Digital Image Copyright Protection Method Based on Blockchain and Perceptual Hashing

Qiu-Yu Zhang and Guo-Rui Wu
(Corresponding author: Qiu-Yu Zhang)

School of Computer and communication, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
Email: zhangqylz@163.com, vigdis_r@163.com

(Received May 7, 2022; Revised and Accepted Dec. 3, 2022; First Online Dec. 10, 2022)

Abstract

To enhance the transparency and credibility of the copyright information of digital images of grotto murals and to solve the problems of low sampling rate in the frequency domain, easy tampering, and unclear ownership of copyright information, a digital image copyright protection method based on blockchain and perceptual hashing was proposed by using the features of blockchain, such as tamper resistance, decentralization, and traceability. Firstly, the copyright owner uses the improved perceptual hashing function to convert the mural image into a 256-bit hash value and uploads it to the blockchain along with other copyright information; Then, the intelligent contract detects the infringement of the image by calculating the similarity of the hash value, and the detected copyright information and encrypted image are uploaded to the InterPlanetary File System (IPFS). Finally, the consumer downloads the image and copyright information initiates a copyright transaction, and calls the double smart contract to obtain the key and decryption the image. The experimental results show that the proposed method solves the problem of unclear ownership of copyright owners and consumers and ensures the security of asset transfer in the process of copyright transaction. The improved perceptual hashing function also improves the accuracy of determining similarity in digital image infringement detection.

Keywords: Blockchain; Copyright Protection; Grotto Murals; IPFS; Perceptual Hashing; Smart Contract

1 Introduction

With the rapid development of cloud storage, internet and multimedia technology, multimedia files show an explosive growth, which embodies the characteristics of digitalization of content, digitalization of product form, digitalization of management process and network of communication channels [35]. As a world cultural heritage [34], the dissemination of grotto murals in the form of digital images has become one of the feasible ways to popularize grotto murals. However, due to the downloading and copying of grotto mural images stored in the cloud, it is difficult to ensure the security of digital copyright, resulting in an increasing number of copyright problems. In recent years, the widely used blockchain has the characteristics of decentralization, de-trust, non-tampering and traceability [6, 18]. It can be applied in the process of image copyright protection and copyright transaction to solve the problems of digital copyright information being easily tampered with, high cost and non-traceability.

At present, the centralized copyright management system adopted in the traditional way of copyright protection is inefficient and costly, which cannot effectively solve the dilemma faced by digital copyright in the digital communication environment. Although there are many existing digital rights management (DRM) technologies such as information hiding [31, 33] and encryption, there are still some deficiencies in image copyright protection. Under the network platform, the existing technologies such as [24] digital watermarking have been unable to fully protect the rights of copyright owners [3, 4]. Users can destroy the digital watermark by removing attacks, geometric attacks, encryption attacks and protocol attacks, or eliminate, destroy and tamper with watermark through image cropping and image restoration software [2,11]. For different digital images, the existing encryption methods also have some problems such as loss of encryption and decryption data, weak security, and difficulty in retrieval. Most of the existing copyright protection methods first process the image data by image encryption based on hash function, and then compare it with the image data stored in the database, so as to determine whether the infringement occurs. Traditional cryptographic hash algorithms such as MD5 and SHA-256 are simple to implement, but due to the avalanche effect, even small changes in the image will cause drastic changes in generated hash, so the infringement detection effect of the image after adding noise and rotating operation is not good. Image perceptual hashing has a certain correlation between the original input data and the input data after slight tampering, and has a good tamper detection effect on the image data that has not changed significantly. Therefore, perceptual hashing is used to process the image data and calculate the similarity of generated hash value to determine whether the image is infringing. The blockchain-based digital image copyright protection method realizes automatic infringement detection by writing smart contracts, but there is still the problem of unclear user ownership. The mainstream blockchain is expensive to store data, and the image copyright file is relatively large, which is not suitable for direct storage on the blockchain. IPFS is a point-to-point distributed file storage system, which has the characteristics of distributed storage and openness. It can dynamically expand the storage capacity, thus effectively solving the problem of insufficient storage capacity on the blockchain caused by the large amount of grotto mural image data. However, the openness of IPFS also makes the stored image data face the risk of misappropriation. The security of copyright information and transaction process cannot be guaranteed.

