

INTECHAIGHT: A Blockchain-Integrated Framework for Authorship Verification and Originality Protection of Digital Images

Iniyavan K¹, Harinee S², and Pothumani S³

¹Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India iniyavan3407@gmail.com

²Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India harinee041007@gmail.com

³Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India pothumani.cse@sathyabama.ac.in

Abstract. The fast development of the digital image distribution has worsened the issues related to copyright violations, unlicensed use, and derivative plagiarism. At the same time, the existing centralized protection systems remain vulnerable to manipulations and rights claims. The framework presented in this paper is known as Intechaight, an implementation of blockchain in an automated digital image copyright protection system that is proposed to check image originality. The suggested system organizations a hybrid plagiarism detection model, combining perceptual hashing (pHash) to analyze structural similarities and CLIP-based embedding to identify semantic similarity and EfficientNet-B0 features to detect visual similarity, ensuring effective exercise to copy, transform or semantically derived images. In order to achieve traceability of the ownership, a frequency-domain DCT-based watermarking method that uses ReedSolomon error correction is utilized; using this allows the embedded ownership information to resist common image manipulations. A smart contract is used to store cryptographic hash of the original image, extracted fingerprint and embedded watermark immutably, stored on the zkSync blockchain along with the wallet address of the creator and the time they were created. It leads to the creation of a decentralized registry that provides tamper-resistant, verifiable authorship evidence, and supports automated adjudication and tracking and is able to produce legal evidence. As it is illustrated by experimental results, the proposed solution is able to attain a good balance between robustness, accuracy, and deployability, which makes it suitable to be used in real-life implementations of copyright protection of digital images.

1 Introduction

There has been a greater number of digital images on online social networks that have significantly increased the difficulties of copyright infringement, unauthorized usage, and derivative plagiarism. As more image editing software and generative models become more accessible, they become easily manipulated, redistributed, or monetized without the authorization of their creation, making the established methods of copyright enforcement obsolete. Traditional centralized models of copyright management have single-point-of-failure weaknesses, inability to effectively verify ownership, and have little protection against malpractice or post-distribution challenges. Empirical studies have examined blockchain-based DRM solutions in order to overcome such constraints through the support of immutability, decentralization, and date-stamps. The copyright protection system demonstrated by Zhang et al. [1] is based on blockchain and applies the principles of zero-trust to increase ownership verification and traceability. Likewise, Li et al. [2] revealed that smart contracts are effective in the digital copying of media into the decentralized registries to effectively control copyrights. The approaches create secure records of ownership, though they mostly rely on the assumption that the registered material has not been altered and do not adequately deal

with the identification of modified and semantically derived copies. Frequency domain watermarking It was found that frequency domain watermarking techniques offer greater resistance to content manipulation. The watermarking scheme proposed by Singh and Verma [3] as a combination of DCT watermarking with error-correcting codes has shown a high level of resistance to compression and signal distortion. Lightweight authentication of images can also be achieved using perceptual hashing, which is not based on pixel perceptions but instead captivates the structural features of images [4] Nonetheless, perceptual hashes do not sufficiently identify images with similar semantics or highly transformed ones. The developments in the field of deep visual representation learning have facilitated the processing of similarity at semantic level with image analysis. The CLIP-based embeddings [5] enable the cross-modal perception of visual representations, whereas the discriminative representations of visual features are offered by convolutional neural networks like EfficientNet [6]. These techniques provide a great contribution to the detection of plagiarism, but do not have embedded protocols to support the existence of unalterable ownership evidence or legal tracking. Blockchain-based proof-of-existence systems [7] and legal admissibility of blockchain evidence research workforce the relevance of cryptographic hash functions and timestamps as

evidence of law. Combination with blockchain: It has also been discussed to integrate watermarking with blockchain: Existing systems may either be based on single-factor verification or merely moderate resilience to strong image transformations. The paper is inspired by such constraints which offer a solution called Intechaight which is an integrated system comprising of hybrid image plagiarism detection, powerful frequency domain watermarking, and authorship verification by blockchain-based systems. The proposed system offers the compliment of perceptual hashing, deep semantic embedding and visual feature extraction with DCT-based watermarking and zkSync blockchain registration to offer an all parameter, tamper resistant system of protecting copyrights and identity of the digital image owner.

