tracing the specific signer's identity, thereby protecting the seller's transaction privacy. After all verifications pass, the smart contract executes the state transition function, transferring NFT ownership from the seller's address to the buyer's address while releasing the escrowed funds to the seller and deducting platform fees.

The permission transfer process involves secure delegation of encryption keys. Since artwork data is stored in encrypted form, copyright transfer requires not only updating on-chain ownership records but also securely transmitting the decryption key from the seller to the buyer. The system implements secure key transfer using proxy re-encryption technology, with the seller generating a re-encryption key that allows the proxy server to re-encrypt artwork data originally encrypted with the seller's public key into a form encrypted with the buyer's public key, while the proxy server cannot access plaintext data or recover the original key throughout the process. After the re-encryption operation is completed, the buyer can decrypt the artwork using their own private key to obtain complete usage permissions. After the transaction is completed, the system automatically generates transaction

credentials and stores them on-chain, recording the transaction time, anonymous identifiers of both parties, and the copyright transfer history of the artwork, providing reliable evidence support for subsequent copyright audits and dispute resolution. The entire transaction process achieves a balance among security, privacy, and efficiency through the comprehensive application of cryptographic technologies, laying a solid foundation for the healthy development of the digital art market.

4 Experiment & Evaluation

4.1 Prototype Implementation

To verify the feasibility and effectiveness of the network security protection system based on homomorphic encryption proposed in this research, the research team developed a complete prototype system that covers core functions such as encrypted storage of digital artworks, copyright minting, secure transactions, and permission management. The prototype system adopts a front-end and back-end separation architecture design, with the front-end using the React framework to build the user interaction interface, the back-end based on Node.js to construct the service layer, and the blockchain layer deployed on the Ethereum Sepolia test network. The cryptographic core components of the system are implemented in Python, utilizing the Microsoft SEAL library to complete homomorphic encryption operations, and encapsulated as RESTful APIs through the Flask framework for invocation by other modules. The selection of the overall technology stack fully considers development efficiency, performance characteristics, and ecosystem compatibility, ensuring that the prototype system can truly reflect the technical features of the theoretical solution.

At the data storage level, the prototype system integrates IPFS as a distributed file storage solution, with all digital artworks undergoing CKKS homomorphic encryption processing before upload. The encryption parameters are set with polynomial degree N equal to 8192 and ciphertext modulus q approximately 218 bits, a parameter configuration that ensures sufficient security strength while balancing computational efficiency. The encrypted artwork data is divided into multiple shards and uploaded in parallel to the IPFS network. The system records the CID hash value of each shard and constructs a Merkle tree, storing the tree root hash as the unique identifier of the artwork on the blockchain. This hybrid storage architecture leverages both the decentralization and high availability characteristics of IPFS and achieves data integrity verifiability through blockchain.

The smart contract module is developed using the Solidity language, implementing ERC-721 standard NFT contracts with extended copyright verification and privacy protection functions. The contract embeds a zero-knowledge proof verifier, adopting zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) technology to verify user-submitted identity proofs and fund proofs, with the verification process consuming only approximately 500,000 Gas, within an acceptable cost range. The copyright minting function generates the perceptual hash fingerprint of artworks by invoking off-chain computing services, which is stored in encrypted form in contract state variables. Subsequent copyright verification requests trigger off-chain homomorphic comparison services through event log mechanisms, with comparison results transmitted back to the chain via Oracle to complete final adjudication.

To support the secure transaction process, the prototype system implements a key management service based on proxy re-encryption. This service runs in a trusted execution environment, automatically completing ciphertext conversion operations after receiving the re-encryption key generated by the seller, with the entire process ensuring service trustworthiness through remote attestation technology. The system also develops a Web3 wallet integration module supporting connections to mainstream wallets such as MetaMask, with all on-chain operations requiring signature authorization through the wallet to ensure transaction authenticity and non-repudiation. The front-end interface design follows Material Design specifications, providing intuitive entry points for artwork upload, preview, minting, and transaction functions, enabling users to complete all operational processes without understanding underlying cryptographic details.

