A Blockchain and Improved Perception Hash Based Copyright Protection Scheme for Purely Chromatic Background Images

Guangyong Gao, Tongchao Feng, Chongtao Guo, Zhihua Xia, *Member, IEEE*, and Yun-Qing Shi, *Life Fellow, IEEE*

***Abstract*—Purely chromatic background images are widely used in computer wallpapers and advertisements, leading to issues such as copyright infringement and the loss of interest of holders. Image hashing is a technique used for comparing the similarity between images, and is often used for image verification, search, and copy detection due to its insensitivity to subtle changes in the original image. In a purely chromatic background image, the central detail of the image is the primary part and the key for copyright authentication. As the perception hash (pHash) algorithm only retains the low-frequency portion of the discrete cosine transform (DCT) matrix, it is unsuitable for purely chromatic background images. To deal with this issue, we propose an improved perception hash (ipHash) algorithm to enhance the universality of the algorithm by extracting purely chromatic background image features. Meanwhile, the development of image hashing is restricted due to the requirement of a trusted third party. To solve this issue, a secure blockchain-based image copyright protection scheme is designed. It realizes the copyright authentication and traceability, and overcomes the issue of a lack of trusted third parties. Experimental results show that the proposed method outperforms the state-of-the-art image copyright protection schemes.**

***Index Terms*—Blockchain, image copyright protection, perceptual hash, smart contract.**

I. Introduction

THE rapid development of the mobile Internet has accelerated the circulation of multimedia information. As a result, it has become more and more common for original images to be misappropriated by others. In this case, the infringer uses the image processing technology to make minor changes to an original image, then uploads the doctored image and obtains the copyright of the work. Purely chromatic background images are an image type with a single color background, i.e., the entire background area is covered by a uniform color. This design causes the graphic elements at the center of the image to stand out, effectively focusing the viewer's attention on the core details of the image. It is an image type that is often infringed upon, and even if copyright registration is carried out, the current copyright registration method cannot automatically prevent pirated images from being registered again.

Copyright authentication has always been a research hotspot in digital forensics [1]. Traditional image copyright protection methods mainly rely on digital watermarking and content-based image copy detection technology. The digital watermarking technology [2] embeds the watermark information in the image to be protected in advance, and subsequently extracts the watermark to verify the copyright of the image when necessary. The content-based image copy detection technology [3] extracts features that singularly identify the image as a whole or a part of the image. It verifies whether the image has been illegally copied by finding images with the same features, achieving copyright protection. Perceptual hashing [4] is a multimedia fingerprinting algorithm that considers various multimedia characteristics. In common cryptographic hashes such as SHA-1 and MD5, subtle changes in the original image will lead to considerably different resulting hashes, while the unique input insensitivity of perceptual hash algorithms enables them to recognize image similarity and avoid the avalanche effect.

The aforementioned image copyright protection techniques face a common challenge: the need for a trusted third party, which should act as a notary public to prove ownership of the image. Therefore, supervising third parties for avoiding data leak-age and illegal tampering by intermediaries has become an urgent problem to be solved. Blockchain [5] is a possible solution to this problem because of its core idea of decentralization. It has the characteristics of openness and transparency, which significantly reduces the possibility of image abuse and the difficulty of proof. At the same time, its smart contract module [6] supports trusted programming, which can meet the needs of trusted third parties in rights protection and arbitration. Although there

Received 21 October 2024; revised 11 December 2024; accepted 17 January 2025. Date of publication 10 July 2025; date of current version 24 September 2025. This work was supported in part by the Humanities and Social Science Foun-dation of Ministry of Education, China under Grant 24YJA870002, in part by the National Key Research and Development Plan of China under Grant 2022YFB3103100, and in part by the National Natural Science Foundation of China under Grant 62122032 and Grant U23B2023. The associate editor coordinating the review of this article and approving it for publication was Dr Jiande Sun. *(Corresponding author: Zhihua Xia.)*

Guangyong Gao, Tongchao Feng, and Chongtao Guo are with the Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science & Technology, Nanjing 210044, China, also with the Jiangsu Yuchi Blockchain Technology Research Institute, Nanjing 210044, China, and also with the School of Computer Science, Nanjing University of Information Science & Technology, Nanjing 210044, China (e-mail: gaoguangyong@163.com; ftc96969@163.com; sxcho-ngtao@163.com).

Zhihua Xia is with the College of Cyber Security, Engineering Research Center of Trustworthy AI, Ministry of Education, Jinan University, Guangzhou 510632, China (e-mail: xia_zhihua@163.com).

Yun-Qing Shi is with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102-1982 USA (e-mail: shi@njit.edu).

Digital Object Identifier 10.1109/TMM.2025.3586150

TABLE I
COMMON IMAGE COPYRIGHT PROTECTION MECHANISMS AND THEIR ADVANTAGES AND DISADVANTAGES

Mechanisms	Advantages	Disadvantages
traditional digital watermark	Embedding and extraction processes are relatively mature	Need for credible third-party arbitration
Content-based image retrieval	High degree of automation	High computational complexity
Perceptual Hashing	High computational efficiency and low storage requirements	Not applicable to all images

are a few blockchain-based digital rights management schemes [7], they focus only on content encryption and license management, and cannot detect the violation of original contents. On the other hand, there is no research scheme that is designed for the characteristics of the specific information carrier-image. Table I provides the common image copyright pro-tection mechanisms and their advantages and disadvantages.

A. Motivation

The fundamental motivation of our scheme is to confirm the attribution of images and provide copyright certification to the authors of original images. These are two main concerns of image creators that apply for copyright certification to copyright identification agencies. The goal of the scheme is to build a secure and rapid copyright infringement detection method, which can be paired with the advantages of a blockchain-based architecture, to ensure that others will not be able to easily steal the copyrights belonging to the authors. Currently, the high handling fee of copyright appraisal agencies is also a common concern of image creators. We also aim to avoid the handling fee required for manual processing and create a blockchain network architecture with lower transaction fees.

B. Our Contributions

1) We propose an improved perception hash (ipHash) algorithm for purely chromatic background images, which enhances the universality of perceptual hashing. At the same time, the common images and purely chromatic background images are classified so that they correspond to these two different hashing algorithms.
2) The blockchain's data storage limitation is mitigated by proposing a technical framework that combines the ipHash algorithm, the Ethereum blockchain, and the distributed file system InterPlanetary File System (IPFS). By introducing the blockchain technology, the traditional image hashing technology no longer needs a trusted third party to achieve decentralization.
3) Existing smart contracts related to image copyright protection lack security. To overcome this limitation, a secure smart contract is proposed that is suitable for the image copyright authentication process. It does not rely on the credit endorsement of a third party, and quickly and objectively performs copyright authentication. The use of smart contract technology considerably improves the efficiency of our scheme compared to traditional methods.

The rest of the paper is organized as follows. Section II includes preliminary and related work. Section III provides details about the implementation of research, followed by the performance analysis in Section IV. Section V presents conclusions and future research prospects.

