A Blockchain-Based Model For Copyright And Privacy Protection Of Industrial New Media Content

Si Wu

School of Journalism and Communications, Zhoukou Normal University, Zhoukou, 466000 Henan,China

Corresponding author. E-mail: wusi_2026@126.com

Received: July. 04, 2026; Accepted: Sep. 29, 2026

Industrial new media content — such as equipment operation videos, technical manuals, engineering drawings, and factory livestreams — faces growing copyright and privacy challenges from complex infringement methods, high on-chain storage pressure, and the risk of exposing creators' identities and proprietary technical information. This study proposes a blockchain-based copyright and privacy protection model that ensures credible copyright evidence while preserving privacy and scalability. Built on a Hyperledger Fabric consortium blockchain, the model follows a layered "content processing – on-chain registration – privacy authorization – off-chain storage – copyright verification" architecture, integrating multimodal copyright fingerprinting, dynamic pseudo-identity generation, attribute-based access control with trust/risk/frequency scoring, hybrid on-chain–off-chain storage, and distributed indexing. Large-scale simulation with millions of content items shows a registration latency of 490 ms, throughput of 2120 TPS, retrieval response time of 430 ms, storage overhead of 280 GB, verification accuracy of 94.5%, and an F1 score of 0.76 under 50% tampering. The privacy leakage rate is reduced to 9.4%, with an 84.6% unauthorized-access interception rate under severe attack. These results indicate improved copyright robustness, stronger privacy protection, and better scalability, supporting staged deployment on consortium-based industrial new media platforms without exposing original content or real identities on-chain.

Keywords: Industrial new media content; Blockchain; Copyright protection; Privacy protection; Multimodal copyright fingerprint; Dynamic pseudo-identity

http://dx.doi.org/10.6180/jase.202612_35.036

1. Introduction

Industrial new media content — equipment demonstration videos, technical manuals, engineering drawings, factory livestreams — is an active but easily copied and redistributed data asset. Diverse production entities, complex dissemination, and multimodal forms make infringement hard to detect and evidence hard to preserve, motivating blockchain, smart contracts, and proactive defense to strengthen immutability and automated processing of copyright records [1].

Most platforms use centralised databases for registration — cheap but prone to single-point failure, weak evidence, sync delay, and privacy exposure at scale. Consortium blockchains like Hyperledger Fabric handle full-lifecycle registration, query, transfer, and cancellation [2], but writing large content or metadata on-chain causes storage expansion and congestion.

Copyright protection also faces privacy risks: equipment manuals may embed proprietary parameters, and registration itself exposes identity, upload time, work category, and access logs. Systems must ensure ownership credibility without over-disclosing real identities and usage trajectories — a tension also noted in blockchain music-copyright research on ownership credibility, revenue distribution, and collaboration [3] — and it is even more prominent for

industrial new media.

Traditional hash-based rights confirmation is also highly sensitive to minor modifications: cropping, transcoding, noise addition, rewriting, or splicing all change the hash value, so simple matching cannot identify semantically similar or secondarily processed infringing content. Combining blockchain with homomorphic encryption and digital watermarking can strengthen protection [4], but a copyright fingerprint mechanism tailored to the multimodal characteristics of industrial new media is still needed.

The main contributions of this study are as follows: first, a general architecture for blockchain-based copyright and privacy protection for industrial new media content; second, a multimodal copyright fingerprint and similarity verification model that improves identification after minor tampering; third, a privacy protection mechanism combining dynamic pseudo-identity and attribute access control; and fourth, a hybrid on-chain and off-chain storage and distributed indexing mechanism.

Unlike existing schemes that register a single content hash or execute access policies in isolation, the proposed model unifies multimodal semantic fingerprinting, verifiable ownership records, dynamic pseudo-identity protection, and hybrid storage in one workflow, addressing three coupled problems in industrial new media platforms: robust identification after secondary editing, credible evidence preservation, and privacy-preserving authorization under high-frequency access.

Blockchain's distributed consensus, timestamping, immutability, and multi-party verification suit copyright evidence and ownership tracking. Chen et al. proposed a scheme with active defense against infringement [1]; Liu et al. built a Hyperledger Fabric system for registration, transaction, query, and cancellation, the basis for the platform used here [2]; Ciriello et al. summarised blockchain design principles for music copyright management, supporting multi-subject collaboration and revenue distribution [3]. Industrial new media content further includes engineering drawings and process documentation with more diverse infringement forms and a text-image-audio-video ontology, so this study replaces single-hash registration with multimodal fingerprints integrated with ownership records, access policies, and verification logs on-chain.

Privacy protection is a key issue for distributed copyright systems, and combining attribute access control with blockchain enables finer-grained authorisation. Han et al. proposed a searchable-encryption and attribute access control framework for multi-user retrieval privacy [5]; Zhang et al. built a smart-contract-driven attribute access control framework covering policy, attribute, and access-decision management [6].

IoT and data-sharing authorisation research offers further reference: Policychain implements decentralised, script-driven authorisation [7]. This paper combines dynamic pseudo-identity, attribute scoring, risk constraints, and smart-contract authorisation accordingly.

Privacy computing, zero-knowledge proofs, and homomorphic encryption increasingly protect data sharing: Ma et al. combined blockchain with ZK-Rollup [8]; Darwish et al. combined blockchain with perceptual-hash video watermarking [9]. For recognition, zero-trust mechanisms and digital watermarking also help protect images [10].