To overcome such drawbacks, this paper adopts the digital images of grotto murals as the research carriers, and presents a digital image copyright protection method based on blockchain and perceptual hashing, which completes the whole process of copyright information registration, consumer information registration, and copyright transaction by writing and calling double smart contract. The summary of contributions of our work is given below:

1) By improving the spatial sampling rate of perceptual hashing frequency domain, the problem of missing image details in feature capture is solved, and the accuracy of determining similarity in digital image infringement detection is improved.

2) To combine the image perceptual hashing and MD5 algorithm, generate the unique corresponding encryption and decryption key related to the image, and encrypting the successfully registered image to be uploaded by chaotic sequence, which effectively solves the data security problem after the image is uploaded to IPFS.

3) The copyright owner and consumers use smart contract to register information respectively, which solves the problem of unclear rights between copyright owner and consumers. Meanwhile, double smart contract is called for triple security verification, which effectively solves the security problem of asset transfer during copyright transactions.

The rest of this paper is organized as follows: Related work is discussed in details in Section 2. Section 3 introduces the proposed system model and specific implementation scheme in details. Section 4 carries out the performance analysis of the proposed scheme, and compared with existing digital image copyright protection scheme. Section 5 gives example simulation results. Finally, Section 6 concludes this paper.

2 Related Works

The DRM is widely used in computer software, audio-on-demand and download, video-on-demand and download, digital library, digital image, mobile payment and other fields [27]. Scholars at home and abroad put forward different DRM schemes from different angles (such as rights sharing DRM [14], privacy protection DRM [7, 8], enterprise DRM [25] and DRM in cloud computing [16, 21]). However, most of the above schemes need centralized license servers and third-party financial platforms to assist in the issuance of licenses and the smooth execution of transactions, while the centralized server is vulnerable to attacks, resulting in services termination, and the rights transaction information and license information are opaque [17].