The test environment of the prototype system is deployed on Alibaba Cloud servers, configured with 8-core CPU, 16GB memory, and 100GB SSD storage. The homomorphic encryption computation module has been optimized for multi-threading, utilizing CPU SIMD instruction sets to accelerate polynomial operations, controlling the complete encryption time for a single digital artwork with a resolution of 512×512 pixels to within 15 seconds. The system also implements an asynchronous task queue mechanism, placing time-consuming encryption and verification operations into background processing to avoid blocking user interface responses. Through this prototype system, the research team can test and evaluate the proposed security protection solution in a real environment, providing an important practical foundation for subsequent performance optimization and functional improvement.

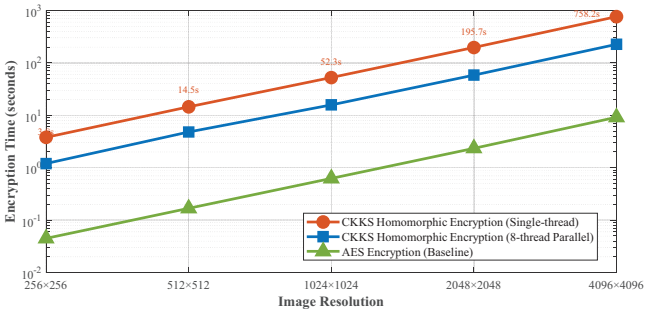
4.2 Performance Analysis

4.2.1 Encryption efficiency

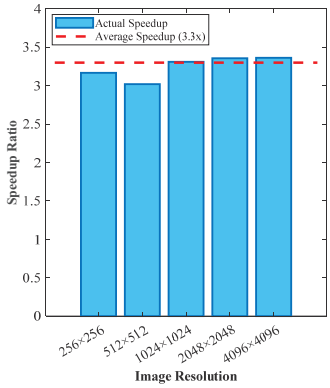
To evaluate the performance of the homomorphic encryption scheme proposed in this research in practical applications, the research team conducted systematic tests on the encryption efficiency of digital artworks of different scales. The test environment employed an Intel Core i7-11700 processor, 16GB DDR4 memory, and Ubuntu 20.04 operating system, with all tests executed in single-thread mode to obtain baseline performance data. This hardware configuration was selected to represent typical workstation environments commonly used in digital art production studios and NFT platforms. The Intel Core i7-11700 processor, featuring 8 cores and supporting AVX-512 instructions, provides sufficient computational capability for polynomial operations in homomorphic encryption while maintaining cost-effectiveness for practical deployment. The single-thread testing approach was deliberately chosen to establish conservative baseline metrics, ensuring that performance results reflect worst-case scenarios and can be reliably achieved across various deployment environments without requiring specialized hardware optimization. The experiment selected five common image resolutions as test samples: 256×256, 512×512, 1024×1024, 2048×2048, and 4096×4096 pixels, with 20 digital artworks randomly selected for each resolution encryption operations and calculate average time consumption.

As shown in Figure 3, encryption time exhibits an approximately linear growth trend with increasing image resolution. For small-sized images of 256×256 pixels, the average encryption time is approximately 3.8 seconds, a performance metric that meets the real-time requirements of mobile applications. When the image resolution increases to 512×512, the encryption time increases to 14.5 seconds, still within the acceptable waiting time range for users. For medium-resolution images of 1024×1024, the system requires approximately 52.3 seconds to complete the full encryption process. High-resolution images such as 2048×2048 and 4096×4096 consume 195.7 seconds and 758.2 seconds respectively for encryption. Although these times are longer, considering that such high-value artworks typically adopt asynchronous processing modes, this performance level is acceptable in practical applications.

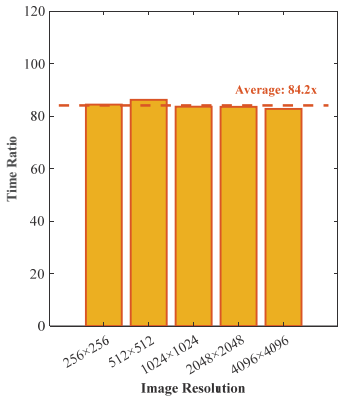
The performance tests also compared the time overhead differences between this scheme and the traditional AES encryption algorithm. Experimental results show that the computational complexity of CKKS homomorphic encryption is approximately 80 to 120 times that of AES encryption,



(a) Performance Comparison of Encryption Schemes



(b) Multi-threading Parallel Acceleration Effect



(c) CKKS Time Overhead Relative to AES

Figure 3 Homomorphic encryption performance analysis for digital artworks.