II. PRELIMINARY AND RELATED WORK

A. Blockchain

Blockchain [8] involves integration and innovation based on multiple disciplines. It allows all nodes to jointly manage a secure and reliable distributed database by means of decentralization and machine-created trust [9]. Blockchain-based mobile edge computing key management scheme ensures secure group communication when mobile devices are dynamically moving from one subnet to another [10]. Fig. 1 shows the basic model structure of the blockchain. Compared with traditional technology, the blockchain technology has four major characteristics:

1) *Decentralization:* Blockchain uses distributed computer resources to store data, which eliminates the need for centralized management of traditional network, and considerably reduces running expenses and security risks.
2) *Immutable:* If the specific transaction information on a block needs to be modified, it requires modification of all the block information generated after the block. This is practically an impossible task, therefore, the blockchain constitutes an extremely stable system.
3) *Transparency:* All transactions generated on the blockchain network are managed openly and transparently. The time of all transactions can be tracked, and anyone on the chain can access these public transaction records.
4) *Privacy and anonymity:* The procedural rules in the blockchain can judge the validity of the activities by themselves when the data are exchanged. Therefore, the data storage and interaction on the chain can be carried out anonymously rather than based on addresses and personal identities.

B. InterPlanetary File System

InterPlanetary File System [11] is a distributed storage network based on the blockchain technology. All nodes in the network form a distributed file system. This system has the advantages of fast access, tamper-resistance, and lower data redundancy. The IPFS uses a Distributed Hash Table (DHT) to obtain file location and node connection data. A file uploaded to the IPFS system is divided into blocks of up to 256 kb in size, where each block is marked by a content identifier, thus forming a Merkle directed acyclic graph [12]. The root hash of the directed acyclic graph is used to represent the entire file data, and the file can be reconstructed as long as the blocks in the graph

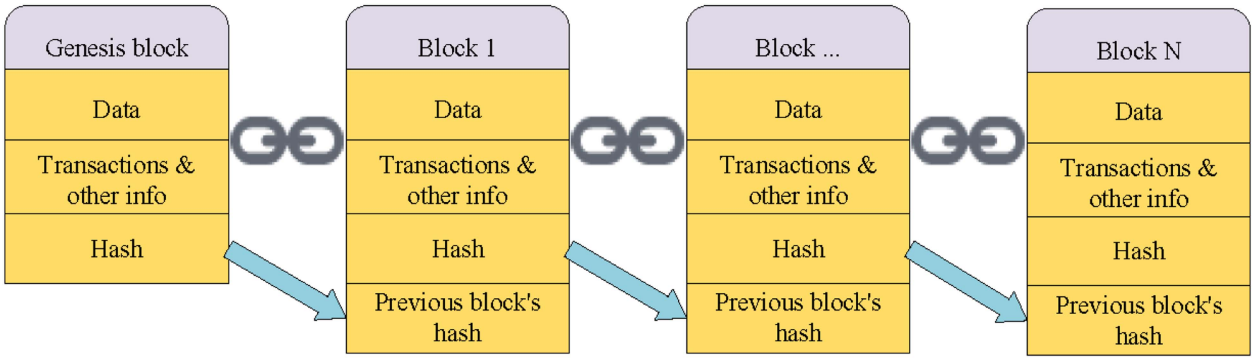

Fig. 1. The basic model structure of blockchain.

can be obtained. At the same time, retrieval of files from the IPFS simply requires the corresponding file hash. Consequently, the retrieval speed is faster compared to general file storage solutions [13]. In most scenarios that require the blockchain to have file storage capabilities, the combination of "IPFS + blockchain" can overcome the limitation of the blockchain where it is not able to store large files [14].

C. Perceptual Hashing

Common perceptual image hashes are Perception Hash (pHash), Average Hash (aHash) and Difference Hash (dHash). Each hash has its advantages and disadvantages under different image transformation operating conditions. As the copyright protection requires higher image copyright identification accuracy, we choose the pHash algorithm and improve it. The pHash is a perceptual hashing technology based on the discrete cosine transform (DCT) [15]. Huang et al. [16] proposed an efficient image hashing method for copy detection and used the locally dominant DCT coefficients from the first row/column of each sub-image to compute the vector distance. Li et al. [17] proposed a CLIP-based knowledge distillation hashing (CKDH) for cross-modal retrieval to address the shortcomings of existing cross-modal retrieval methods based on depth hashing. The calculation steps of pHash are as follows:

1) Reduce the input image to a size of $N \times N$, usually equal to 32 × 32 or 8 × 8 pixels. The purpose of this step is to simplify the subsequent DCT operations and reduce the differences caused by different image sizes and proportions. The value of N in this paper is chosen as 32 to minimize the quality impact of shrinking.
2) The input RGB image is uniformly converted into a grayscale image and represented in a matrix form f, where $f(i,j), i\epsilon[1,N], j\epsilon[1,N]$ is the matrix element value. In this way, the amount of color information in the RGB image is reduced to black-and-white grayscale values.
3) The DCT calculation is performed using (1) to convert the image from spatial domain to frequency domain. The resulting frequency matrix is represented by the square matrix A. The n × n low-frequency part of the upper left corner of A is retained and the rest is deleted, where n ≤ N. The final perceptual hash code is a binary sequence code that is 64 bits in size, therefore, n is set to 8 in this step.

$$\begin{aligned} &A(u,v) \\ &= c(u)\,c(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cos\left[\frac{(2i+1)u\pi}{2N}\right] \\ &\quad\times\cos\left[\frac{(2j+1)v\pi}{2N}\right] \\ &(u = 0,1,\ldots,N,-1;\ v = 0,1,\ldots,N-1), \end{aligned} \tag{1}$$

where

$$c(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{1}{N}}, & u \neq 0 \end{cases} \quad c(v) = \begin{cases} \sqrt{\frac{1}{N}}, & v = 0 \\ \sqrt{\frac{1}{N}}, & v \neq 0 \end{cases} \tag{2}$$

1) (3) is used to calculate the average value of the remaining part of A as follows:

$$\bar{m} = \frac{1}{64}\sum_{u=0}^{7}\sum_{v=0}^{7} A(u,v) \tag{3}$$

2) The values of A are compared with the average value in (3) respectively. If a value is less than the average value, the output is 0; otherwise it is 1. Therefore, the 64-bit sequence of the entire image is obtained after normalization, which represents the final hash value of the image. This step is shown in (4) below.

$$\begin{aligned} h = \{&\{0, A(u,v) < \bar{m}\}, \{1, A(u,v) \geq \bar{m}\}, \\ &\forall u, v \in [0,7]\} \end{aligned} \tag{4}$$

D. Image Copyright Protection

The blockchain technology has developed actively in recent years and is widely used in finance, military, supply chain, copyright and other fields [18]. Technical research on image copyright protection using the blockchain has also emerged, which utilized the blockchain characteristics such as data immutability and timestamp correlation.

White et al. [19] studied and confirmed the possibility of combining image hashing with blockchain. The authors submitted a tampered image to the blockchain and verified whether the original image would be generated as the output. This work provided a sound theoretical basis and experimental support for subsequent

related research. Kuang et al. [20] researched and implemented a new generation of image digital copyright system based on the blockchain technology and the scale-invariant feature transform (SIFT) feature extraction algorithm. In this system, the local features of an image under a geometrical attack could still be correctly extracted, which effectively prevented the copyright registration of the infringing image. Mehta et al. [21] used three indicators to analyze the performance quality of four perceptual hashing algorithms, i.e., pHash, dHash, wHash, aHash, on the BSDS-500 dataset. The results showed that the dHash was faster but had a lower robustness against rotation operations. Wang et al. [22] utilized the de-trusted third parties feature of the blockchain and the zero-watermark algorithm to solve the problem of trusted third-party dependence in digital watermark arbitration. The experimental results demonstrated that the time and contract costs were both acceptable compared to traditional copyright protection provided by the copyright authorities. Although all the above-mentioned methods used the blockchain technology, they neither involved the design of smart contracts related to the image copyright protection process, nor did they consider the system security.