In recent years, many scholars have tried to apply blockchain to DRM system to solve the problems existing in traditional DRM system. Mehta *et al.* [20] proposed a decentralized peer-to-peer photo sharing marketplace built on top of Ethereum test chain, which effectively avoided the avalanche effect, but the image hashing could not deal with the 90 ° rotation of image. Shi *et al.* [28] proposed a DRM system based on blockchain and SIFT local feature extraction algorithm, which realized automatic similar infringement detection, decentralized storage, tamper-proof and traceability of copyright information. Guo *et al.* [10] proposed a blockchain-enabled DRM system, which includes an entirely new network architecture for sharing and managing multimedia resources of online education on the basis of the combination of the public and private blockchains, as well as three specific smart contract schemes for the realization of the recording of multimedia digital rights, the secure storage and the unmediated verification of digital certificates, respectively. Li *et al.* [15] proposed an image copyright protection system based on the fusion of deep neuron network and blockchain, and design a scalable DNN accelerator and SHA-256 using field-programmable gate array (FPGA). Experimental results show that the whole acceleration system can achieve up to 40x speedup comparing to software implementation on CPU. Dobre *et al.* [5] proposed a digital image copyright protection system based on blockchain, which uses as the picture identifier a joint photographic experts group (JPEG) resistant image signature. Through testing in the process of image compression, it is proved that the image signature extraction algorithm can effectively resist JPEG compression. Wang *et al.* [30] proposed a secure image copyright protection framework combines blockchain and zero-watermark technology, which realize the copyright traceability of the image and solve the problem of lack of trusted third parties. Sultana *et al.* [29] proposed a secure medical image sharing system based on zero trust principles and blockchain, which effectively improves the security of medical images in the complete transmission stage through the audit tracking of blockchain reserved data transmission, but there are still some limitations in network speed. Kr *et* *al.* [12] proposed a social media DRM system based on secret sharing, which effectively realized decentralized social media copyright management. However, when implement on traditional social media could suffer latency and low transaction rate. Abba *et al.* [9] proposed a distributed media transaction framework for DRM, which is based on the digital watermarking and a scalable blockchain model, and built a scalable blockchain model using an overlay network, which solved the scalability and security problems of DRM system. Ren *et al.* [26] proposed a robust zero-watermarking algorithm based on the angular features, and introduced blockchain to solve the problem that zero-watermarking relies on third-party copyright organizations. This framework is robust against common watermark attacks, and realizes the copyright protection for the lossless vector map. Abrar *et al.* [1] proposed to use blockchain and digital watermark for image security authentication. By using SHA-256 encryption algorithm to extract the hash value of the generated watermark, it was stored in the blockchain to realize identity authentication independent of the third-party platform. Kumar *et al.* [13] proposed a secure distributed industrial image and video data security detection system based on IPFS and blockchain, which effectively avoided a single point of failure with the help of blockchain characteristics. Liu *et al.* [19] proposed a blockchain copyright protection system combined with fabric's smart contract, which realized the automatic management of the complete digital rights life cycle of digital copyright. Nan *et al.* [22] proposed a code copyright management system based on blockchain, which verified the originality of code based on abstract syntax tree, and achieved good response speed and storage efficiency. Wang *et al.* [32] proposed an image copyright protection model based on blockchain, which ensured that the image information would not be tampered with through consensus nodes, and added digital watermark to prevent the leakage of image information. Natgunanathan *et al.* [23] proposed a multimedia copyright protection audio watermarking technology based on blockchain, which kept the perceived quality of audio signals to the greatest extent.

In summary, most of the existing DRM framework is divided into three parts: image processing, infringement detection and image storage. Considering the problem that the digital watermark is easy to be tampered with, this paper chooses perceptual hashing instead of digital watermark, and calls smart contract to calculate the similarity of hash value to complete the image infringement detection. Most of the existing smart contracts are single-chain codes, and the ownership is unclear. At the same time, the encryption algorithm of data files uploaded to IPFS and the method of obtaining keys by calling contracts are complex, which is not suitable for image information storage in big data environment. Therefore, this paper presents a digital image copyright protection method combining blockchain, improved perceptual hashing, image encryption and IPFS. The proposed method not only improves the accuracy of similarity determination in image infringement detection, but also encrypts the simple chaotic sequence by using the key related to image hashing, which enhances the security of grotto mural image data stored in IPFS, and enhances the security of copyright transaction process through double contract call and triple verification.

3 The Proposed Scheme

3.1 System Model

Figure 1 shows the system model of digital image copyright protection method based on blockchain and perceptual hashing. This model is divided into three different parts: blockchain, user and IPFS, and realizes the functions of copyright information registration, consumer information registration and copyright transaction through smart contracts.

As shown in Figure 1, the users in the system model are divided into copyright owner and consumers. The copyright owner uploads the digital images of grotto murals and related copyright information to the blockchain and IPFS, using the perceptual hashing generated by the images for infringement detection, and encrypting the images with the relevance key. Anyone who obtain grotto mural images and corresponding copyright information through legal channels as a consumer. They can download encrypted mural images and part of copyright information from IPFS as needed, which uploaded by copyright owner, and calls the double smart contract to obtain the decryption key according to the obtained copyright information. If the image file is not invalid, consumers can get the decryption key after completing asset evaluation and payment.