2 Related Works

The recent interest in digital copyright protection of image has increasingly developed the incorporation of blockchain technology and digital watermarking, as well as similarity analysis in image, to overcome the challenges associated with the verification of ownership, tamper resistance and court admissibility. Zhang et al. [1] devised a blockchain-based architecture that has a zero-trust mechanism, wherein image hashes and ownership information are stored in an immutable manner, as such, to provide verifiable proofs of authorship. Equally, Li et al. [2] developed a decentralized copyright management system of digital media and proved that smart contracts can self-enforce the registration of ownership and access control not depending on centralized authorities. These additions make blockchain a reliable platform to time-stamps and proof of ownership, but do not concern the thorough detection of plagiarism under the conditions of image modification.

Frequency-domain watermarking methods have received much research to enhance resistance against unauthorized modifications. Singh and Verma [3] developed a DCT based watermarking algorithm along with error correcting codes and obtained a fair resistance of compression as well as signal distortions. Zhaoxiong et al. [9] also extended the methodology of watermarking by incorporating the role of blockchain in managing copyright, thus highlighting the benefits of using blockchain technology to imbue ownership data in addition to having an immutable ledger. Zero-watermarking methods, such as the one suggested by Wang et al. [10], do not require direct interaction with the contents of the images but they still can be copyrighted by extracting the features and registering them with blockchain.

One of the research directions is the sphere of image similarity judgement and plagiarism. Kang et al. [4] came up with a perceptual hashing algorithm that has the ability to determine near duplicate images even when subjected to some standard transformations. However, perceptual hashing in itself is poor in representing semantic similarity. In order to address this problem, they have been replaced with semantic-level deep learning embeddings. Radford et al. [5] proposed CLIP model, which

states the semantic image representation; at the same time, Tan and Le [6] provided EfficientNet that provides efficient and discriminative visual feature extraction. In spite of the fact that these models have been widely used in similarity analysis, they are not combined with blockchain-based legal proof mechanisms.

Cryptographic hashes and timestamps can be used to prove a claim of ownership of digital assets, as in blockchain-based proof-of-existence systems, including the project by Wang et al. [7]. Moreover, Finck [8] studied the legality of evidence obtained with the help of blockchains, which is increasingly relevant in the field of digital forensics and copyright lawsuits. Although these developments have been made, the current literature is more focused on individual items- blockchain, watermarking or plagiarism detection, but it does not offer an integrated, multi-faceted model.

3 Proposed System

3.1 System Overview

In this paper, it will suggest the Intechaight infrastructure, which is the multi-layer hybrid authorship validation model, combining powerful watermarking and deep visual-semantic fingerprinting with blockchain-based ownership attestations. There are four major layers of operation in the system architecture:

System Architecture

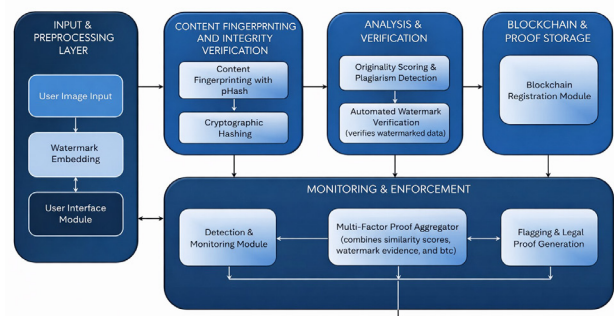


Figure 1. Multi-layer architecture for evaluating AI fingerprinting, watermark authentication, and blockchain certificates of provenance storage.