Watermarking research shows copyright systems cannot rely solely on file hashes: Wang et al. proposed periodic blind watermarking [11]; Fkirin et al. compared neural-network watermarking, showing protection has expanded to algorithmic models [12]. IPFS combined with blockchain reduces on-chain pressure and improves distributed storage of large files [13, 14].

In summary, existing studies provide foundations for copyright registration, access control, watermarking, and storage, but mostly address a single media type or an isolated layer. The gap here is an integrated framework combining multimodal recognition, privacy-preserving identity management, scalable off-chain storage, and on-chain evidence verification.

2. Methods

2.1. Overall Model Architecture

The model adopts a layered architecture of "content processing – on-chain registration – privacy authorisation – off-chain storage – copyright verification," shown in Fig. 1. It uses a consortium blockchain as the core trusted layer, multimodal content fingerprints as the basis for copyright recognition, attribute access control and dynamic pseudo-identity as privacy protection mechanisms, and IPFS with a distributed metadata database to support large-scale content storage.

The model's operation flow, shown in Fig. 2, is as follows: after content is uploaded, the system performs preprocessing and feature extraction, generates a multimodal copyright fingerprint, and invokes the registration contract; access requests are then judged via a privacy policy contract, and if authorised, the encrypted content is retrieved from off-chain storage and decrypted; if a dispute occurs, verification uses on-chain evidence, fingerprints, and timestamps.

The security boundary assumes the blockchain is maintained by authenticated operators, service agencies, and

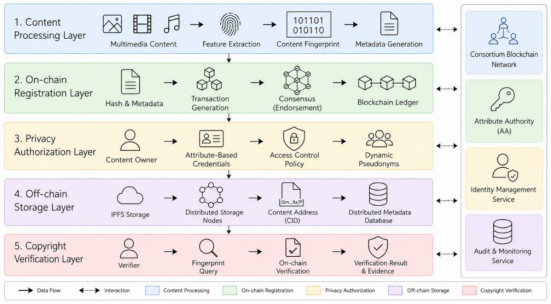

Fig. 1. Overall Architecture of a Blockchain-Based Industrial New Media Content Copyright and Privacy Protection Model

verifiers, while attackers may copy or tamper with content, replay requests, forge identities, or crawl at high frequency. The model counters these via off-chain encryption, dynamic pseudo-identities, and on-chain timestamps, fingerprints, policies, and logs.

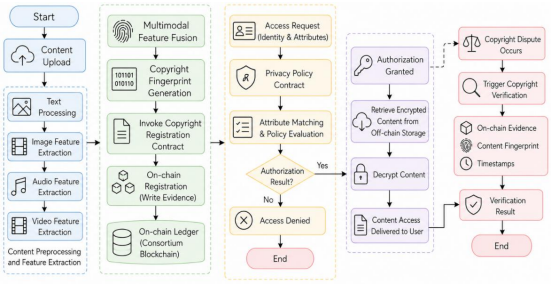

Fig. 2. Operation Flow of the Proposed Model

2.2. Multimodal Copyright Authentication Model

2.2.1. *Industrial New Media Content Feature Representation*

$$C_i = \left\{ x_i^{text}, x_i^{image}, x_i^{audio}, x_i^{video} \right\} \tag{1}$$

Where x_i^{text}, x_i^{image}, x_i^{audio} and x_i^{video} represent text, image, audio, and video components, respectively. After feature extraction for each modality, the fused feature vector shown in eEq. (2) is obtained.

$$F_i = \phi\left(C_i\right) = \left[\phi_t\left(x_i^{text}\right), \phi_v\left(x_i^{image}\right), \phi_a\left(x_i^{audio}\right), \phi_m\left(x_i^{video}\right)\right] \tag{2}$$

In the formula, ϕ_t, ϕ_v, ϕ_a and ϕ_m represent the text semantic coding, visual feature coding, audio spectral coding, and video temporal coding functions, respectively. Compared with a single hash, this representation can preserve the semantics, visual structure, and temporal variation features of the content, and is therefore more suitable for handling secondary editing and minor tampering in industrial new media platforms.

2.2.2. *Copyright Fingerprint Generation*

Based on multimodal features, this study constructs a weighted fusion fingerprint, as shown in Eq. (3).

$$MF_i = \omega_t f_i^{text} + \omega_v f_i^{image} + \omega_a f_i^{audio} + \omega_m f_i^{video}, \quad \sum_{k\in\{t,v,a,m\}} \omega_k = 1 \tag{3}$$

To avoid directly exposing the creator's identity on the blockchain, the system does not use the real identity ID for public registration, but instead uses a dynamic pseudo-identity PID_i^t. The final copyright fingerprint is defined as Eq. (4).

$$CF_i = Hash\left(MF_i \parallel PID_i^t \parallel T_i \parallel Sig_i \parallel H_{meta}\right) \tag{4}$$

Where T_i is the registration timestamp, Sig_i is the creator's digital signature, and H_{meta} is the content metadata digest. This design retains the verifiability required for copyright registration while avoiding directly writing the original content and real identity of the work onto the blockchain.