3.2 Algorithm Design

3.2.1 Improved Perceptual Hashing Algorithm

In order to tolerate the deformation of the image, the traditional perceptual hashing function only selects the low-frequency part of the image when it is created, which leads to the lack of image details during feature capture, reduces the accuracy of determining similarity in digital image infringement detection, and makes the result of infringement detection unsatisfactory. After cropping, noise addition, blur, sharpen, rotation and re-size similar but different images, we compared with the accuracy in the realization of infringement detection of three different hashing algorithms, Average hash (Ahash), Difference hash (Dhash) and Perception hash (Phash), and it is found that perceptual hashing algorithm is stable for the similarity measurement of images after different degrees of noise processing. Combining with the characteristics of digital images of grotto murals, the perceptual hashing algorithm is improved, and the specific processing steps are as follows:

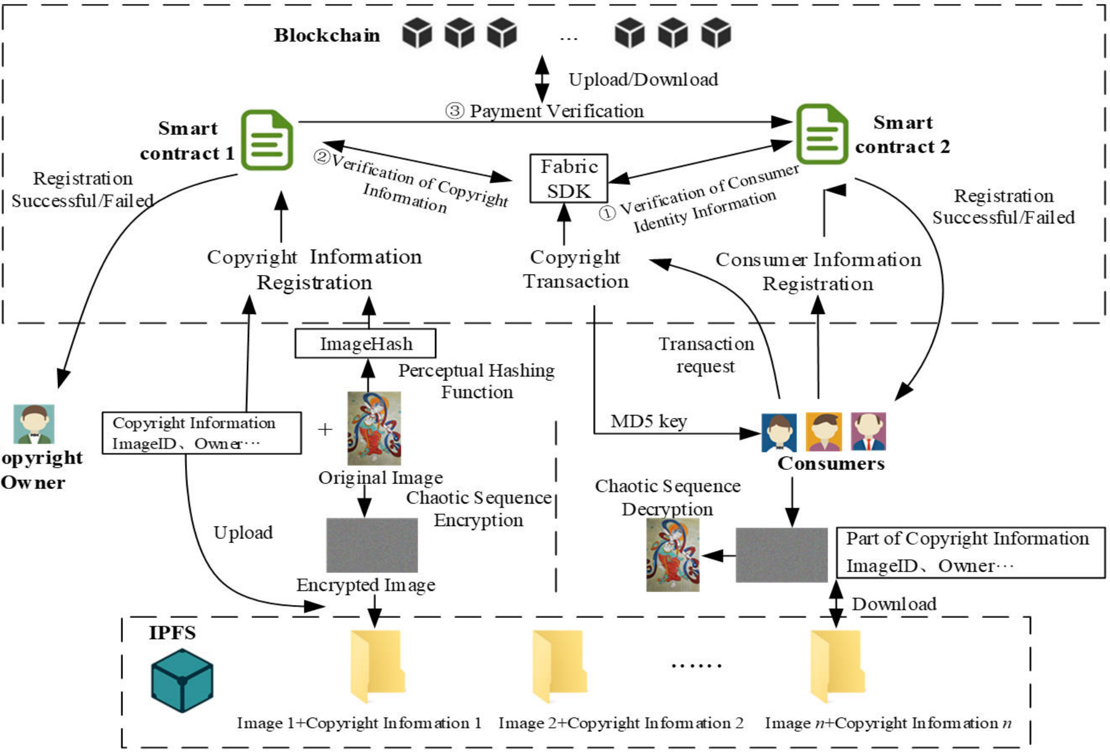

Blockchain
...
Upload/Download
③ Payment Verification
Smart contract 1
Smart contract 2
②Verification of Copyright Information
Fabric SDK
① Verification of Consumer Identity Information
Registration Successful/Failed
Registration Successful/Failed
Copyright Information Registration
Copyright Transaction
Consumer Information Registration
ImageHash
Perceptual Hashing Function
Transaction request
MD5 key
Copyright Owner
Copyright Information ImageID、Owner…
+
Original Image
Chaotic Sequence Encryption
Consumers
Chaotic Sequence Decryption
Part of Copyright Information ImageID、Owner…
Upload
Encrypted Image
Download
IPFS
……
Image 1+Copyright Information 1
Image 2+Copyright Information 2
Image n+Copyright Information n

Figure 1: The system model

Step 1. Reduces the image to get a three-dimensional array of 32 × 32 × 3.