The methodology is based on five consecutive steps:

- (1) Image preprocessing and image input.
- (2) Content fingerprinting and integrity checking.
- (3) Intelligence-based originality and comparison.
- (4) Proof registration in the blockchain.
- (5) Multi-factor proof aggregation and monitoring.

Let an input image be represented as :

$$I \in RH \times W \times C \quad (1)$$

where H, W, and C represent the image height, image width and channels respectively.

3.2 Image Preprocessing and Image Input

The input layer has the effect of normalizing, colour-space separation as well as preparing towards watermark embedding.

3.2.1 Preprocessing Transformation

$$I_n = \frac{I - \mu}{\sigma} \quad (2)$$

where

μ = dataset mean vector,

σ = dataset standard deviation vector

Such change ensures that there is consistent extraction of the features between EfficientNet and CLIP pipelines.

3.2.2 Watermarking Model (DCT ReedSolomon Protected)

The watermark payload W_d is coded with the help of the ReedSolomon error correction:

$$C(u, v) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} B(x, y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \times \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (3)$$

Watermark embedding rule:

$$\begin{cases} C(4, 3) = C(4, 3) + S, & \text{if bit} = 1 \\ C(3, 4) = C(3, 4) + S, & \text{if bit} = 0 \end{cases} \quad (4)$$

where S is the embedding strength.

Algorithm 1 Ultra-Strong Watermark Embedding

Require: Input image I , watermark W , embedding strength S

Ensure: Watermarked image I_w

- 1: Encode W using Reed–Solomon coding to obtain W_{rs}
 - 2: Convert W_{rs} into a binary bitstream
 - 3: Convert I to the YCrCb color space
 - 4: **for** each 8×8 block in the Y channel **do**
 - 5: Compute the DCT coefficients
 - 6: Modify the mid-frequency coefficients based on the current bit
 - 7: Apply the inverse DCT
 - 8: **end for**
 - 9: Merge the Y, Cr, and Cb channels to obtain I_w
 - 10: **return** I_w
-

The watermark embedding procedure is summarized in Algorithm 1.

The use of mid-frequency coefficients gives it resistance to JPEG compression and luminance distortion, and thus, maintains perceptual fidelity. Reed Solomon redundancy enables recovery with stochastic noise and adversarial perturbations and is thus compatible with applications in the real world where social media is being repressed.

3.3 Content Fingerprinting and Integrity Checking

Fingerprint module combines structural representations with semantic representations and deep learned visual representations.

3.3.1 Robust Structural Fingerprint (pHash)

Structural similarity:

$$S_{pHash} = \frac{64 - dH(H_a, H_b)}{64} \quad (5)$$

where d_H is Hamming distance. Mirror in-variant score:

$$S_{pHash} = \max(S_{orig}, S_{flip}) \quad (6)$$

It improves the ability to resist to geometrical manipulations, including horizontal flipping, which is a common technique used in plagiarism evasion.

3.3.2 Semantic Similarity (CLIP)

Normalized embedding:

$$E_{CLIP} = \frac{f_{clip}(I)}{\|f_{clip}(I)\|} \quad (7)$$

Similarity:

$$S_{clip} = \cos(E_a, E_b) \quad (8)$$

The conceptual high similarity at a higher level is captured by CLIP and thus it is easy to identify some copying or theft in styles and semantics that goes beyond the similarity of pixels.

3.3.3 Deep Visual Feature Similarity (EfficientNet)

Feature vector normalization:

$$E_{CLIP} = \frac{f_{eff}(I)}{\|f_{eff}(I)\|} \quad (9)$$

Similarity:

$$S_{eff} = \cos(E_{eff,a}, E_{eff,b}) \quad (10)$$

EfficientNet uses fine-grained texture, structure, and object-level visual representations, which supplements semantic cognition by CLIP.