2.2.3. *Copyright Similarity Verification*

When the system receives suspected infringing content C_j, it first extracts its multimodal features F_j and matches them with the index fingerprint of the registered content on the blockchain. Copyright similarity is calculated using a weighted cosine similarity function, as shown in Eq. (5).

$$S\left(C_i, C_j\right) = \frac{\sum_{k=1}^{d} w_k f_{ik} f_{jk}}{\sqrt{\sum_{k=1}^{d} f_{ik}^2}\sqrt{\sum_{k=1}^{d} f_{jk}^2} + \varepsilon} \tag{5}$$

Considering that copyright judgment depends not only on content similarity but also on time consistency, source credibility, and ownership record reliability, this study further defines the copyright authentication probability as shown in Eq. (6).

$$P_{auth} = \sigma\left(\alpha S\left(C_i, C_j\right) + \beta R_t + \gamma R_s + \delta R_o - \lambda D_{edit}\right) \tag{6}$$

Where R_t represents temporal consistency, R_s represents source credibility, R_o represents the reliability of on-chain ownership records, and D_{edit} represents edit distance or tampering strength. If $P_{auth} \geq \theta$, the system determines that the two content objects have a copyright association.

2.3. Privacy Protection and Access Control Model

2.3.1. *Dynamic Pseudo-Identity Generation*

To reduce the risk of identity association during on-chain registration and access, this study adopts a dynamic

pseudo-identity mechanism. The pseudo-identity of the i user at time t is defined as Eq. (7).

$$PID_i^t = Hash\left(ID_i \parallel Nonce_i^t \parallel T_i \parallel r_i\right) \tag{7}$$

Where ID_i represents the user's real identity, $Nonce_i^t$ is a one-time random number, and r_i is a system-side random salt. Since $Nonce_i^t$ and T_i change over time, it is difficult for attackers to associate the same real user through multiple registration records.

2.3.2. *Attribute Access Control*

Access control adopts an attribute-based scoring model. Suppose user u requests access to resource r, and its attribute matching score is defined as Eq. (8).

$$Score(u,r) = \sum_{m=1}^{M} \lambda_m A_m(u,r) + \eta Trust(u) - \zeta Risk(u) - \chi Freq(u) \tag{8}$$

Where $A_m(u,r)$ represents whether the m attribute satisfies the access policy, $Trust(u)$ represents the user's trustworthiness, $Risk(u)$ represents the risk of abnormal access, and $Freq(u)$ represents the penalty for short-term high-frequency access. The access decision is shown in Eq. (9).

$$Access(u,r) = \begin{cases} 1, & Score(u,r) \geq \tau, \\ 0, & Score(u,r) < \tau. \end{cases} \tag{9}$$

2.3.3. *Privacy Leakage Risk and Optimization Goals*

In order to quantify the privacy risk of the system, this paper defines the privacy leakage rate PLR, as shown in Eq. (10).

$$PLR = 1 - \prod_{i=1}^{N} (1 - p_i q_i \kappa_i s_i) \tag{10}$$

Where p_i represents the node leakage probability, q_i represents the node access probability, κ_i represents the metadata sensitivity coefficient, and s_i represents the proportion of sensitive information stored in the node. The system optimization objective is shown in Eq. (11).

$$\begin{aligned} \max J = {} & \lambda U(Q,R) - (1-\lambda) PLR \\ & - \mu Cost_{enc} - \nu T_{access} - \rho O_{chain} \end{aligned} \tag{11}$$

In the formula, $U(Q,R)$ represents content quality and retrieval availability, $Cost_{enc}$ is the encryption overhead, T_{access} is the access latency, and O_{chain} is the on-chain transaction overhead. This objective function reflects a comprehensive trade-off between privacy protection, system efficiency, and on-chain resource consumption.

2.4. Scalable Storage and Retrieval Mechanism

Considering the large file size, rapid updates, and high access concurrency of industrial new media content, this study does not directly write the original content to the chain but adopts a hybrid on-chain and off-chain storage approach. Copyright fingerprints, content hashes, access policies, and verification logs are stored on the chain, while encrypted original files are stored off-chain. The total on-chain and off-chain storage volume and storage cost are defined by Eq. (12), respectively.

$$\begin{aligned} & D_{total} = D_{chain} + D_{off}, \quad Cost_{store} \\ & = c_1 D_{chain} + c_2 D_{off} + c_3 N_{tx} + c_4 N_{index} \end{aligned} \tag{12}$$

To improve copyright retrieval efficiency, this study constructs a distributed index $Index_i$, as shown in Eq. (13).

$$Index_i = \{CF_i, Hash_i, Location_i, PID_i^t, T_i, Policy_i, V_i\} \tag{13}$$

Where $Location_i$ is the address of the off-chain content, $Policy_i$ is the access policy, and V_i is the verification status. The retrieval response time is defined as Eq. (14).

$$T_q = T_{index} + \max_{1 \leq k \leq K} T_{fetch}^k + T_{verify} + T_{policy} + T_{decrypt} \tag{14}$$

As the number of nodes increases, the system throughput is not only related to the number of nodes but also affected by consensus complexity and network communication pressure. Therefore, this study defines a throughput expansion function, as shown in Eq. (15).

$$TPS(N) = \frac{\eta N}{1 + \mu \log N + \rho C_{cons} + \xi B_{net} + \psi Q_{policy}} \tag{15}$$

2.5. Experimental Design

A large-scale simulation verified the model. The platform used Hyperledger Fabric for the consortium blockchain, IPFS and a distributed metadata database for off-chain storage, and smart contracts for registration, verification, authorisation, and evidence recording. Nodes ranged 10–100, content scale 10K–1M, concurrent users 100–5000. Comparison methods were centralised DRM, Ethereum-based registration, IPFS-only storage, the Fabric baseline, and the proposed model, evaluated for system efficiency, copyright recognition, privacy protection, and security interception via dataset construction, attack sample generation, parameter sensitivity, and stress testing (Table 1).