Step 2. Convert the image into grayscale.

Step 3. Carry out discrete cosine transform (DCT) on the image and convert it into frequency domain.

Step 4. Select the part with frequency domain of 16×16 to calculate the average value.

Step 5. Generate a 2D array according to the binarization of the average value (if less than the average value then assign 1 otherwise 0), it constructs the 256-bit perceptual hashing by expanding the 2D array into a 1D array.

The improved perceptual hashing algorithm obtains the outline details of the image by moving the value part in the frequency domain, and at the same time, it doubles the sampling matrix in the frequency domain, so that the length of the generated corresponding hash value is expanded by 4 times, the sampling efficiency is high in the approximate sampling time, and the accuracy of infringement detection of hash value is greatly improved. Table 1 shows the time required to generate the hash values and calculate the similarity measurement of the images 1.jpg and 2.jpg before and after improving the perceptual hashing algorithm.

As shown in Table 1, the accuracy of the improved perceptual hashing algorithm for judging the similarity of different images has nearly doubled and the verification time has only increased by 0.000005 seconds (basically negligible).

3.2.2 Image Encryption Algorithm

IPFS is designed for all users, allowing all nodes to access it at will. The nodes connected to IPFS network can find file content and download it. At the same time, the file upload of IPFS does not need to verify the identity of the sender, and generates a unique hash value according to the file content. When the file content changes, the hash value is completely different. The grotto mural data files stored in IPFS face the following two possible threats: 1) Once a user obtains the image data through illegal means and publishes the data to IPFS or other distributed file storage systems in advance before the copyright owner completes the copyright registration of the image data, the infringing party cannot be verified according to the generation time; 2) Users can easily obtain the data stored in IPFS. After obtaining the data, they can also tamper with the image data and copyright files and publish them to other platforms.

After considering the above situation, before the copyright owner uploads the grotto mural images and copyright information to IPFS, the copyright owner must encrypt the chaotic sequence of the images by using 1D Logistic chaotic map. The equation of 1D Logistic chaotic map is shown in Equation (1).

$$X_{k+1} = U * X_k * [1 - X_k] \quad (1)$$

Table 1: The hash value generation and similarity measurement time of Images 1.jpg, 2.jpg

		Traditional Phash	The improved Phash
	Hash value (bit)	1000001010101100 0100000001000010 1000011001000010 0000000000010000	1110110000110101011001010110010000000011001001 0100000011010010111100101010000101110111001111 0110010110001110001101101100111100001101110000 1111011110001010010011100011010100011001011100 0101011100011001101110100001010000110001101010 10001110001110011101010100101000
1.jpg	Generate time (s)	0.000979	0.000997
	Hash value (bit)	1010000010001000 0100100000010001 0100000000100000 0000001000000001	0000111110100100110011100110011110101011001100 0111001001111110000110011001111001011011101000 1100111001110110001100101001100110110100110000 1100010010010110110000110101111010011001010110 1100111001101010011101111110101011011011100000 01101100110001000110010100000110
2.jpg	Generate time (s)	0.000978	0.000997
Similarity	Similarity (%)	70.31250	47.65625
measurement	Execution time (s)	0.000996	0.001001

where $k = 0, 1, ..., n$.

When the initial value $X_0 \in (0,1)$ and the control parameter $U \in (3.569945,4]$, the Logistic mapping reaches chaotic state. As the value of the U approaches 4, the iterative generated values are pseudo-random distribution, and the better encryption effect of chaotic sequences. In a chaotic system, even if the initial value X_0 changes slightly, the structure of the obtained data is completely different. In case of a fixed set of parameters, the algorithm can be easily cracked even if it is iterated to achieve a fully chaotic state. In order to solve this problem, U=4, and the key generation method is improved from a fixed X_0 to a different random key $Q(0<Q<1)$ uniquely corresponding to the image as the initial value, so as to improve the security of chaotic sequence encryption. The specific processing steps of the image encryption algorithm are as follows:

Step 1. Calculate the perceived hash value of the original image, and perform MD5 encryption on the generated 256-bit binary hash value to generate a unique $Md5Key$ (32-bit hexadecimal string).