Kumar et al. [23] proposed a distributed peer-to-peer image and video sharing platform based on the blockchain and the IPFS to solve the infringement problems of industrial image and video content. However, their work had a limited application domain because the distributed detection technology was only developed for industrial images and videos. Xia et al. [24] proposed a digital media copyright protection system using the Fabric blockchain and the IPFS. The authors applied three different perceptual hashing methods: pHash, dHash, and aHash to the copyright protection of digital media content. However, they neither provided a concrete validation of the model's implementation, nor did they give details of how these hashing techniques used similarity estimation to check the image copyright. Zauner et al. [25] proposed a new benchmarking framework called the Rihamark to benchmark four different perceptual hashing algorithms. The authors compared the computing speed, robustness, and ability to distinguish the similarity. However, they did not provide details of the copyright protection method, lacking a systematic and complete image copyright protection strategy. Wang et al. [26] proposed a real perceptual image hash method for content authentication that combined statistical analysis methods and visual perception theory. The proposed method had better comprehensive performance in content-based image tampering detection and localization. However, this solution was restricted to the picture authentication stage and did not perform an in-depth study on copyright traceability and protection. Tang et al. [27] proposed a two-stage robust reversible watermarking (RRW) scheme that improved the watermark robustness and capacity for copyright protection through embedding optimization and rounding error compensation. Yang et al. [28] proposed a method for reversible data hiding in encrypted images based on the time-varying Huffman coding table (TV-HCT) to achieve image copyright protection. Li et al. [29] proposed a blockchain-based security protocol that ensured the verification of the integrity of outsourced data based on a dynamic audit strategy. The above literature review shows that the existing methods share a common problem in image types: the research objects are confined to popular colored images. When these methods are applied to particular images like the aforementioned purely chromatic background images, their performance effectiveness is not up to par.

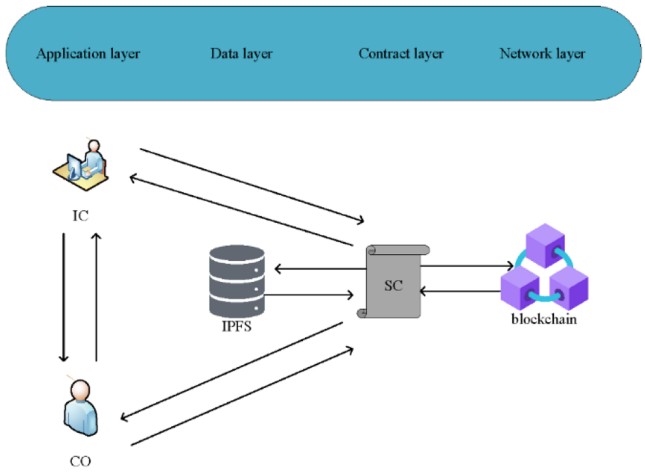

Fig. 2. Framework architecture diagram.

III. Implementation of The Proposed Scheme

In order to effectively protect image copyright data, a framework divided into four layers is proposed in this section. There are two main subjects in the framework, namely image copyright owners (CO) and image creators (IC), as shown in Fig. 2. A specific system is implemented based on this framework. At the same time, the application of the existing pHash algorithm in this system does not produce the expected results for the similarity detection of purely chromatic background images, which are different from the generally-used colored images. Therefore, we improve the traditional pHash algorithm and propose a scheme with preferable image universality.

A. Design of Iphash Algorithm

The pHash algorithm is different from the general encryption algorithms such as the MD5 and SHA-1. These algorithms are very sensitive to the changes in data, and slight changes will cause differences in the resulting hash. However, the pHash algorithm is less sensitive to the changes and consequently, it can correctly reflect the similarity between the changed data and the original data. Therefore, it is suitable for the similarity comparison of images. However, the pHash algorithm only retains the low-frequency part of the DCT matrix [30], which limits the diversity of images. Therefore, this paper proposes a more widely applicable image hashing scheme. The proposed ipHash algorithm can correctly detect the similarity of purely chromatic background images and exhibits enhanced robustness under specific attacks. The perceptual hashing techniques consist of two parts: the traditional pHash algorithm for common images and the ipHash algorithm for purely chromatic background images.

An analysis of the steps of the pHash algorithm provided in Section II shows that most of the image data are stored in the low-frequency domain. In order to reduce the computational burden, the pHash algorithm only retains the 8×8 part of the upper left corner of the DCT matrix in the third step. The remaining matrix is ignored and discarded. For most common images, this step has a good effect, because the similarity of two images can be judged effectively by their basic information reflected in the low frequency domain. On the contrary, in a purely chromatic background image, its central detail is the primary part and the key for copyright authentication. However, a large proportion of the background color acts as interference, which becomes the origin of the energy in the upper left corner of the matrix. Therefore, the impact of this step in the pHash algorithm is magnified, which is a limitation of the algorithm.

The image details appear as the high-frequency part in the DCT matrix. Therefore, for purely chromatic background images, our proposed scheme does not retain the low-frequency part of the DCT matrix obtained in the third step of the pHash algorithm. Instead, it uses the high-frequency part in the lower right corner of the pixel matrix of the image for subsequent calculation of the image hash, which is also known as the image fingerprint. The steps of the ipHash algorithm for similarity detection of purely chromatic background images are similar to those of perceptual image hashing in Section II. The first two steps are the same. In the third step, the difference is that after obtaining the square matrix, the 8×8 high frequency part in the lower right corner of the matrix is kept and the rest is discarded. Therefore, the average is calculated differently according to (5), which is different from the calculation of the average shown in Section II. Finally, after normalization, the 64-bit binary sequence of the entire image is obtained, which represents the final hash value of the image. The new normalization formula is shown in (6).

$$\bar{m} = \frac{1}{64} \sum_{u=24}^{31} \sum_{v=24}^{31} A(u,v) \tag{5}$$

$$h = \{\{0, A(u,v) < \bar{m}\}, \{1, A(u,v) \geq \bar{m}\}, \forall u, v \in [24, 31]\} \tag{6}$$

B. Image Similarity Detection

The traditional centralized approach needs a higher storage space to meet the requirements of copyright infringement detection in peer-to-peer distributed file storage systems. The proposed IPFS-based blockchain system aims to provide on-chain and off-chain storages for copyright summaries and the original image content, respectively. In addition, the system also validates transactions based on the pHash value, which is used to detect whether the same object exists in the blockchain network. The flowchart shown in Fig. 3 describes the general process of the method, and the corresponding steps are explained below.

1) The user uploads an image to the system. In this step, the user is the creator who wants to verify the copyright of the original image. However, the user may also be a copyright infringer, who uses another copyrighted image and modifies it by scaling, rotating, blurring, sharpening, etc., and subsequently tries to apply for copyright again for the modified image.
2) Next, the system will first call the corresponding function to preliminarily divide the uploaded image. The goal is to determine whether the image is a purely chromatic background image or a common image. Subsequently, it uses different pHash algorithms for these two different types of images to calculate the pHash values.
3) In this step, the calculated pHash is matched with the pHash values of the images in the blockchain network.
4) If the similarity between two images is greater than the preset threshold, it indicates an infringement. Therefore, the image will be discarded, and the blockchain network will not be updated.
5) Otherwise, if the similarity is less than the threshold, the uploaded image will be added to the IPFS, and its pHash value will be added to the blockchain network. The blockchain network will make the corresponding updates.