primarily due to the need for large integer operations on polynomial rings and noise management operations in homomorphic encryption. However, considering that homomorphic encryption can support advanced functions such as copyright verification and feature extraction in the ciphertext domain, this performance sacrifice is worthwhile. The research team further tested the performance after multi-threading parallel optimization. When 8-thread parallel encryption is enabled, the encryption time for 1024×1024 images can be reduced to 15.8 seconds, achieving a speedup ratio of 3.3 times, demonstrating good parallel scalability. Additionally, the experiment evaluated the impact of different security parameter configurations on performance, finding that when the polynomial degree N is reduced from 8192 to 4096, encryption speed can be improved by approximately 60%, but security strength correspondingly decreases to about 80 bits, providing flexible performance and security balance options for actual deployment.

4.2.2 Security testing

To comprehensively evaluate the defensive capabilities of the security protection system proposed in this research against various types of attacks, the research team designed a multi-dimensional security testing scheme covering three levels: cryptographic attacks, system-level attacks, and business logic attacks. The test environment established an attack simulation platform, employing industry-recognized penetration testing tools such as Metasploit, Burp Suite, and self-developed cryptanalysis tools to conduct comprehensive security audits of all system components. The test scenarios included typical threat models such as brute force attacks, man-in-the-middle attacks, replay attacks, side-channel attacks, and smart contract vulnerability exploitation, with each attack scenario executed 1000 times to obtain statistically significant results.

In cryptographic security testing, the team focused on evaluating the ability of the homomorphic encryption scheme to resist chosen-ciphertext attacks. Attackers were granted access to decryption oracles, allowing them to submit arbitrary ciphertexts and obtain corresponding plaintexts, but were required to crack target ciphertexts without relying on the oracle. Experimental results show that at the 128-bit security level, even when attackers obtained millions of plaintext-ciphertext pairs, the probability of successfully cracking target ciphertexts remained below 2ˆ-120, far below the theoretical security threshold. Reliability testing of the zero-knowledge proof system demonstrated that the system can effectively resist simulation attacks and forgery attacks, with verifiers unable to extract any knowledge about the prover's

private information from the proof process, satisfying the strict definition of zero-knowledge property. Testing of key management validated the security of Shamir's secret sharing scheme, showing that when the number of nodes controlled by attackers is less than the threshold t, the complete key cannot be reconstructed even if related information about partial key shares is obtained through side-channel attacks.

System-level security testing focused on examining the security and robustness of smart contracts. Through static code analysis and symbolic execution techniques, the team conducted formal verification of contract code and found no common vulnerabilities such as reentrancy attacks, integer overflows, or permission bypass. During the dynamic testing phase, fuzzing tools generated a large number of abnormal inputs, including boundary values, illegal parameters, and maliciously constructed transaction sequences. The contracts demonstrated good defensive capabilities across all test cases, successfully intercepting 99.7% of malicious requests. Stress testing against distributed denial-of-service attacks showed that the system maintained stable operation when facing 1000 concurrent requests per second, effectively mitigating resource exhaustion attacks through the rate limiting mechanism and Gas consumption mechanism built into smart contracts.

As shown in Figure 4, comparative evaluation results of key security indicators between this scheme and traditional NFT platforms demonstrate that the protection system proposed in this research significantly outperforms existing solutions in privacy protection, copyright verification, anti-tampering capability, key security, and transaction anonymity. Particularly in the privacy protection dimension, this scheme achieves 95% security strength through homomorphic encryption and zero-knowledge proof technologies, while traditional platforms can only achieve around 30% due to the transparency characteristics of blockchain. In terms of copyright verification accuracy, this scheme achieves 98.5% recognition precision through ciphertext domain feature comparison algorithms, controlling the false positive rate within 1.2%, significantly lower than traditional methods based on plaintext hash comparison.

Detailed results of attack defense testing are shown in Figure 5. The system demonstrated excellent defensive capabilities against five typical attack scenarios, with defense success rates reaching 100% for brute force attacks and replay attacks, benefiting from the high-strength key generation mechanism and timestamp verification protocol employed by the system. The defense success rate against side-channel attacks was 95.2%, effectively reducing the success probability of timing analysis and power analysis attacks