Step 2. Partition $Md5Key$ and convert each digit from hexadecimal to decimal, and find the maximum value. In order to ensure that the chaotic function is in a chaotic state, the generated Q value must meet the condition that it is greater than 0 and less than 1. Therefore, the maximum value obtained is treated as R. After $Md5Key$ segmentation and conversion, each decimal number is divided by R (Ten decimal places are reserved). The median of the generated 32 numbers is Q.

Step 3. This 1D chaotic sequence **A** is generated by iterating Q for the same number of times according to the pixel size of the original image, then another 1D chaotic sequence **B** is obtained by normalizing the 1D sequence **A** to (0, 255), and transform **B** into a 2D matrix **G** of $M \times N$.

Step 4. The **G** and the image are bitwise XOR to obtain chaotic sequence encrypted image.

The realization of chaotic sequence encryption algorithm is shown in Algorithm 1.

Algorithm 1 Logistic chaotic sequence encryption

```
Input: $Md5Key$, $original\ image$
Output: $encrypted\ image$
initialization $R$, array $a$, array $b$, 1D sequence A, 2D matrix G
for $i \rightarrow Md5Key$ do
    $a \leftarrow$ int($i$,16)
end for
$R \leftarrow \max(a) * (3/2)$
for $j \rightarrow a$ do
    $b \leftarrow$ round($j/R$,10)
end for
$Q \leftarrow$ median($b$)
for $s \rightarrow 100$ do
    $X_0 \leftarrow Q$
end for
Generate chaotic sequence A by applying Equation (1)
Generate matrix G by applying Step 3
Get the encrypted image according to Step 4
return encrypted image
```

3.2.3 Construction of Double Smart Contract

In order to realize the copyright protection of digital images of grotto murals, by setting up Hyperledger Fabric network, creating channels and nodes (Orderer, Peer) and issuing corresponding certificates, smart contract 1 and smart contract 2 (smart contract 1 realizes the registration of copyright information and smart contract 2 realizes the registration of consumer information) are written for copyright owner and consumers respectively. The contracts are deployed to the same channel of the same network, and written by Typescript language. When a consumer initiates a copyright transaction application, it interacts with peer-to-peer service nodes through Fabric-SDK to realize the call of double smart contract, and improves the algorithm of copyright information creation and copyright transaction process.

1) Registration of copyright information

a. Copyright information creation module
Before writing the copyright information into the blockchain, the copyright owner generates a 256-bit binary string from the image data by using the improved perceptual hashing function, and then uploads it to the blockchain network with other copyright information. Then, it calls the smart contract 1 to verify whether the $imageID$ in the copyright information to be created exists, if it exists, the creation fails. If not, the uploaded image data is subject to infringement detection. By automatically calculating the Hamming distance between the $imageHash$ of copyright information to be created and $HashAll$ already stored in the blockchain, and then calculate similarity. When the similarity is less than or equal to the pre-set threshold of 47.65625%, it is proved that the image is different from others stored in the blockchain, and no infringement is involved. At this time, the copyright information is created successfully, and the unique corresponding $Md5Key$ is generated according to the hash value of the image. Otherwise, the image is judged as an infringing image, and the input is refused.

b. Copyright information inquiry module
The copyright owner can read the copyright information according to the $imageID$, and compare the $imageID$ of the copyright information to be queried with the $imageID$ existing in the blockchain. If it exists, the data will be returned to the copyright owner, otherwise the query will fail.

c. Copyright information update module
Firstly, the copyright owner inputs the $imageID$, and queries the corresponding storage position of copyright information in the blockchain according to the $imageID$, so as to update all data including $imageID$, $imageName$, $imageHash$, $Md5Key$, $imageResolution$, $CopyrightOwnerEmailAddress$, $imageCopyrightOwnerName$ and $phocopyrightValue$.

d. Copyright information deletion module
Updating copyright information in real time helps to save the storage space of blockchain, so it is necessary to delete copyright information for lost image data or expired copyright information (the copyright owner or individual of the image is changed).