3.3.4 Weighted Similarity Fusion

$$S_{final} = 0.5S_{eff} + 0.3S_{clip} + 0.2S_{struct} \quad (11)$$

The relative weights are based on an empirically collected significance on visual feature similarity as the contexts of derivative image plagiarism. Algorithm 2 shows the procedure for computing the final similarity score using a multi-modal fusion of structural, semantic, and visual features.

Algorithm 2 Multi-Modal Similarity Computation

Require: Query image I_q , Reference image I_r , fusion weights $\{w_1, w_2, w_3\}$

Ensure: Final similarity score S_{final}

- 1: Compute pHash similarity $\rightarrow S_{\text{struct}}$
- 2: Compute CLIP embedding similarity $\rightarrow S_{\text{clip}}$
- 3: Compute EfficientNet feature similarity $\rightarrow S_{\text{eff}}$
- 4: Compute weighted fusion:

$$S_{\text{final}} = w_1 S_{\text{struct}} + w_2 S_{\text{clip}} + w_3 S_{\text{eff}}$$

- 5: **return** S_{final}
-

3.4 Analysis and Verification

The extraction of watermarks using an automated method is performed through inverse discrete cosine transform (IDCT) analysis with the use of ReedSolomon (RS) decoding. The retrieval of the embedded payload reaches its objective, and creates a cryptographic association between the image of the suspect and the registered ownership information. The thresholds of plagiarism confidence based on the direct results of program, m , allow categorizing the cases as original, suspicious and high-confidence cases.

3.5 Proof Registration in blockchain

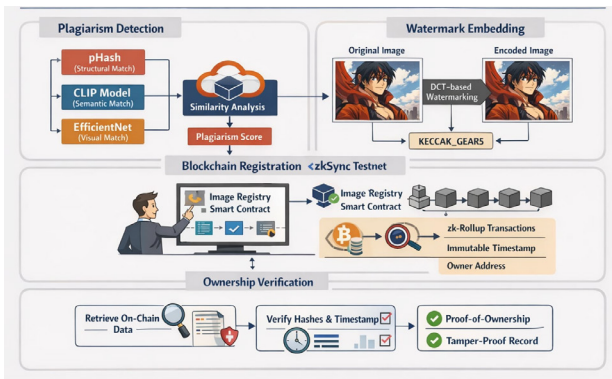


Figure 2. Workflow of blockchain

Hash generation:

$$\begin{aligned} H_{img} &= SHA256(I) \\ H_{fp} &= SHA256(\text{Fingerprint}) \\ H_{wm} &= SHA256(\text{Watermark}) \end{aligned} \quad (12)$$

On-chain record tuples:

$$R = (H_{img}, H_{fp}, H_{wm}, \text{Owner}, \text{BlockNo}, \text{Timestamp}) \quad (13)$$

The zkSync Layer 2 architecture provides an inexpensive immutable timestamping and enjoys the security properties of Ethereum Layer 1.

Multi-hash framework is also useful in avoiding substitution attacks by making sure that distortions to a watermark or a fingerprint does not reduce the integrity of the evidence.

Algorithm 3 Blockchain Registration

Require: Image hash set $\{H_{img}, H_{fp}, H_{wm}\}$

Ensure: Proof record P

- 1: Generate SHA256 hashes of image, fingerprint, and watermark
 - 2: Connect to user blockchain wallet
 - 3: Call smart contract function `registerImage()`
 - 4: Wait for transaction confirmation
 - 5: Store local proof metadata
 - 6: **return** proof record P
-

3.6 Multi Factor Proof Aggregation and Monitoring

Verification function:

$$\text{verify}(I_q) = \begin{cases} \text{True}, & H_{img}(I_q) \in \text{Blockchain} \\ \text{False}, & \text{otherwise} \end{cases} \quad (14)$$

The automation of copyright protection and the owners verification is simpler through permanent watching. Evaluation and training is based on real and heterogeneous data sets.