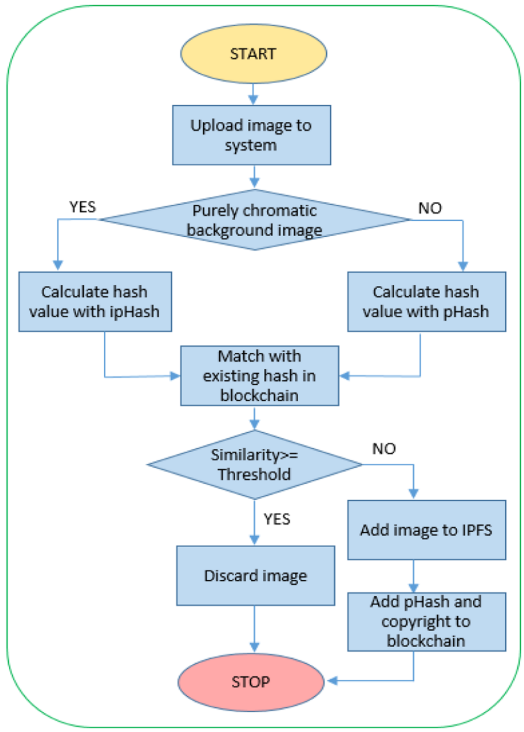

Fig. 3. Image copyright infringement detection process.

In Algorithm 1, first the proposed lightweight purely chromatic background image (PCBI) algorithm will classify the uploaded images, and then call different pHash algorithms to generate pHash values of the images and store them in the blockchain network. Furthermore, the images are stored in the IPFS distributed file storage system at the given URL ('127.0.0.1', 5001). The IPFS returns the addresses of the images and stores them in the blockchain.

Algorithm 2 calculates the similarity between the pHash values of two images. First, it obtains the length of the pHash value, and then uses the Hamming distance [31] to calculate the similarity percentage. The Hamming distance represents the number of bits with different values. Therefore, it can be noted from the

algorithm that the pHash values of the two images are matched bit-by-bit until the last bit of the pHash value is reached. Subsequently, the image similarity is calculated, which is represented by the variable *sim* in Algorithm 2.

Algorithm 1: Generating pHash and IPFS Hash of an Image

Input: testImage.bmp: a test image
Output: *imagePhash*: image hash of test image
From PIL import Image //PIL: Python Imaging Library
import ImageHash
imagePhash ← 0;
//Storing image address into the *fadd*
fadd ← request.file (testImage.bmp);
//Storing pHash of an image. PCBI is a function used to determine whether an image belongs to a purely chromatic background image.
if (PCBI(*fadd*) = = True) **then**
imagePhash ← str(iphash(image.open(*fadd*)));
else
imagePhash ← str(phash(image.open(*fadd*)));
end
//Connecting to the IPFS storage
api ← ipfsapi.connect ("127.0.0.1",5001);
res ← api.add (*fadd*); //Adding the file into the IPFS storage;
//Storing the IPFS address of the image into blockchain
blockchain ← *res*;
Return *imagePhash*;

C. Smart Contract Design

Smart contracts are a radical innovation in the blockchain, which can be described as an automatically executable program deployed on the blockchain. Smart contracts obtain data from outside the system. When the conditions set by the program are satisfied, the system will automatically execute the corresponding contracts and realize the data processing functions [32]. The smart contract module of this system mainly includes three functions: register(), verify() and reward()-and-punish(). In this section, we explain the smart contracts SCs used in this paper and their logic. All SCs are written in Solidity, which is a Turing-complete language for Ethereum [33]. Table II provides the symbols used in the remainder of this paper.

1) Registration Contract: This contract is mainly used for image registration and is known as the image registration contract. It is created by the blockchain and initialized with the system. The contract mainly involves two subjects: 1) validator: This is an authorization node used to verify transactions on the blockchain, where any authorized node can become a validator. 2) user: This is the user node accessing the blockchain, where any operation by the user node will be regarded as a blockchain transaction. In fact, all contracts contain these two transaction entities. In this contract, the user must pay a deposit $\mathcal{p}$ for the transaction data prior to initiating a transaction, where the deposit is generally twice the token amount $\mathcal{T}$ spent by the transaction. The contract algorithm is shown in Algorithm 3.

Algorithm 2: Matching Hashes for Checking Similarity of Images Using Hamming Distance

Input:
*hash*1: image hash of test image
*hash*2: image hash of copyrighted image
Output: *sim*: similarity in Percentage
*hash*1 ← ImageHashOne;
*hash*2 ← ImageHashTwo;
lengthOfHash ← length(hash1);
sim←0, *dissim*←0;
i←1;
while ($i \leq lengthOfHash$) **do**
if ($hash1[i] \neq hash2[i]$) **then**
dissim←*dissim*+1;
else
continue;
end
end
sim←(1 – *dissim* / *lengthOfHash*) × 100%;
return *sim*;

TABLE II
LIST OF SYMBOLS AND THEIR ASSOCIATED MEANINGS

Notations	Description
$\mathcal{T}$	Tokens required for the transaction
$\mathcal{p}$	User's pledged margin
$\mathcal{d}$	The data of the image to be checked
ADDR	User's Ethereum account address
$\mathcal{R}$	Validator's validation report
$\mathcal{ts}$	Transaction result
$\mathcal{V}$	The pHash value of the image
$\mathcal{V}^{''}$	The pHash value of the registered image
$\mathcal{B}$	Image copyright verification result
$\mathcal{P}$	Transaction processing result
$\mathcal{M}$	Transaction details related to the image

2) Verification Contract: This contract is used to verify the copyright of images. Users will utilize the relevant functions of this contract when applying for copyright registration or inquiring about the copyright. Notably, access to this contract is limited to validators, because the return value of the function in the smart contract can only be obtained through the log event. However, as Ethereum is a public blockchain and everyone can access it through event monitoring, there is a privacy leakage problem. Therefore, we solve this problem by invoking this contract using the registration contract on the validator node. The contract algorithm is shown in Algorithm 4.

3) Reward and Punishment Contract: This contract is especially designed to encourage miners to participate in verification and avoid dishonest behavior by malicious nodes. It implements a reward and punishment mechanism for the behavior of all nodes in the blockchain. Specifically, nodes working normally and maintaining the stability of the blockchain are rewarded for their positive behavior by the contract. Otherwise, negative behavior such as uploading infringing images illegally in an

Algorithm 3: Design of Registration Module

Input: β, $\mathcal{T}$, d', ADDR, R
Output: ts

User sends β to SC;
if Validator sends $\mathcal{T}$ to SC **then**
  Validator check validity of User;
  if Validator add ADDR to set of authorized users **then**
    if SC confirms $\mathcal{T} ==$ True and $\beta ==$ True **then**
      User sends d' to validator;
      Validator calls SC to check d';
      if d' is correct **then**
        User ends the transaction;
        SC sends β to User and $\mathcal{T}$ to validator;
        $ts =$ True;
      else
        Validator ends the transaction and sends R to SC;
        $ts =$ false;
      end
    else
      User terminates the transaction;
      SC sends $\mathcal{T}$ to validator and β to user;
    end
  else
    Validator terminates the transaction;
    SC sends $\mathcal{T}$ to validator and β to user;
  end
else
  User ends the transaction;
  SC sends β to user;
end
return ts

Algorithm 4: Design of Verification Module

Input: d', ADDR, V
Output: $\mathcal{B}$

User uploads d' to validator;
Validator reads d' and calls SC;
if d' is purely chromatic background image **then**
  SC calculates V by invoking ipHash algorithm and sends V to validator;
  Validator compares V with V'';
else
  SC calculates V by invoking pHash and sends to validator;
  Validator compares V with V'';
end
if $V == V''$ **then**
  Validator rejects d' and ends the transaction;
  $\mathcal{B} =$ false;
  Validator sends $\mathcal{B}$ to user and R to SC;
else
  Validator uploads d' to IPFS and sends M to blockchain;
    $\mathcal{B} =$ True;
    Validator sends $\mathcal{B}$ to user;
    user ends the transaction;
end
return $\mathcal{B}$

attempt to obtain a copyright, or colluding with dishonest nodes to destroy the blockchain is penalized.