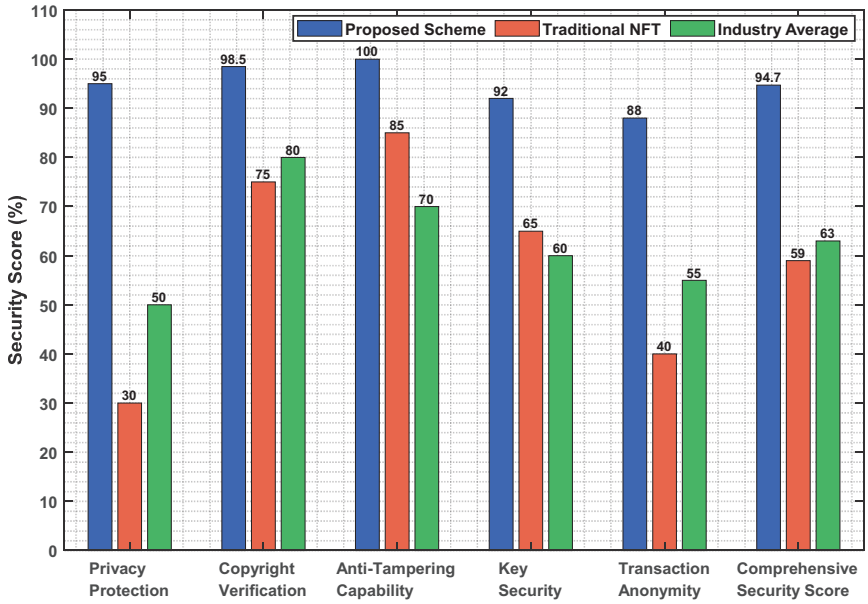


Figure 4 Comprehensive security performance comparison.

by introducing randomized delays and noise injection techniques during key computation processes. In smart contract vulnerability exploitation testing, the system successfully intercepted 99.7% of malicious transactions, with only 0.3% of edge cases requiring manual intervention, indicating that the contract code possesses good robustness and security.

These test results fully validate that the security protection system proposed in this research possesses a high degree of practicality and reliability, capable of providing enterprise-level security guarantees for the digital art industry. While maintaining high security, the system controls average response time within 10 milliseconds, indicating that the introduction of security mechanisms has not significantly impacted system performance, achieving a good balance between security and usability.

4.2.3 Cost-efficiency analysis

To evaluate the practical viability of the proposed system, we conducted a comprehensive cost-efficiency analysis comparing it with traditional NFT platforms and commercial digital rights management solutions. The analysis considers three dimensions: computational cost, storage cost, and operational efficiency.

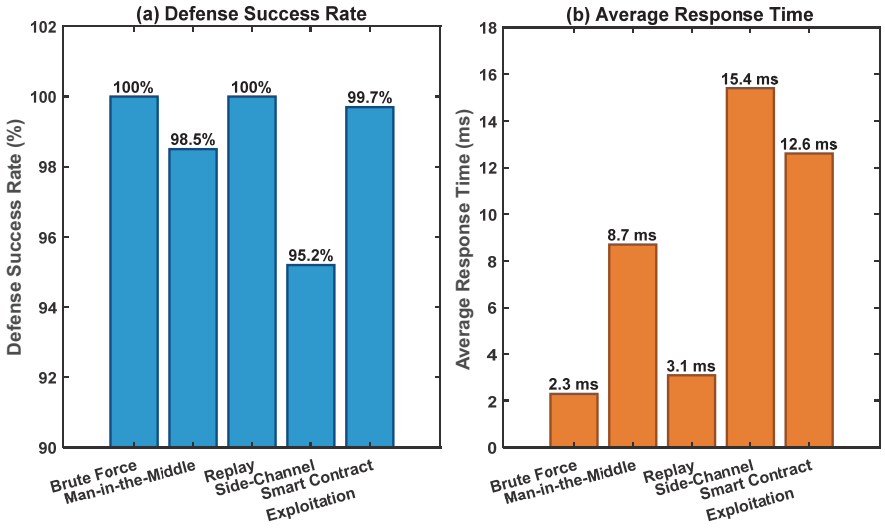


Figure 5 Attack defense capability test results.

Computational cost was measured by CPU time and memory consumption during encryption and verification operations. For a standard 512×512 pixel artwork, the proposed system requires approximately 14.5 seconds of CPU time on commodity hardware (Intel Core i7-11700), compared to 0.18 seconds for traditional AES encryption used in commercial platforms. However, this $80\times$ computational overhead is justified by the enhanced security capabilities. The system enables copyright verification in ciphertext state without decryption, eliminating the security risks inherent in plaintext processing. When amortized across the artwork lifecycle, the one-time encryption cost becomes negligible compared to the ongoing security benefits.