3.7 Dataset Description

There was a heterogeneous dataset used in the evaluation and contained original photos as well as modified versions of the original photos, which encompassed resizing, compressing, changing colors, mirroring, cropping, and semantic re-rendering. Both drawings and real life pictures were used to evaluate the strength in visual domains.

4 Results and Discussion

The current section is the full assessment of the intended Intechaight framework, consolidating image plagiarism detection on the basis of deep-learning, the watermarking on the robust bases of DCT in addition to blockchain-based ownership due to zkSync Era. The effectiveness, robustness, and practical feasibility of the system in the real world is shown using experimental results.

4.1 Image Plagiarism Detection Performance

The plagiarism detection module combines structural, semantic, and visual similarity analysis using pHash, CLIP, and EfficientNet respectively. This multimodal design prevents common evasion techniques such as mirroring, recoloring, or partial editing. Table 1. summarizes the similarity scores obtained for a representative test case involving an original image (gear5.jpg) and a suspected derivative image (luffy.jpg). The final plagiarism probability is computed using a weighted fusion strategy (EfficientNet 50%, CLIP 30%, pHash 20). A score of 49.4% falls within the Suspicious Similarity range, indicating that the suspect image is likely edited or derived rather than an exact duplicate.

This result confirms that the proposed approach successfully captures conceptual similarity even when low-level pixel resemblance is reduced, a key limitation in traditional hash-only plagiarism systems.

Table 1. Multi-Modal Similarity Scores

Feature Type	Model Used	Similarity Score
Structural	pHash	53.12
Semantic	CLIP	78.07
Visual	EfficientNet	30.71
Final Score	Weighted Fusion	49.40

```
PS D:\sem_viii\fyf\intechaight\plagiarism> python multimodel2.py
Loading AI Models... (This happens once)
[✓] Models Loaded Successfully.

Comparing:
1. D:\sem_viii\fyf\intechaight\plagiarism\plagiarism data\gear5.jpg
2. D:\sem_viii\fyf\intechaight\plagiarism\plagiarism data\luffy.jpg

=====
✎ PLAGIARISM PROBABILITY: 49.4%
=====
Detailed Breakdown:
- Structural Match (pHash): 53.12%
- Concept Match (CLIP): 78.07%
- Visual Match (EffNet): 30.71%
=====
🚫 VERDICT: Suspicious Similarity (Likely Edited/Derived).
```

Figure 3. Output of the Proposed AI-Based Image Plagiarism Detection System

4.2 Robustness of DCT-Based Watermarking

To ensure ownership traceability, an ultra-strong invisible watermark was embedded into the luminance channel of the image using mid-frequency DCT coefficient modulation combined with Reed–Solomon error correction.

During experimentation, a 176-bit watermark payload encoding a cryptographic identifier (KECCAK_GEAR5) was embedded without introducing visible artifacts. Successful extraction was achieved after recompression and minor image modifications.

```
PS D:\sem_viii\fyf\intechaight\watermarking_project> python dct.py
Attempting to create watermarked image...
Embedding Complete. Embedded 176 bits.
SUCCESS! Your watermarked image is at: D:\sem_viii\fyf\intechaight\watermarking_project\watermarkdata\dot.jpg
DEBUG: Extracted bytes (ASCII): [75, 69, 67, 67, 65, 75, 95, 71, 69, 65, 82, 53]
EXTRACTED RESULT: KECCAK_GEAR5
```

Figure 4. Digital Watermark Embedding and Extraction Result Using DCT

The extracted watermark bytes matched the original payload, demonstrating high robustness against signal noise and compression distortions. The use of mid-frequency coefficients ensures resistance against both spatial attacks and common JPEG compression pipelines. These results validate the suitability of the watermarking module for forensic-grade ownership protection.