In addition, nodes can receive a regular fee for participating in the verification process, which is achieved by the automatic execution of the distribution by the smart contract. For example, if the input d' uploaded by the user is indeed an original work, the nodes verifying it can get 3% of the $\mathcal{T}$ as a reward for their work. This reward can serve as an incentive for nodes to participate in blockchain maintenance. In short, it is unlikely for the malicious behavior to occur because dishonest behavior in our proposed system scheme will result in deduction of tokens of the node. The contract algorithm is shown in Algorithm 5.

The above-mentioned three modules together constitute a complete image copyright registration and verification system. It ensures that the images uploaded by users are strictly verified throughout the process, and the fairness and integrity of the system are maintained through the reward and punishment mechanism. First, the registration module is responsible for verifying the eligibility of the user, ensuring that the user is qualified for registration, and processing the user's deposit and tokens. Second, the verification module ensures the data uniqueness and legitimacy by processing the image data, calculating the hash value and comparing it with the registered image. Last, the rewards and punishments module ensures that the validator com-plies with the rules and handles any misbehavior during the validation process.

IV. Experimental Comparative Analysis

In this section, experiments are conducted on the ipHash algorithm and smart contracts in the system, where the blockchain part is verified on the local test network. A case is implemented to analyze the cost and performance of the system. The operating environment is: GHz CPU, 16 GB RAM. We achieve the interaction between the test chain and smart contracts using Truffle v4.1.17, Ganache v2.5.4(TestRPC) and Metamask v4.5.1.

A. Performance

This subsection demonstrates the effectiveness and robustness of the proposed ipHash algorithm and compares it with the general perceptual hashing algorithms and zero-watermarking algorithms proposed in other related studies. As official datasets of purely chromatic background images are not available, we collect a total of 200 such images of size 256 × 256 [34]. Due to limited space, we only show eight of them in Fig. 4: House, Apple, Cat, Elephant, Christmas, Cook, Coffee and Hat. These images have different background colors and core contents, and thus, they are the representative experimental objects for showing the performance and universality of the proposed method. The difference between the final hash values of the original image and the test image is quantified by using the Hamming Distance as the objective metric, as shown in (7). The expression given in (7) calculates the number of different bits in the corresponding position between two hash strings, and the similarity

Fig. 4. Eight images used for experiments of comparing NC values: (a) House, (b) Apple, (c) Cat, (d) Elephant, (e) Christmas, (f) cook, (g) Coffee, (h) Hat.

Algorithm 5: Design of Reward-and-Punishment Module

Input: d, R
Output: $\mathcal{P}$
User sends d to validator;
Validator calls SC to check d;
if validator sends R to SC **then**
  if SC receives R **then**
    Another miner verifies R;
    if d has existed **then**
      $\mathcal{P}$ = True;
    else
      $\mathcal{P}$ = False;
    end
  else
    User or validator ends the transaction;
    SC sends $\mathcal{T}$ to validator and β to user;
  end
else
  User or validator ends the transaction;
  SC sends $\mathcal{T}$ to validator and β to user;
SC judges the result of R;
end
if $\mathcal{P}$ == True **then**
  Validator ends the transaction;
  SC sends $\mathcal{T}$ and β to validator;
else
  User ends the transaction;
  SC sends $\mathcal{T}$ and β to user;
end
return $\mathcal{P}$

S can be defined as shown in (8):

$$H_d = \sum_{k=0}^{63} \left(h_k^1 \oplus h_k^2\right) \tag{7}$$

$$\mathrm{S} = 1 - \frac{H_d}{HBC} \tag{8}$$

where HBC stands for the length of the hash value, which is equal to 64 in this article. At the same time, to effectively compare the experimental results with those of other studies and demonstrate the robustness of the algorithm, an objective metric called the normalized correlation (NC) value is also introduced to measure the similarity between two image hashes. Let x_i and y_i be two image hash values, then the normalized correlation value is defined according to (9) as

$$f = \frac{\sum_{i=1}^{L}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)}{\sqrt{\sum_{i=1}^{L}\left(x_i - \bar{x}\right)^2}\sqrt{\sum_{i=1}^{L}\left(y_i - \bar{y}\right)^2}} \tag{9}$$

where $\bar{x}$ and $\bar{y}$ are the mean of x_i and y_i, respectively, and L is the length of the image hash. The value of f represents the NC value, expressed as a decimal number ranging between 0 and 1, where its larger value indicates a higher similarity between the input images. If f is greater than the predefined threshold, the images are treated as visually identical images; otherwise, they are considered as different images.

In the experiment, we conduct attack tests on our dataset containing these 200 images, including noise, filtering, JPEG compression, rotation, scaling, translation, etc. The test results of the images depicted in Fig. 4 obtained using the ipHash and pHash algorithms are shown in Tables III and IV, respectively. The results indicate that the eight purely chromatic background images are highly robust against geometric and common attacks. In addition, the overall average of the experimental results for all 200 images in the dataset obtained using the ipHash algorithm is greater than 0.9. However, the NC values obtined using the pHash algorithm are all less than 0.5, as shown in Table V. This further confirms that the pHash algorithm, which retains the low-frequency portion of the DCT, is not suitable for copyright protection of purely chromatic background images.

The proposed scheme is also compared with three other similar studies to demonstrate its effectiveness and advantages for similarity detection on purely chromatic background images. Specially, the research of Mehta et al. [21] used the wHash algorithm, Wang et al. [22] adopted the zero-watermark algorithm and Kumar et al. [23] used the traditional pHash algorithm. All 200 images are divided into 100 groups, and images in each

TABLE III
NC VALUES OF IPHASH ALGORITHM UNDER DIFFERENT ATTACKS

Attack	House	Apple	Cat	Elephant	Cook	Christmas	Coffee	Hat
Gaussian noise(0.02)	0.9414	0.9513	0.9180	0.7930	0.9609	0.9883	0.9375	0.9414
Salt and pepper noise(0.02)	0.9766	0.9327	0.8516	0.8698	0.9570	0.9688	0.9531	0.8698
Wiener filter(4x4)	0.9961	0.9689	0.9961	0.8633	1.0000	0.9922	0.9414	0.9689
Median filter(4x4)	0.9727	0.9518	0.9805	0.8555	0.9961	0.9883	0.9375	0.9727
JPEG compression(Q=10)	0.9961	0.9714	0.9805	0.8555	0.9922	0.9805	0.9961	0.9714
Rotation(30°)	0.9961	0.9857	0.9883	0.9844	1.0000	0.9883	1.0000	0.9609
Scale(0.9)	0.9922	0.9783	0.9805	0.9727	0.9961	0.9883	0.9414	0.9805
Shift(30 pixels)	0.9961	0.9805	0.9844	0.957	0.9961	0.9961	1.0000	0.9518