Table 1. Experimental Environment and Parameter Settings

Project	Set up
Blockchain Platform	Hyperledger Fabric consortium blockchain
Off-Chain Storage	IPFS + Distributed Metadatabase
Node Scale	10, 20, 40, 60, 80, 100
Content Scale	10K, 50K, 100K, 300K, 500K, 1M
Content Type	Text, images, audio, video, mixed media, technical documents
Comparison Method	Centralized DRM, Ethereum-based, Fabric baseline, IPFS-only, Proposed model

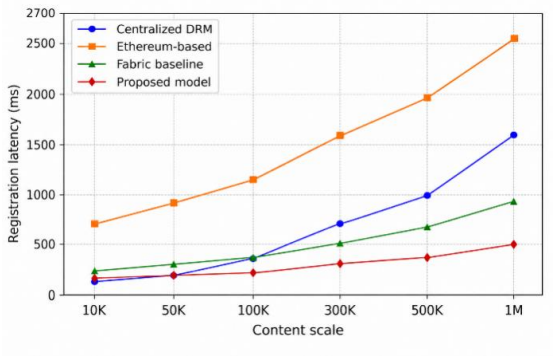

Fig. 3. Comparison of copyright registration latency under different content scales

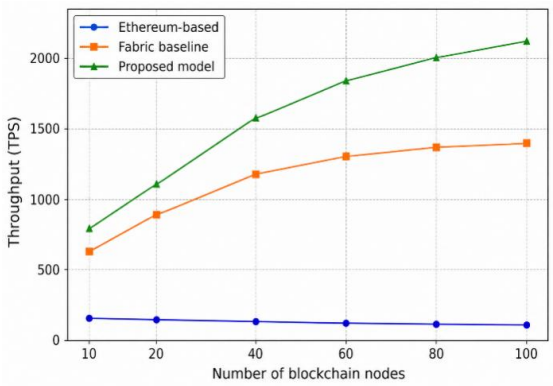

Fig. 4. Comparison of System Throughput under Different Node Sizes

2.5.1. *Simulation Dataset and Attack Sample Construction*

Tampering ratios were set to 10–50%, and suspected infringing samples were matched against on-chain registered samples by similarity. Six privacy-attack types were constructed — identity forgery, replay request, policy bypass, high-frequency crawling, illegal secondary distribution, and on-chain behaviour association — and each experiment was repeated 10 times, with the average taken to reduce the impact of random request arrivals, latency fluctuation, and node-load changes.

These attack samples reflect real infringement and privacy-risk behaviour rather than synthetic noise: for copyright, whether related content remains associable after rewriting or reconstruction; for privacy, whether repeated access or policy-bypass attempts reveal the real creator or trajectory — closer to actual dispute and authorisation scenarios.

The simulation reproduces a multi-institution registration scenario (Table 2) with sorting, endorsement, verification, and client nodes. Smart contracts cover registration, verification, authorisation, and evidence recording; on-chain records include fingerprints, timestamps, pseudo-identities, policies, summaries, and logs; off-chain data (addresses, indexes, access states) uses IPFS and a distributed metadata database. All methods ran under identical scale, concurrency, and node settings.

2.5.2. *Evaluation Metric Calculation Method*

Model performance is evaluated on system efficiency, copyright recognition, privacy protection, and security interception. Registration latency, throughput, retrieval time, and storage overhead measure efficiency; verification accuracy and F1 score measure recognition under tampering; privacy leakage rate measures identity/trajectory inference risk from access logs and on-chain behaviour; and unauthorised-access interception rate and confirmation latency measure security and responsiveness.

For fairness and reproducibility, all comparison methods were evaluated under identical content scale, node scale, concurrency, and tampering-ratio settings, using the same request traces and attack sample groups. Reported results are averages across repeated runs, reducing the influence of random delay, node load, and request-order fluctuation.

3. Results and discussion

3.1. Copyright Registration Latency Analysis

Fig. 3 shows registration latency as scale grows from 10K to 1M: centralised DRM rises quickly under indexing pressure; the Ethereum-based scheme has the highest latency from public-network confirmation; the Fabric baseline still processes heavy metadata at scale. Because the proposed model writes only the fingerprint, summary, and policy

Table 2. Simulation Experiment Parameters and Attack Scenario Settings

Parameter	Set up
Block size	100, 200, 500 transactions/block
Transaction arrival rate	100, 500, 1000, 3000, 5000 requests/s
Endorsement strategy	2-of-N, 3-of-N
Content Scale	10K, 50K, 100K, 300K, 500K, 1M
Tampering with proportions	10%, 20%, 30%, 40%, 50%
Attack type	Identity forgery, replay requests, strategy bypass, high-frequency crawling, illegal distribution, and on-chain behavior correlation
Number of repetitions	Each experiment was repeated 10 times
Statistical methods	Mean + Standard Deviation

on-chain, its latency increases far more gradually.