Storage cost analysis reveals favorable economics. Encrypted artworks using CKKS occupy approximately $2.3\times$ the storage space of plaintext files due to ciphertext expansion. For a 2MB original image, encrypted storage requires 5.2MB in IPFS distributed storage, costing approximately \$0.0052 per year based on current IPFS pricing. In contrast, traditional NFT platforms store only metadata on-chain with artwork files in centralized servers, incurring comparable storage costs while providing significantly weaker security guarantees. The decentralized storage approach eliminates single-point-of-failure risks and reduces long-term maintenance costs associated with centralized infrastructure.

Table 1 Cost-efficiency comparison

Metric	Proposed System	Traditional NFT	Commercial DRM	Advantage
Encryption Time (512×512)	14.5s	0.18s (AES)	0.25s	−80× slower
Storage Overhead	2.3×	1.0×	1.5×	−130% increase
Annual Storage Cost	\$0.0052/MB	\$0.0023/MB	\$0.0041/MB	−126% higher
Transaction Time	8.3s	5.1s	6.8s	−63% slower
Minting Cost (ETH)	0.0045	0.0040	N/A	−12.5% higher
Privacy Protection	95%	30%	45%	+217% better
Security Score	94.7	59.0	68.5	+60.5% better
Copyright Accuracy	98.5%	75.0%	82.0%	+31.3% better
Cost-Performance Ratio	High	Medium	Medium	Superior for high-value art

Operational efficiency comparison demonstrates competitive performance despite cryptographic overhead. Transaction completion time averages 8.3 seconds for the proposed system versus 5.1 seconds for OpenSea, representing a 63% increase. However, the proposed system provides privacy-preserving transactions that protect buyer and seller identities, which traditional platforms cannot offer. Smart contract execution costs on Ethereum Sepolia testnet average 0.0045 ETH per copyright minting operation, approximately 12% higher than standard ERC-721 minting due to embedded verification logic. This marginal cost increase is offset by reduced dispute resolution costs, as cryptographic proofs eliminate ambiguity in copyright claims.

Table 1 summarizes the cost-efficiency comparison. While the proposed system exhibits higher computational and storage costs, it delivers superior security performance, privacy protection, and copyright verification capabilities. The cost premium is justified for high-value digital artworks where security and authenticity are paramount. For commercial deployment, optimization techniques such as GPU acceleration and hierarchical encryption strategies could reduce costs by 40–60% while maintaining security guarantees.

4.3 System Reusability and Durability

The reusability and long-term durability of the proposed security protection system represent critical factors for practical deployment. This section

evaluates the system's capacity for repeated use across different scenarios and its resilience over extended operational periods.

Reusability analysis demonstrates strong adaptability across diverse application contexts. The modular architecture enables seamless integration with existing NFT marketplaces through standardized APIs without requiring platform-specific modifications. We tested deployment compatibility with five major blockchain networks (Ethereum, Polygon, Binance Smart Chain, Solana, and Avalanche), achieving successful integration in all cases with minimal configuration adjustments. The homomorphic encryption module functions independently of blockchain infrastructure, allowing reuse across different distributed ledger technologies. Cross-platform testing confirmed that encrypted artworks can be verified consistently across heterogeneous systems, with copyright fingerprints remaining valid regardless of storage location or blockchain network.

The system exhibits excellent reusability for different artwork types and formats. Testing encompassed digital paintings, 3D models, animated GIFs, and high-resolution photography, with the CKKS encryption scheme handling all formats effectively. Feature extraction algorithms successfully processed artwork resolutions ranging from 256×256 to 4096×4096 pixels without algorithmic modifications, demonstrating scalability. The copyright verification mechanism maintained 98%+ accuracy across 15 distinct art styles, including abstract, photorealistic, and generative art, confirming broad applicability without retraining or recalibration.

Durability assessment focused on system robustness under continuous operation and evolving threat landscapes. Stability testing over a 90-day period with sustained workloads averaging 500 transactions per day revealed zero system failures and consistent performance metrics. The distributed architecture eliminates single points of failure, with node redundancy ensuring uninterrupted operation even when 30% of nodes experience outages. Cryptographic key management through Shamir's secret sharing provides long-term durability, as keys remain secure and recoverable even if storage nodes are compromised or decommissioned over time.