TABLE IV
NC VALUES OF PHASH ALGORITHM UNDER DIFFERENT ATTACKS

Attack	House	Apple	Cat	Elephant	Cook	Christmas	Coffee	Hat
Gaussian noise(0.02)	0.3458	0.2430	0.3182	0.3098	0.4718	0.3362	0.2229	0.4218
Salt and pepper noise(0.02)	0.3329	0.3388	0.3173	0.3639	0.3522	0.4652	0.3775	0.4414
Wiener filter(4x4)	0.3673	0.3194	0.3423	0.3253	0.3862	0.4204	0.3987	0.4566
Median filter(4x4)	0.4210	0.4120	0.2478	0.3391	0.3935	0.4427	0.4025	0.3482
JPEG compression(Q=10)	0.2510	0.3182	0.3365	0.3672	0.3323	0.3162	0.2271	0.4771
Rotation(30°)	0.2779	0.2369	0.4293	0.4192	0.3289	0.4346	0.2516	0.4697
Scale(0.9)	0.3529	0.4120	0.3753	0.2587	0.4718	0.3652	0.2229	0.3346
Shift(30 pixels)	0.4361	0.3922	0.3173	0.2587	0.2928	0.3294	0.1710	0.3812

TABLE V
AVERAGE NC VALUES OF IPHASH AND PHASH ALGORITHM UNDER DIFFERENT ATTACKS

Attack	Gaussian noise (0.02)	Salt and pepper noise (0.02)	Wiener filter (4x4)	Median filter (4x4)	JPEG compression (Q=10)	Rotation (30°)	Scale (0.9)	Shift (30 pixels)
ipHash Average	0.9291	0.9223	0.9689	0.9543	0.9631	0.9812	0.9734	0.9825
pHash Average	0.3252	0.3380	0.3186	0.4913	0.3410	0.3396	0.2974	0.3261

TABLE VI
AVERAGE SIMILARITY OF 100 GROUPS OF PURELY CHROMATIC BACKGROUND IMAGES UNDER DIFFERENT SCHEMES

Scheme	wHash [21]	Zero-watermark [22]	pHash [23]	ipHash
Average	0.58	0.91	0.57	0.37

group have identical background colors, as shown by the examples in Fig. 5.

Fig. 6 compares the similarity detection results of the algorithm proposed in this paper and other algorithms on purely chromatic background images. Referring to the experimental results of the pHash algorithm threshold in Mehta et al. [21], the similarity threshold is preset to 0.4. Fig. 6 shows that when the algorithm proposed in this paper detects different purely chromatic background images with the same background color, the obtained similarity value is below the threshold. In addition, the average values of similarity of all 100 groups under different schemes are shown in Table VI. The average similarity of all remaining images is also less than 0.4, reaching a value of 0.37. As expected, the images are recognized as two original images. On the contrary, the similarity values obtained with other algorithms [21], [22] and [23] are generally higher than 0.5 and are equal to 0.58, 0.91 and 0.57, respectively. These values signify that the algorithms in [21], [22] and [23] mistakenly regard a purely chromatic background image as an infringing version of another image, which is inconsistent with reality. This occurs because the algorithms in [21] and [22] used the DWT transform, and that in [23] used the traditional DCT transform. The ultimate goal of these algorithms was to obtain the low-frequency coefficients where most of the energy was concentrated. However, this methodology does not work for purely chromatic background images. Therefore, as mentioned in Section III, our proposed ipHash algorithm modifies the original pHash algorithm. Specifically, the proposed scheme adds a novel operation after the DCT transformation such that the key information of the purely chromatic background image represented by the high frequency part of the DCT matrix is better preserved. This modification provides an advantage where the error factor caused by the same background is ignored as much as possible, and the focus is instead retained on the target object of the image. In general, the

Fig. 5. Four groups of purely chromatic background images with the same background color.

TABLE VII
SIMILARITIES GENERATED BY PHASH AFTER DIFFERENT IMAGE ATTACKS

Attack	Pepper	Jetplane	Goldhill	Barbara	Boats	Baboon	Average
Gaussian noise(0.02)	1	1	0.969	1	0.891	1	0.992
Salt and pepper noise(0.02)	1	0.969	1	1	0.969	1	0.992
Wiener filter(4x4)	1	1	1	1	0.984	1	1.000
Median filter(4x4)	1	0.984	1	1	0.984	1	0.997
Jpeg compression(Q = 10)	1	0.969	1	1	0.953	1	0.990
Rotate(30°)	0.594	0.453	0.609	0.5	0.411	0.481	0.508
Scale(0.9)	1	1	1	1	1	0.5	0.914
Translate(30 pixels)	0.453	0.609	0.469	0.578	0.578	0.625	0.560

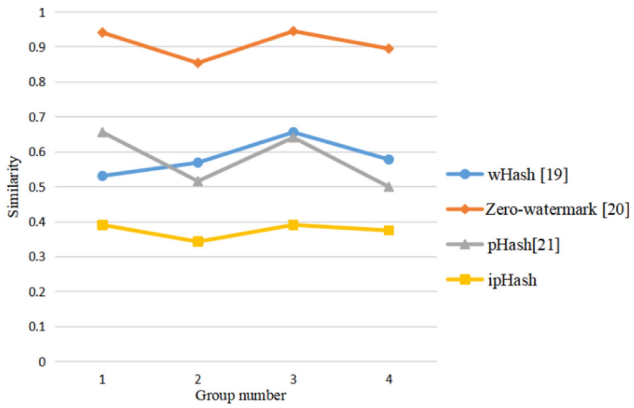

Fig. 6. Similarity comparison between ipHash and other algorithms for four groups of purely chromatic background images.

TABLE VIII
THE COST OF SMART CONTRACTS ON TEST NETWORK (GASPRICE = 20 GWEI, ETHER = 1242.08 USD AT PRESENT)

Image	Gas cost	Ether cost	USD cost
House	203738	0.00407476	5.0612
Apple	183355	0.00366710	4.5548
Cat	183691	0.00367382	4.5632
Elephant	198547	0.00397094	4.9322
Cook	229562	0.00459124	5.7027
Christmas	204974	0.00409948	5.0919
Coffee	215437	0.00430874	5.3518
Hat	189516	0.00379032	4.7079

proposed ipHash algorithm has a higher accuracy than other image protection algorithms in copyright authentication of purely chromatic background images.

In order to verify whether the ipHash algorithm performs as expected on the copyright authentication of common images, an experiment is carried out where the same image attacks as in Table III are performed on six images: Pepper, Jetplane, Goldhill, Barbara, Boats, and Baboon, as shown in Fig. 7. The pHash and ipHash algorithms are used to check their similarities, and the similarity results are shown in Table VII. It can be observed that our proposed scheme can also achieve copyright protection for general images.