4.3 Blockchain-Based Ownership Verification on zkSync

The ownership verification layer was deployed on the zkSync Era Sepolia testnet, leveraging its low gas cost and zero-knowledge rollup security guarantees. Each image is registered on-chain using three cryptographic hashes:

- Image content hash

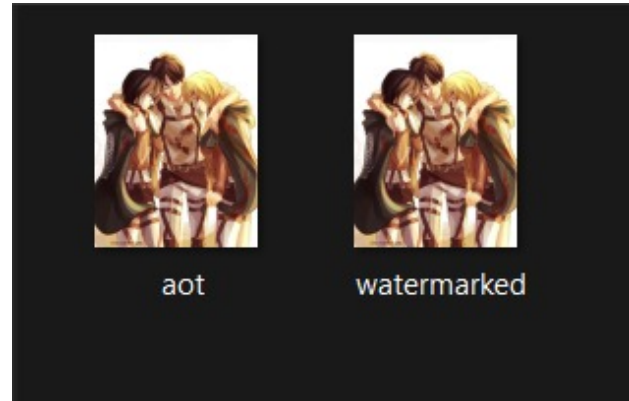


Figure 5. Visual Comparison of Original and Watermarked Images

- Fingerprint (feature) hash
- Watermark hash

Upon successful registration, the blockchain permanently stores the image metadata along with the block number and timestamp. The recorded data confirms:

- Verified wallet ownership
- Immutable registration timestamp
- Tamper-proof storage of image fingerprints

This ensures non-repudiable proof of ownership, which is critical for copyright enforcement, digital forensics, and intellectual property disputes.

```
IMAGE OWNERSHIP VERIFICATION RESULT
{
  imageHash: '0xba9ff5fc986ee8f6dc3da3e4fdae2b9ef6e5ad6be859402ec7eb696788ffef',
  fingerprintHash: '0xba9ff5fc986ee8f6dc3da3e4fdae2b9ef6e5ad6be859402ec7eb696788ffef',
  watermarkHash: '0xf3de80d9409518ee06c5f8ca4e86e8c32ecc813bb0938cc09a6f9afd29592eaf',
  owner: '0xe9f6c1c8588f277023cb372140dA337634E9Fa08',
  registeredBy: '✓Verified Owner',
  contractAddress: '0x7c42E60A155eCf982CCBa51aBe49057865aF51de',
  blockNumber: '6694246',
  timestampUTC: '2026-02-04T07:56:55.000Z',
  transactionHash: '0x79e68786d34800a3226dc7ef43a4bfffbb4e0e4f2027fd02dab76c25d1e0061',
  imagePath: 'D:\\sem_viii\\fyf\\intechaight\\zksync\\images\\luffy.jpg',
  proofSummary: '✓Image exists on-chain with immutable timestamp and ownership'
}
```

Figure 6. Blockchain-Based Image Ownership Verification Result

4.4 End to End System Discussion

The similarity method based on AI and ownership verification through blockchain forms the flawless lifecycle solution to protect digital images.

The proposed framework is an improvement over other existing systems that use watermarking or hashing, because:

- Derivative plagiarism is detected,
- Religion of ownership as obscurity.
- Indestructible legal evidence in the blockchain.

In addition, transaction costs are significantly lowered with the introduction of zkSync which makes the system suitable to large image repositories.

One of the drawbacks of the existing implementation is presented in the computational cost related to deep neural inference, which can be addressed in future research by using lightweight vision transformers or using batches.

4.5 Comparative Advantage

Intechaight clearly offers as compared to traditional plagiarism detection systems:

- Login plagiarism: plagiarism of varied nature (via CLIP).
- Recovery of error corrupt watermarks.
- Fractional roll-up-secured ownership proof with zero-knowledge.

These combined functions make the system an advanced system of protection of digital content.