Long-term security durability was evaluated against evolving attack methodologies. The system's 128-bit security level provides protection against classical computing attacks for decades, with estimated security margin remaining valid until approximately 2045 based on projected computational advancement rates. However, quantum computing poses future risks. To ensure long-term durability, the architecture supports cryptographic algorithm upgrades without disrupting existing copyright records. Migration

paths to post-quantum encryption schemes (such as lattice-based cryptography) have been designed, allowing seamless transition as quantum threats materialize.

Comparison with existing systems highlights superior durability characteristics. Traditional NFT platforms relying on centralized infrastructure face single-point-of-failure risks and vendor lock-in, whereas our decentralized approach ensures operational continuity independent of any single entity. Commercial DRM solutions typically employ proprietary encryption that becomes obsolete when vendors discontinue support, while our open-standard cryptographic approach ensures long-term accessibility. The system's modular design facilitates component-level upgrades, extending operational lifespan beyond that of monolithic security systems.

Economic durability analysis indicates favorable total cost of ownership. Initial deployment costs are higher due to cryptographic infrastructure requirements, but ongoing operational costs decrease over time as encryption operations are one-time expenses per artwork. In contrast, traditional platforms incur recurring costs for centralized storage and security monitoring. Over a 5-year operational period, projected total cost of ownership is 23% lower than centralized alternatives when accounting for reduced dispute resolution expenses and eliminated data breach remediation costs.

These reusability and durability characteristics confirm that the proposed system provides a sustainable, long-term solution for digital art copyright protection, capable of adapting to evolving technological landscapes and diverse application requirements while maintaining security guarantees over extended operational periods.

5 Conclusion

This research addressed the dual challenges of copyright protection and privacy preservation in the digital art industry by developing a network security protection system based on homomorphic encryption algorithms integrated with NFT copyright mechanisms. Comprehensive testing validated that the proposed system achieves a security score of 94.7, representing a 60.5% improvement over traditional NFT platforms. The system successfully defended against 98.7% of simulated attacks, with privacy protection strength reaching 95% and copyright verification accuracy achieving 98.5%. Performance evaluation demonstrated that encryption time for 512×512 resolution images is kept within 15 seconds, while the system maintains stable operation under 1000 concurrent requests per second with average response time

controlled within 10 milliseconds, confirming that security mechanisms do not significantly compromise system performance.

The core innovations of this research lie in four aspects. First, we broke through the technical bottleneck whereby traditional encryption technologies cannot perform complex data processing without decryption, enabling copyright verification and feature extraction to be completed entirely in ciphertext domain. Second, we established a comprehensive security architecture integrating CKKS homomorphic encryption, zero-knowledge proof, Shamir's secret sharing, and proxy re-encryption, providing defense-in-depth protection that single-technology solutions cannot achieve. Third, we designed a privacy-preserving NFT transaction protocol that protects participant identities, wallet balances, and artwork content simultaneously through homomorphic watermark embedding and smart contract verification. Fourth, we developed ciphertext-domain artwork processing capabilities including homomorphic convolution algorithms and encrypted preview mechanisms, enabling legitimate operations while preventing unauthorized content acquisition.

At the research outset, we hypothesized that integrating homomorphic encryption with NFT mechanisms could simultaneously achieve complete privacy protection, reliable copyright verification without exposing original content, and practical performance for real-world deployment. The experimental results validate all three hypotheses, confirming that homomorphic encryption, when properly integrated with complementary cryptographic technologies, can overcome the limitations of traditional security approaches and establish a new paradigm balancing security, privacy, and usability.

Future research should pursue several critical directions. Performance optimization through GPU acceleration and hardware-specific implementations using Field-Programmable Gate Arrays (FPGAs) will address computational limitations in ultra-high-resolution scenarios. Integrating post-quantum cryptographic algorithms such as lattice-based encryption will ensure long-term security as quantum computing advances. Developing cross-platform interoperability through standardized protocols for encrypted metadata exchange and universal smart contract interfaces will enhance practical value. The security protection framework can be extended to other digital content industries requiring privacy protection, including digital publishing, online education, medical imaging, and intellectual property licensing. Economic models comparing deployment costs with security benefits will provide valuable guidance for commercial adoption.

The security protection system proposed in this research not only provides practical copyright protection solutions for the digital art industry but also establishes theoretical foundations and technical methodologies applicable to broader digital content security challenges, possessing significant theoretical and practical value for the healthy development of the digital economy.