Table VIII shows the contract cost tested in Ganache. In Ethereum, operations such as creating contracts, accessing accounts, and storing data need to consume gas. The introduction of gas prevents any abuse of blockchain network resources and provides a mechanical security guarantee for the operation of the chain. Once the gas required for an operation exceeds the pricing limit, the entire transaction is rolled back. It can be observed that the contract execution cost is related to the gas price, which affects the execution cost of contracts deployed in Ethereum over a long time. However, the way Ethereum works is that a

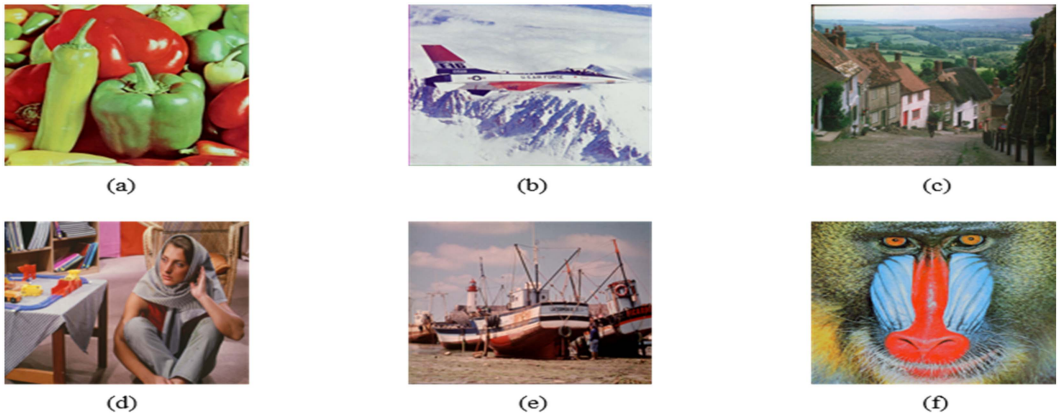

Fig. 7. Six images for the experiment: (a) Pepper, (b) Jetplane, (c) Goldhill, (d) Barbara, (e) Boats, (f) Baboon.

transaction will be prioritized and processed faster if one is willing to pay higher transaction fees. Thus, users can choose between time and money according to their needs. In our experiments, a medium gas price is chosen. Table VIII shows that the copyright authentication cost is still acceptable even with a medium gas price, and the average cost of registering the copyright of all 200 images is less than $6, which is considerably lower than the copyright fee charged by third-party agencies in reality. The experimental results show that the image copyright protection scheme based on blockchain has the advantages of low cost and high reliability.

B. Security Analysis

The image copyright protection framework based on blockchain, IPFS, and SC technologies has the following three advantages compared with the traditional watermarking methods: less risk, lower cost and higher efficiency of business processes. In reality, both users and miners might be malicious, which means that they can deceive each other to gain illegal benefits. The dissemination of the transaction records throughout the whole blockchain network is more worrying, which makes all the transactions visible to everyone in the networks. However, most current smart contracts [35], [36], [37] and blockchain platforms lack security mechanisms. Therefore, it is crucial to ensure that the smart contract is free of any vulnerabilities and the model is secure against attacks. Considering the potential security concerns of smart contracts in the copyright protection field, we add a unique reward and punishment function to the smart contracts in our scheme to regulate the behavior of nodes. In this part, we analyze the security of the proposed scheme by presenting several possible attack types.

As aforementioned, security is evaluated in the proposed scheme based on three categories. (I). A malicious user may send illegal images to deceive some miners. (II). A corrupt miner may intentionally reject the users' legitimate transactions. (III). A malicious user and a corrupt miner may collude to cheat the system. These adversaries can discard transactions, create false transactions or forge the fake node. We focus on how the system defends against possible attacks rather than how these attackers launch these different attacks.

Case (I) Malicious users. Malicious users may send an image transaction TX containing a pirated image, and the miners verify its legitimacy by calculating the perceptual hash $H_{I'}$ of the image I'. Subsequently, the miners access the original image I from the database and check the validity of $H_{I'}$ with the perceptual hash H_I of the image I. If $H_{I'} = H_I$, miners will not accept the transaction, and subsequently, the malicious users cannot submit illegal image transactions into the system.

Case (II) Corrupt miners. Corrupt miners may reject a user's legitimate transactions on purpose. A new reward and punishment mechanism is designed to alleviate the impact of such attacks. Especially, an authorized user who wants to access services in the system needs to deposit a fee in advance, which depends on the transaction value and is set by platform owners. This fee can serve as a maintenance fee for blockchain as well as a penalty fee in case of infringement. If it is found during the verification process that an entity tries to infringe the copyright and the miner does not properly respond to the illegal behavior, the validator will send a report to the smart contract for processing. The validator will get the corresponding reward when they discover any malicious behavior. Meanwhile, the corrupt miners may be subject to penalties such as forfeiture of some or all of their deposit fees.

Case (III) Collusion attack. The malicious users may collude with corrupt miners to add illegal image transactions to the system, which will be included in the blockchain. Upon receiving the illegal transactions, the corrupt miners directly pack them into the block without verifying them. When the block containing these transactions is propagated in the blockchain network, some honest miners receive and validate the new block, and can easily discover the illegal transaction inside. In this case, malicious users fail in their attempt to add illegal images, and corrupt miners are punished accordingly. In conclusion, our system can resist these three kinds of attacks and realize image copyright protection.

V. Conclusion

Images are a popular carrier of information and currently use digital watermarking technology to protect their copyrights. It is difficult to obtain absolute credibility from third parties due

to human factors, and the blockchain technology offers a viable solution to mitigate this issue. This paper proposed the use of blockchain to solve the problem of trusted third parties in image copyright protection, and mitigate the inherent weakness in copyright authentication of the traditional pHash algorithm for purely chromatic background images. The current state of copyright protection for images was studied, and a better image hash scheme, distributed storage system IPFS, and Ethereum blockchain were proposed as a framework. In the system implemented under this framework, smart contracts replaced trusted third parties in the real world to execute transactions and guarantee results, with greater reliability and lower operating costs. At the same time, we proposed the ipHash algorithm and conducted experimental comparisons to validate the rationality and superiority of this scheme. In future work, we intend to integrate a node evaluation protocol into the blockchain framework. Its aim is to perfect the consensus mechanism, while simultaneously striving to diminish the transaction expenses and bolster the network's efficiency and security.

REFERENCES

[1] X.-L. Liu, C.-C. Lin, and S.-M. Yuan, "Blind dual watermarking for color images' Authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, May 2018.

[2] S. Kamalraj Mohanarathinam, G. K. D. Prasanna Venkatesan, R. V. Ravi, and C. S. Manikandababu, "Digital watermarking techniques for image security: A review," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 8, pp. 3221–3229, Aug. 2020.

[3] A. J. C. Trappey, "An intelligent content-based image retrieval methodology using transfer learning for digital IP protection," *Adv. Eng. Inform.*, vol. 48, Apr. 2021, Art. no. 101291.

[4] Z. Huang and S. Liu, "Perceptual image hashing with texture and invariant vector distance for copy detection," *IEEE Trans. Multimedia*, vol. 23, pp. 1516–1529, Jun. 2021.

[5] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integration*, vol. 15, pp. 80–90, Sep. 2019.

[6] Z. Zheng, S Xie, and Hong-Ning Dai, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[7] J. Gao, H. Yu, X. Zhu, and X. Li, "Blockchain-based digital rights Management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption," *IEEE Syst. J.*, vol. 15, no. 4, pp. 5233–5244, Dec. 2021.

[8] K. T. Seow, "Supervisory control of blockchain networks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 50, no. 1, pp. 159–171, Jan. 2020.

[9] P. Zhang and M. Zhou, "Security and trust in blockchains: Architecture, key technologies, and open issues," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 3, pp. 790–801, Jun. 2020.

[10] J. Li, J. Wu, L. Chen, J. Li, and S.-K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 1, pp. 100–114, Jan. 2023.

[11] E. Politou, E. Alepis, C. Patsakis, F. Casino, and M. Alazab, "Delegated content erasure in IPFS," *Future Gener. Comput. Syst.*, vol. 112, pp. 956–964, Nov. 2020.