5 Conclusion

The proposed paper presents Intechaight, a multifaceted and resistant to any types of tampering image plagiarism detector and ownership identifier. This system combines the usage of deep-learning-driven similarity analysis, watermarking with using robust DCT-domain watermarks, and blockchain-duncanoon / proof of ownership with the help of zkSync Era. The proposed architecture is directly aimed to overcome such serious shortcomings of traditional image protection methods as the lack of semantic interpretation, forensic resilience, and unalterable registration by incorporating all three fundamentals in a single pipeline.

As per an experimental assessment, the multimodal plagiarism detection model effectively identifies edited files together with derivative files, even those files that have undergone a structural change like mirroring, resizing and image enhancement.

By combining pHash structural analysis, CLIP semantic similarity, and the use of EfficientNet extracting visual features, the system improves detection reliability of non-identical instances of plagiarism by reducing the shortcomings of single-model strategies and significantly increases those of the former.

Modulation of mid-frequency DCT coefficients and supported by Reed-Solomon error correction led to the watermarking module, which successfully embedded and extracted the watermark invisibly and did not suffer noticeable image distortion. The ability of the watermark to resist compression artifacts and moderate signal noise is proven by empirical results and renders the watermark successful in when it comes to ownership recovery in practice.

In addition, the blockchain ownership layer deployed on the zkSync Era Testnet provides cryptographically verifiable records of ownership with timestamps, and which

are immutable. The framework ensures non-repudiable ownership of any image because of storing image hashes, fingerprint information, and watermark identifiers in the blockchain so as to maintain low transaction fees, as well as scalability through the use of zero-knowledge rollups. This combination creates the traceability of a legal level, which makes the proposed methodology appropriate to implementations in the fields of copyright protection, digital forensics, and content-verifying.

In general, the suggested Intechaight framework can work positively to overcome the lack of a link between AI-based plagiarism detection and decentralized trust framework in the context of providing resilient and scalable protection of digital visual content.

References

- [1] Y. Zhang, X. Liu, H. Wang, L. Chen and Z. Zhao, Digital image copyright protection method based on blockchain and zero-trust mechanism, *IEEE Trans. Inf. Forensics Secur.* **19**, 4123–4136 (2024)
- [2] J. Li, S. Chen and Y. Xu, Blockchain-based secure copyright management for digital media, *IEEE Trans. Multimedia* **26**, 1124–1137 (2024)
- [3] D. Singh and P. Verma, Robust frequency-domain image watermarking using DCT and error-correcting codes, *IEEE Trans. Circuits Syst. Video Technol.* **34**(2), 1245–1258 (2024)
- [4] X. Kang, J. Huang and Y. Q. Shi, Robust perceptual image hashing for content authentication, *IEEE Trans. Image Process.* **33**, 1501–1514 (2024)
- [5] A. Radford et al., Learning transferable visual models from natural language supervision, *IEEE Trans. Pattern Anal. Mach. Intell.* **45**(2), 2034–2050 (2023)
- [6] M. Tan and Q. V. Le, EfficientNet: Rethinking model scaling for convolutional neural networks, *IEEE Trans. Pattern Anal. Mach. Intell.* **44**(9), 5359–5374 (2022)
- [7] S. Wang, Y. Li, Z. Chen and H. Zhang, Blockchain-based proof of existence and ownership for digital assets, *Future Gener. Comput. Syst.* **145**, 12–25 (2024)
- [8] M. Finck, Blockchain evidence and digital forensics, *Comput. Law Secur. Rev.* **50**, 105781 (2024)
- [9] M. Zhaoxiong, T. Morizumi, S. Miyata and H. Kinoshita, Design scheme of copyright management system based on digital watermarking and blockchain, in *Proc. IEEE Int. Conf. Comput., Softw., Appl. (COMPSAC)*, 1–10 (2024)
- [10] B. Wang, J. Shi, W. Wang and P. Zhao, A blockchain-based system for secure image protection using zero-watermark, in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sens. Syst. (MASS)* (2025)