3.2. Throughput Analysis under Node Expansion

Fig. 4 shows throughput across node scales: the Ethereum-based scheme gains little as nodes increase, owing to heavy consensus; the Fabric baseline is markedly higher but with diminishing gains. By reducing redundant transactions, compressing the data structure, and using off-chain storage, the proposed model sustains 2120 TPS at 100 nodes — about 51.4% above the Fabric baseline.

3.3. Retrieval Response Time Analysis

Fig. 5 shows retrieval response time across content scales. Centralised DRM is fast at small scale but its index comes under heavy pressure at millions of items; IPFS-only storage offers distributed addressing but lacks structured indexes for copyright verification. By associating fingerprints, off-chain locations, and access policies through a distributed index and avoiding full-chain traversal, the proposed model achieves the lowest retrieval latency.

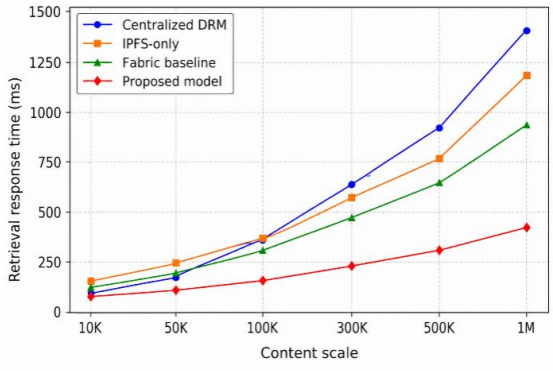

Fig. 5. Comparison of Copyright Retrieval Response Time under Different Content Sizes

3.4. Storage Overhead Analysis

Fig. 6 compares storage overhead across schemes. Full on-chain storage grows sharply with data size; IPFS-only storage reduces on-chain pressure but lacks on-chain evidence and policy management. Because the proposed hybrid scheme stores only summaries, fingerprints, policies, and verification logs on-chain while keeping encrypted originals off-chain, it substantially lowers storage overhead while preserving evidence credibility.

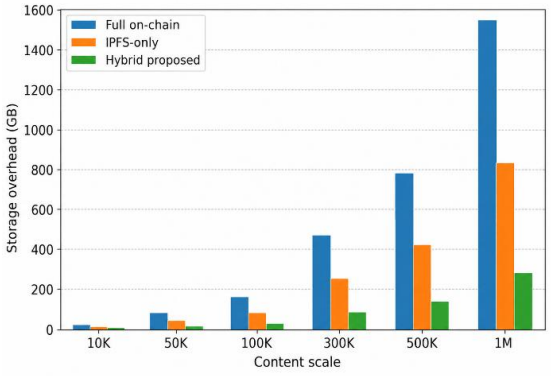

Fig. 6. Comparison of Storage Overhead under Different Storage Schemes

Table 3 shows that at 1M content scale, the proposed model's registration latency is lower than the Fabric baseline and Ethereum-based schemes, since only the fingerprint, digest, policy, and log go on-chain. It sustains high throughput at 100 nodes, confirming hybrid storage and distributed indexing relieve on-chain pressure, and its retrieval time stays below the IPFS-only scheme thanks to the fingerprint-oriented index.

3.5. Copyright Verification Accuracy Analysis

Fig. 7 compares verification accuracy across text, image, audio, video, and mixed-media content. Hash-only methods are sensitive to minor modifications, especially for video and mixed media; feature-matching methods use content features but lack on-chain timestamp and ownership fusion. By incorporating multimodal features, on-chain ownership records, temporal consistency, and source credibility into the authentication probability, the proposed model

Table 3. Comparison of System Efficiency of Different Methods with a Content Scale of Millions

Method	Registration delay/ms	Throughput /TPS	retrieval response/ms	Storage overhead/GB	Confirmation delay/ms
Centralized DRM	1580	-	1410	-	-
Ethereum-based	2550	118	-	-	2260
Fabric baseline	930	1400	940	-	860
IPFS-only	-	-	1180	830	-
Proposed model	490	2120	430	280	560

achieves the highest overall accuracy.

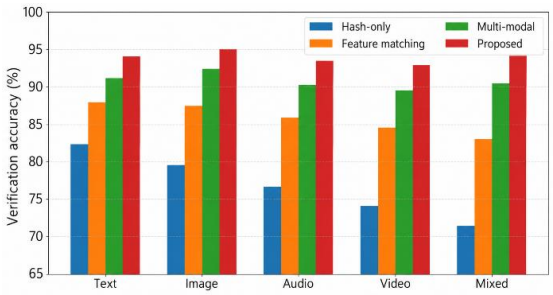

Fig. 7. Comparison of Copyright Verification Accuracy under Different Content Types

3.6. Robustness Analysis of Content Tampering

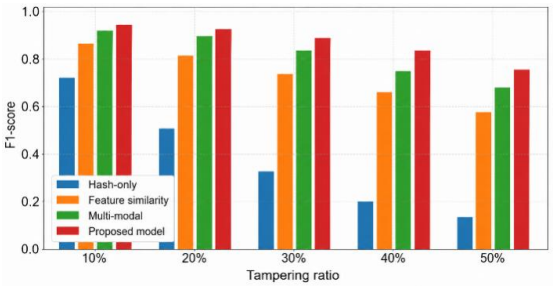

Fig. 8. Comparison of F1 scores under different content tampering ratios

Fig. 9 shows privacy leakage across access-request scales: the no-protection scheme rises sharply; static anonymity is correlated with long-term behaviour; ABAC-only cannot prevent identity association. At 50K requests the proposed model's leakage is 9.4%, lower than both, showing pseudo-identities curb behavioural association, risk scoring suppresses abnormal requests, and off-chain storage limits on-chain exposure.