[12] P. Kang, W. Yang, and J. Zheng, "Blockchain private file storage-sharing method based on IPFS," *Sensors*, vol. 22, no. 14, Jul. 2022, Art. no. 5100.

[13] L. Rao, H. Zhang, and T. Tu, "Dynamic outsourced auditing services for cloud storage based on batch-leaves-authenticated merkle hash tree," *IEEE Trans. Serv. Comput.*, vol. 13, no. 3, pp. 451–463, May/Jun. 2020.

[14] L. Chen, X. Zhang, and Z. Sun, "Scalable blockchain storage model based on DHT and IPFS," *KSII Trans. Internet Inf. Syst.*, vol. 16, no. 7, pp. 2286–2304, Jul. 2022.

[15] Z. Tang, F. Yang, L.-Y. Huang, and X.-Q. Zhang, "Robust image hashing with dominant DCT coefficients," *Optik*, vol. 125, no. 18, pp. 5102–5107, Sep. 2014.

[16] Z. Huang and S. Liu, "Perceptual image hashing with texture and invariant vector distance for copy detection," *IEEE Trans. Multimedia*, vol. 23, pp. 1516–1529, 2021.

[17] J. Li et al., "CKDH: CLIP-based knowledge distillation hashing for cross-modal retrieval," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 7, pp. 6530–6541, Jul. 2024.

[18] G. Cheng, Y. Chen, S. Deng, H. Gao, and J. Yin, "A blockchain-based Mutual authentication scheme for collaborative edge computing," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 1, pp. 146–158, Feb. 2022.

[19] C. C. White, M. Paul, and S. Chakraborty, "A practical blockchain framework using image hashing for image authentication," Apr. 2020, *arXiv:2004.06860*.

[20] J. Shi, D. Yi, and J. Kuang, "A blockchain and SIFT based system for image copyright protection," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 1–6.

[21] R. Mehta, N. Kapoor, S. Sourav, and R. Shorey, "Decentralised image sharing and copyright protection using blockchain and perceptual hashes," in *Proc. 11th Int. Conf. Commun. Syst. Netw.*, May 2019, pp. 1–6.

[22] B. Wang, J.-W. Shi, W.-S. Wang, and P. Zhao, "Image copyright protection based on blockchain and Zero-watermark," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2188–2199, Jul./Aug. 2022.

[23] R. Kumar et al., "A secured distributed detection system based on IPFS and blockchain for industrial image and video data security," *J. Parallel Distrib. Comput.*, vol. 152, pp. 128–143, Jun. 2021.

[24] K. O.-B. O. Agyekum et al., "Digital Media copyright and content protection using IPFS and blockchain," in *Proc. 10th Int. Conf. Imag. Graph., Lecture Notes Comput. Sci.*, Nov. 2019, vol. 11903, pp. 266–277.

[25] C. Zauner, M. Steinebach, and E. Hermann, "Rihamark: Perceptual image hash benchmarking," *Proc. SPIE*, vol. 7880, pp. 1–14, Feb. 2011.

[26] X. Wang et al., "A visual model-based perceptual image hash for content authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 7, pp. 1336–1349, Jul. 2015.

[27] Y. Tang, S. Wang, C. Wang, S. Xiang, and Y.-M. Cheung, "A highly robust reversible watermarking scheme using embedding optimization and rounded error compensation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 4, pp. 1593–1609, Apr. 2023.

[28] Y. Yang, H. He, F. Chen, Y. Yuan, and N. Mao, "Reversible data hiding in encrypted images based on time-varying huffman coding table," *IEEE Trans. Multimedia*, vol. 25, pp. 8607–8619, 2023.

[29] J. Li, J. Wu, L. Jiang, and J. Li, "Blockchain-based public auditing with deep reinforcement learning for cloud storage," *Expert Syst. Appl.*, vol. 242, May 2024, Art. no. 122764.

[30] X.-R. Li, C. Qin, Z.-C. Wang, Z.-X. Qian, and X.-P. Zhang, "Unified performance evaluation method for perceptual image hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1404–1419, Mar. 2022.

[31] M. Norouzi, D. J. Fleet, and R. R. Salakhutdinov, "Hamming distance metric learning," in *Proc. Adv. Neur. Inf. Process. Syst.*, Feb. 2012, vol. 25, pp. 1061–1069.

[32] W. Xiong and L. Xiong, "Data trading certification based on consortium blockchain and smart contracts," *IEEE Access*, vol. 9, pp. 3482–3496, Feb. 2021.

[33] A. D. Sorbo, S. Laudanna, A. Vacca, C. A. Visaggio, and G. Canfora, "Profiling gas consumption in solidity smart contracts," *J. Syst. Softw.*, vol. 186, Apr. 2022, Art. no. 111193.

[34] C.-T. Guo, "A data set for purely chromatic background images," 2022. [Online]. Available: https://github.com/Gct96/images

[35] N. Jing, Q. Liu, and V. Sugumaran, "A blockchain-based code copyright management system," *Inf. Process. Manag.*, vol. 58, no. 3, May 2021, Art. no. 102518.

[36] Z.-F. Ma, M. Jiang, H.-M. Gao, and Z. Wang, "Blockchain for digital rights management," *Future Gener. Comput. Syst.*, vol. 89, pp. 746–764, Dec. 2018.

[37] I. Natgunanathan, P. Praitheeshan, L. Gao, Y. Xiang, and L. Pan, "Blockchain-based audio watermarking technique for multimedia copyright protection in distribution networks," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 18, no. 3, pp. 1–23, Aug. 2022.

Guangyong Gao received the Ph.D. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012. He is currently a Professor with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing. His research interests include reversible data hiding, computer networks security, multimedia information security, and digital image processing.

Tongchao Feng received the B.E. degree in information secutity from Shandong Agriculture and Engineering University, Jinan, China, in 2023. He is currently working toward the M.E. degree in network and information security with the College of Computer Science, Nanjing University of Information Science & Technology, Nanjing, China. His research interests include image copyright protection based on blockchain and Robust watermarking based on deep learning.

Chongtao Guo received the B.E. degree in computer science and technology from the Yancheng Institute of Technology, Yancheng, China. He is currently working toward the M.E. degree in electronic information with the College of Computer Science, Nanjing University of Information Science & Technology, Nanjing, China. His research focuses on image copyright protection based on blockchain.

Zhihua Xia (Member, IEEE) received the B.S. degree from Hunan City University, Yiyang, China, in 2006 and the Ph.D. degree in computer science and technology from Hunan University, Changsha, China, in 2011. He is a Professor with the College of Cyber Security, Jinan University, Guangzhou, China. His research interests include digital forensic and encrypted image processing.

Yun-Qing Shi (Life Fellow, IEEE) received the B.S. and M.S. degrees from Shanghai Jiao Tong University, Shanghai, China, and the Ph.D. degree from the University of Pittsburgh, Pittsburgh, PA, USA. Since 1987, he has been with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA, and is currently a Professor. His research interests include multimedia data hiding, forensics and security (robust watermarking, reversible data hiding, authentication, steganography and steganalysis, tampering detection, computer graphics classification from photographic images, camera identification, detection of double JPEG or MPEG compression), visual signal processing and communications (motion analysis, and video compression and transmission), applications of image processing, computer vision and pattern recognition to industrial automation and biomedical engineering, theory of multidimensional systems, and signal processing (robust stability of linear systems, 2-D spectral factorization, and 2-D or 3-D interleaving).