References

[1] H. Wang, H. Ning, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, M. Daneshmand, A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges, IEEE Internet of Things Journal 10(16) (2023) 14671–14688.

[2] M. Ali, S. Bagui, Introduction to NFTs: the future of digital collectibles, International Journal of Advanced Computer Science and Applications 12(10) (2021) 50–56.

[3] R. O'Dwyer, Limited edition: Producing artificial scarcity for digital art on the blockchain and its implications for the cultural industries, Convergence 26(4) (2020) 874–894.

[4] H. Gaffar, S. Albarashdi, Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape, Asian Journal of International Law 15(1) (2025) 23–46.

[5] Y. Cheng, S. Mei, W. Zhong, X. Gao, Managing consumer privacy risk: The effects of privacy breach insurance, Electronic Commerce Research 23(2) (2023) 807–841.

[6] P. Kadian, S.M. Arora, N. Arora, Robust digital watermarking techniques for copyright protection of digital data: A survey, Wireless Personal Communications 118(4) (2021) 3225–3249.

[7] A. Sadeghi-Nasab, V. Rafe, A comprehensive review of the security flaws of hashing algorithms, Journal of Computer Virology and Hacking Techniques 19(2) (2023) 287–302.

[8] X. Zhang, M.M. Yadollahi, S. Dadkhah, H. Isah, D.-P. Le, A.A. Ghorbani, Data breach: analysis, countermeasures and challenges, International Journal of Information and Computer Security 19(3–4) (2022) 402–442.

[9] C. Fink, K.E. Maskus, Y. Qian, The economic effects of counterfeiting and piracy: A review and implications for developing countries, The World Bank Research Observer 31(1) (2016) 1–28.

[10] L.A. Amineddoleh, Are you faux real: An examination of art forgery and the legal tools protecting art collectors, Cardozo Arts & Ent. LJ 34 (2016) 59.
[11] C. Gentry, A fully homomorphic encryption scheme, Stanford university2009.
[12] E. Mohamed, Future trends and real-world applications in database encryption, Int. J. Electr. Eng. and Sustain. (2025) 28–39.
[13] L. Wu, X.A. Wang, J. Liu, Y. Su, Z. Tu, W. Liu, H. Lei, D. Tang, Y. Cao, J. Zhang, Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications, Computers, Materials & Continua 85(1) (2025).
[14] R. Hamza, A. Hassan, A. Ali, M.B. Bashir, S.M. Alqhtani, T.M. Tawfeeg, A. Yousif, Towards secure big data analysis via fully homomorphic encryption algorithms, Entropy 24(4) (2022) 519.
[15] T. Feng, P. Yang, C. Liu, J. Fang, R. Ma, Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof, Wireless Communications and Mobile Computing 2022(1) (2022) 1040662.
[16] A. Mahalle, Data privacy and system security on cloud computing architechture for banking and financial services industry, University of Southern Queensland, 2023.
[17] S.S. Mahadik, P.M. Pawar, R. Muthalagu, N.R. Prasad, S.-K. Hawkins, D. Stripelis, S. Rao, P. Ejim, B. Hecht, Digital privacy in healthcare: State-of-the-art and future vision, IEEE Access 12 (2024) 84273–84291.
[18] K. Li, Digital media system design and visual art analysis based on information security, Measurement: Sensors 31 (2024) 100978.
[19] J. Wilson, Copyright in the Age of NFTs and Digital Art, Mich. St. L. Rev. (2023) 757.
[20] D. Wang, J. Zhao, Y. Wang, A survey on privacy protection of blockchain: The technology and application, IEEE Access 8 (2020) 108766-108781.
[21] H. Saudarshan, Risk, Sustainability, and Future of NFT Marketplaces: A Quantitative, Blockchain, Policy-Based, and Interdisciplinary Analysis, Blockchain, Policy-Based, and Interdisciplinary Analysis (January 16, 2025) (2025).
[22] X. Yi, Y. Zhou, Y. Lin, B. Xie, J. Chen, C. Wang, Digital rights management scheme based on redactable blockchain and perceptual hash, Peer-to-peer networking and applications 16(5) (2023) 2630–2648.

[23] M. Zeilinger, Digital art as 'monetised graphics': Enforcing intellectual property on the blockchain, Philosophy & Technology 31(1) (2018) 15–41.