3.7. Analysis of Unauthorized Access Interception Rate

Fig. 10 compares interception rates across attack types — identity forgery, replay requests, policy bypass, high-frequency crawling, and illegal distribution — as intensity increases. Password-based schemes lack fine-grained

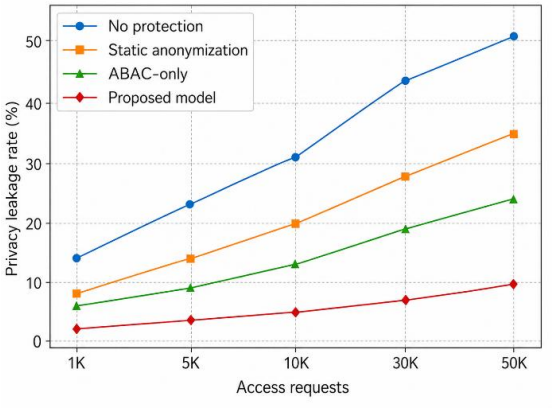

Fig. 9. Comparison of Privacy Leakage Rates under Different Access Request Scales

policy constraints, RBAC struggles to express dynamic attributes, and ABAC offers stronger authorisation. Adding on-chain policy execution, trust scoring, and abnormal-access penalties to ABAC lets the proposed model maintain a high interception rate even under severe attack.

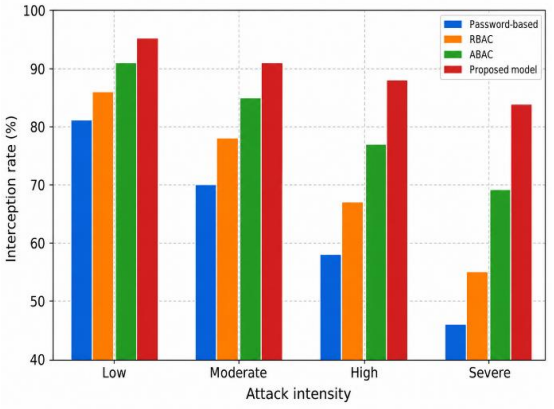

Fig. 10. Comparison of Unauthorized Access Interception Rates under Different Attack Intensities

3.8. Transaction Confirmation Delay Analysis

Fig. 11 shows confirmation delay across consensus workflows. PoW has the highest delay and suits high-frequency

registration poorly; PBFT's communication complexity grows quickly with node count; Raft is faster in consortium settings but still incurs overhead from excessive metadata writing. Rather than proposing a new consensus algorithm, this paper reduces delay by compressing the on-chain transaction structure, limiting original-content writes, and optimising the contract call process.

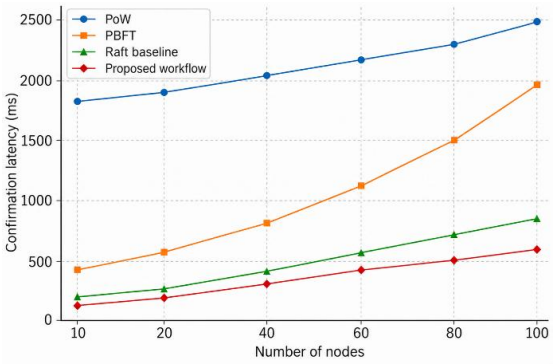

Fig. 11. Comparison of transaction confirmation delays under different node sizes

As Table 4 shows, hash-only fails easily under minor changes, especially at high tampering; feature-matching and multi-modal methods improve similarity recognition but lack on-chain timestamp and credibility constraints. Combining multimodal features with on-chain evidence and source credibility gives the proposed model more stable accuracy and tamper robustness. For privacy, static anonymity and ABAC-only are vulnerable to behavioural or identity association, while the model's pseudo-identities, risk scoring, and off-chain storage achieve the lowest leakage rate.

3.9. t-SNE Feature Distribution Visualization

t-SNE visualisation (Fig. 12) shows the copyright feature space: original and slightly modified content lie close together, indicating identifiable rewritten content; irrelevant content is clearly separated; heavily modified content falls between the two, consistent with similarity decreasing as tampering intensifies.

3.10. Ablation Experiment Analysis

Fig. 13 shows ablation results: removing the privacy module drops the privacy score from 93 to 61; removing IPFS drops throughput to 78; removing the distributed index drops retrieval to 65; removing the multimodal fingerprint drops recognition accuracy to 78 — confirming each module's distinct contribution.

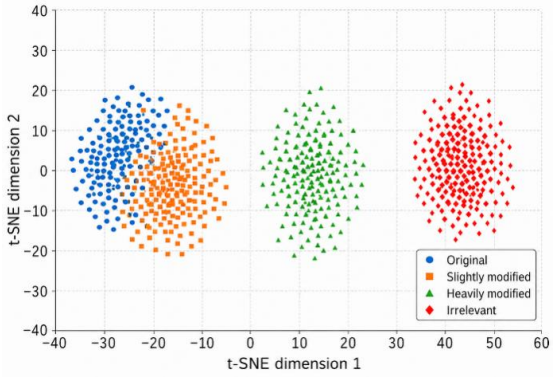

Fig. 12. Visualization of t-SNE distribution of copyright features for industrial new media content

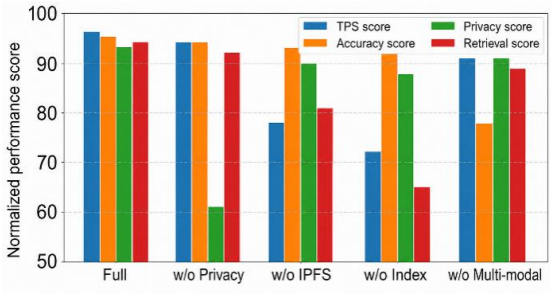

Fig. 13. Comparison of comprehensive performance under different module ablation conditions

3.11. Parameter Sensitivity Analysis

Block size affects latency and throughput: smaller blocks reduce wait time but raise overhead; larger blocks improve batching but may increase wait under high concurrency. 200–500 transactions/block significantly improves throughput while keeping latency acceptable; a higher endorsing-node ratio improves credibility at higher communication cost, so this study adopts 2-of-N or 3-of-N endorsement.

These results suggest the authentication threshold should not be chosen solely for maximum accuracy; a moderate threshold better suits dispute screening by preserving recall for slightly altered content while controlling false positives. Block size and endorsement policy should likewise be tuned to platform workload, evidence-credibility needs, and acceptable confirmation delay.

3.12. High-Concurrency Stress Test

A high-concurrency stress test raised requests from 100 to 5000 across registration, retrieval, and authorisation. Table 6 shows latency rising for all methods but far less for the proposed model: centralised DRM suffers from indexing/database pressure, the Fabric baseline from metadata-driven queue backlog, while the proposed model's off-

Table 4. Overall performance of different methods in security and copyright recognition tasks

Method	Validation accuracy / %	50% F1	Privacy breach rate /%	Interception rate under severe attacks /%
Hash-only	78.1	0.14	-	-
Feature matching	86.2	0.58	-	-
Multi-modal	90.8	0.69	-	-
ABAC-only	-	-	24.3	69.5
Static anonymization	-	-	35.1	-
Proposed model	94.5	0.76	9.4	84.6

Table 5. Sensitivity Analysis Results under Different Parameter Configurations

Parameter configuration	Accuracy/%	Recall rate /%	F1 value	Throughput/TPS	Confirmation delay/ms
Threshold 0.70	91.8	96.2	0.94	2090	552
Threshold 0.80	94.5	94.1	0.94	2120	560
Threshold 0.90	96.0	88.7	0.92	2115	565
Block 100 tx	94.2	93.9	0.94	1760	430
Block 500 tx	94.5	94.1	0.94	2180	610
3-of-N endorsement	94.8	94.0	0.94	1980	640

Table 6. Comparison of Average Response Time under High Concurrency Conditions

Concurrent request count	Centralized DRM/ms	Fabric baseline/ms	IPFS-only/ms	Proposed model/ms
100	120	160	150	95
500	210	240	230	130
1000	360	390	340	175
3000	780	690	610	260
5000	1280	980	860	380

chain storage, on-chain summaries, and distributed indexing keep processing capacity relatively stable.

As shown in Table 6, the proposed model's average response time is 380 ms at 5000 concurrent requests, well below centralised DRM, the Fabric baseline, and IPFS-only — confirming that hybrid storage, distributed indexing, and contract-process compression improve applicability under high-concurrency conditions.

3.13. Discussion on Security and Scalability

For tamper protection, the model writes fingerprints, timestamps, metadata summaries, and verification logs to the consortium blockchain, so an attacker modifying a copyright record must disrupt both the consensus process and on-chain history, greatly raising the cost of tampering. For replay-attack protection, the dynamic pseudo-identity function's random numbers and timestamps prevent expired requests from passing contract expiration checks.

For unauthorised-access protection, smart contracts enforce attribute, trust, and risk constraints before granting authorisation, so even an obtained access record does not readily reveal subsequent valid identities and keys. For content privacy, original content is never written on-chain — only summaries and indexes are — limiting the exposure risk of a public ledger.

For scalability, the model eases large-scale system burden through hybrid on-chain/off-chain storage (reducing on-chain data bloat), distributed indexes (avoiding full-chain traversal during retrieval), and transaction/contract compression (reducing confirmation latency). Beyond individual-metric gains, it achieves a relatively balanced overall performance across throughput, latency, privacy, robustness, concurrency stress, and parameter stability.

The model can be deployed incrementally: a platform may first add on-chain fingerprint registration and off-chain encrypted storage for new content, then extend distributed retrieval and smart-contract authorisation to high-value or high-risk categories. Cross-platform deployment also needs governance rules for identity-credential issuance, key recovery, evidence export, and dispute verification — factors that do not change the core model but affect how efficiently it can be adopted in practice.