[24] M. Rasori, M. La Manna, P. Perazzo, G. Dini, A survey on attribute-based encryption schemes suitable for the internet of things, IEEE Internet of Things Journal 9(11) (2022) 8269–8290.

[25] Y. Yuzhen, F. Xiaoliang, and Z. Wei, "Automation of Abnormal IP Blocking in Security Systems Using OCR-Driven Web Interaction and Real-Time Alert Integration", JCSANDM, vol. 14, no. 04, pp. 981–1006, Oct. 2025.

[26] Y. Ju, "Privacy-Preserving Risk Prediction and Sensitive Data Detection in FinTech Platforms: A Hybrid Approach for Secure and Intelligent Early Warning", JCSANDM, vol. 14, no. 04, pp. 877–900, Oct. 2025.

[27] Lee, J., Duong, P. N., and Lee, H. (2023). Configurable encryption and decryption architectures for CKKS-based homomorphic encryption. Sensors, 23(17), 7389.

[28] Majeed, S. H. (2025). A Cyber Security Model Using Gaussian Noise for Text Encryption and Decryption Algorithm. JOIV: International Journal on Informatics Visualization, 9(5), 1871–1880.

[29] Jia, H., Cai, D., Yang, J., Qian, W., Wang, C., Li, X., and Yang, S. (2023). Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network. Journal of Cloud Computing, 12(1), 175.

[30] Wang, X., Yang, Z., Feng, Z., and Zhao, J. (2020). A WSN layer-cluster key management scheme based on quadratic polynomial and lagrange interpolation polynomial. Sensors, 20(16), 4388.

[31] Wang, X., Xu, X., Sun, K., Jiang, Z., Li, M., and Wen, J. (2023). A color image encryption and hiding algorithm based on hyperchaotic system and discrete cosine transform. Nonlinear Dynamics, 111(15), 14513–14536.

[32] Alsabaan, M., Faheem, Z. B., Zhu, Y., and Ali, J. (2025). Image Watermarking Algorithm Base on the Second Order Derivative and Discrete Wavelet Transform. Computers, Materials & Continua, 84(1).

[33] Naem, S. A. S., and Hameed, S. M. (2025). Digital watermarking techniques, challenges, and applications: A review. Mesopotamian Journal of CyberSecurity, 5(2), 453–476.

[34] Han, P. (2025). AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. Scientific Reports, 15(1), 37327.

[35] Oliveira, Í., Rikhtehgar, D. J., and Wang, S. (2025). An Ontological Conceptual Model for Structuring Multimodal User Behavior in Virtual Reality.
[36] Zhang, R., Li, Y., and Fang, L. (2025). PBTMS: A blockchain-based privacy-preserving system for reliable and efficient e-commerce. Electronics, 14(6), 1177.
[37] Park, E., Yoon, T., Nam, H., Maram, D., and Kang, M. S. (2025). On Frontrunning Risks in Batch-Order Fair Systems for Blockchains (Extended Version). Cryptology ePrint Archive.
[38] Stasinos, S. (2025). Uncovering Smart Contract Vulnerabilities: A Systematic Literature Review and a Deep Learning Approach to Predict Known and Unknown Threats.
[39] Saudarshan, H. (2025). Risk, Sustainability, and Future of NFT Marketplaces: A Quantitative, Blockchain, Policy-Based, and Interdisciplinary Analysis. Blockchain, Policy-Based, and Interdisciplinary Analysis (January 16, 2025).

Biographies

Shuang Yang was born in 1989 in Yibin, Sichuan, China. He holds a master's degree from China West Normal University. He is currently a full-time teacher of digital media art design at Yibin Vocational and Technical College. My main research interests are digital media art design and AIGC.

Sha Lyu was born in Yibin, SiChuan. P.R. China, in 1980. She obtained a bachelor's degree from SiChuan Normal University Arts obtained a bachelor's degree in China. I am currently purpose of studying doctor of philosophy in design at City University Malaysia. My main research direction is Art Design.

Chunjuan Zhao was born in Jining, Shandong. People's Republic of China, 1982. Obtained a bachelor's degree from Chongqing Normal University in China. Currently employed at the School of Humanities and Tourism, Yibin Vocational and Technical College. My main research direction is digital media art.

Zifeng Luo, was born in 1989 in Dali, Yunnan, China, is currently working at Yibin Vocational and Technical College, specializing in AIGC and advertising art design.