This study addresses copyright challenges for industrial new media content — complex infringement, high on-chain storage pressure, and privacy exposure — via a model integrating blockchain, multimodal copyright fingerprinting, dynamic pseudo-identity, attribute access control, and hybrid on-chain/off-chain storage. At a content scale of millions, it reduces registration latency to 490 ms, reaches 2120

TPS and 430 ms retrieval time, and outperforms centralised DRM, Ethereum-based, Fabric baseline, and IPFS-only solutions. Multimodal features combined with on-chain ownership evidence give 94.5% verification accuracy and an F1 score of 0.76 at 50% tampering, showing robustness to rewriting, cropping, transcoding, and mixed-media reconstruction. Dynamic pseudo-identities, risk scoring, and off-chain storage cut the privacy leakage rate to 9.4% and achieve 84.6% interception under severe attack. Limitations include reliance on simulated datasets rather than real deployment, and preset fingerprint weights, thresholds, and endorsement strategies. Future work should incorporate real platform data, federated learning, zero-knowledge proofs, adaptive parameter optimisation, cross-platform governance, and key recovery to move toward long-term operation in real media ecosystems.

References

[1] X. Chen, A. Yang, J. Weng, Y. Tong, C. Huang, and T. Li, (2023) *"A Blockchain-Based Copyright Protection Scheme with Proactive Defense"* **IEEE Transactions on Services Computing *16***(4): 2316–2329. DOI: 10.1109/TSC.2023.3246476.

[2] Y. Liu, J. Zhang, S. Wu, and M. S. Pathan, (2021) *"Research on Digital Copyright Protection Based on the Hyperledger Fabric Blockchain Network Technology"* **PeerJ Computer Science *7***: e709. DOI: 10.7717/peerj-cs.709.

[3] R. F. Ciriello, A. C. G. Torbensen, M. R. P. Hansen, and C. Müller-Bloch, (2023) *"Blockchain-Based Digital Rights Management Systems: Design Principles for the Music Industry"* **Electronic Markets *33***(1): 1–21. DOI: 10.1007/s12525-023-00628-5.

[4] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, (2021) *"Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection"* **IEEE Transactions on Emerging Topics in Computing *9***(3): 1410–1420. DOI: 10.1109/TETC.2020.2993032.

[5] J. Han, Z. Li, J. Liu, H. Wang, M. Xian, Y. Zhang, and Y. Chen, (2022) *"Attribute-Based Access Control Meets Blockchain-Enabled Searchable Encryption: A Flexible and Privacy-Preserving Framework for Multi-User Search"* **Electronics *11***(16): DOI: 10.3390/electronics11162536.

[6] Y. Zhang, M. Yutaka, M. Sasabe, and S. Kasahara, (2021) *"Attribute-Based Access Control for Smart Cities: A Smart-Contract-Driven Framework"* **IEEE Internet of Things Journal *8***(8): 6372–6384. DOI: 10.1109/JIOT.2020.3033434.

[7] E. Chen, Y. Zhu, Z. Zhou, S.-Y. Lee, W. E. Wong, and W. C.-C. Chu, (2022) *"Policychain: A Decentralized Authorization Service with Script-Driven Policy on Blockchain for Internet of Things"* **IEEE Internet of Things Journal *9***(7): 5391–5409. DOI: 10.1109/JIOT.2021.3109147.

[8] S. Ma and X. Zhang, (2024) *"Integrating Blockchain and ZK-Rollup for Efficient Healthcare Data Privacy Protection System via IPFS"* **Scientific Reports *14***: DOI: 10.1038/s41598-024-62292-9.

[9] S. M. Darwish, M. M. Abu-Deif, and S. M. Elkaffas, (2024) *"Blockchain for Video Watermarking: An Enhanced Copyright Protection Approach for Video Forensics Based on Perceptual Hash Function"* **PLOS ONE *19***(10): DOI: 10.1371/journal.pone.0308451.

[10] Q.-Y. Zhang, G.-R. Wu, R. Yang, and J.-Y. Chen, (2024) *"Digital Image Copyright Protection Method Based on Blockchain and Zero Trust Mechanism"* **Multimedia Tools and Applications *83***(32): 77267–77302. DOI: 10.1007/s11042-024-18514-3.

[11] J. Wang, D. Wu, L. Li, J. Zhao, H. Wu, and Y. Tang, (2023) *"Robust Periodic Blind Watermarking Based on Sub-Block Mapping and Block Encryption"* **Expert Systems with Applications *224***: DOI: 10.1016/j.eswa.2023.119981.

[12] A. Fkirin, G. Attiya, A. El-Sayed, and M. A. Shouman, (2022) *"Copyright Protection of Deep Neural Network Models Using Digital Watermarking: A Comparative Study"* **Multimedia Tools and Applications *81***(11): 15961–15975. DOI: 10.1007/s11042-022-12566-z.

[13] X. Xiao, X. He, Y. Zhang, X. Dong, L.-X. Yang, and Y. Xiang, (2023) *"Blockchain-Based Reliable Image Copyright Protection"* **IET Blockchain *3***(4): 222–237. DOI: 10.1049/blc2.12027.

[14] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, (2021) *"A Secured Distributed Detection System Based on IPFS and Blockchain for Industrial Image and Video Data Security"* **Journal of Parallel and Distributed Computing *152***: 128–143. DOI: 10.1016/j.jpdc.2021.02.022.