The process of copyright information registration is shown in Algorithm 2.

Algorithm 2 Registration of copyright information

```
Input: $imageID, imageName, phocopyrightValue,$
    $imageResolution, imageCopyrightOwnerName,$
    $imageHash, CopyrightOwnerEmailAddress$
Output: results of copyright information creation, inquiry, update and deletion
initialization $Similarity$, $Hamming\ distance$, $HashAll \in \{0,1\}^{256}$
// calculate similarity
for $i \rightarrow 256$ do
    if $imageHash[i] != HashAll[i]$ then
        $Hamming\ distance$ += 1
    end if
end for
$Similarity = (1 - Hamming\ distance/256) * 100\%$
if $imageID$ exists then
    The copyright has been registered, so you can inquire, update and delete it
else if $Similarity > 47.65625$ then
    The $imageHash$ already exists, and the copyright creation failed
else
    Input image copyright information and generate $Md5Key$ according to $imageHash$
end if
return results of copyright information creation, inquiry, update and deletion
```

2) Registration of consumer information

a. Consumer information creation module
Consumers must have a legal identity before conducting copyright transactions, so they need to create consumer information and complete the audit through smart contract 2. After the approval, consumers can recharge certain assets to their wallets for payment in the copyright transactions.

b. Consumer information inquiry module
Consumers can query the asset value according to their personal account $OwnerName$, and determine whether they meet the conditions for purchasing digital images of grotto murals.

c. Consumer information update module
Considering the popularity of the sharing economy, current consumers may sell their accounts.

At this time, they need to change $OwnerName$ of their personal account so that they can continue to use the remaining assets under the original account. When consumers want to buy copyright information, but the current asset value is not enough, they can recharge their accounts and update the asset value part of the information.

d. Consumer information deletion module
Generally, the consumer may register multiple accounts and own corresponding assets in real applications. Once the consumer forgets the account, the account and its assets become "inactive assets" similar to banks, which not only causes the waste of blockchain storage, but also causes the loss of consumers. Therefore, consumers need to delete useless $OwnerName$ in time.

The process of consumers information registration is shown in Algorithm 3.

Algorithm 3 Registration of consumer information

```
Input: $OwnerName$, $OwnerValue$
Output: results of consumer information creation, inquiry, update and deletion
if $OwnerName$ ! exists then
    Create consumer information($OwnerName$, $OwnerValue$)
else
    The consumers has been registered, so you can inquire, update and delete it
end if
return results of consumer information creation, inquiry, update and deletion
```

3) Copyright transaction
Any node can download data from IPFS. Thus, the grotto mural images and copyright information files uploaded to IPFS will be tampered with. Therefore, the copyright owner encrypts the image and deletes some copyright information before uploading the data. When consumers download images and copyright information, the obtained images are encrypted images of grotto murals encrypted by chaotic sequences, and the obtained copyright information files are other copyright data excluding $imageHash$ and $Md5Key$. Consumers can obtain encryption and decryption keys by purchasing image copyright to decrypt images, and this process is realized by calls double smart contract. Firstly, the consumer calls smart contract 2 to verify the identity information according to their personal accounts. If consumer information exists, they calls smart contract 1 to verify the existence of image copyright information according to $imageID$. If copyright information exists, they calls smart contract 2 again for asset evaluation, and determine whether the current assets of consumers meet the payment conditions. If so, complete payment, change the balance of consumer assets and return $Md5Key$. If not, the transaction fails. After consumers get the key, they can decrypt the image, thus obtaining the digital image of grotto murals. The copyright transaction process is shown in Algorithm 4.

Algorithm 4 Copyright transaction

```
Input: $imageID$, $OwnerName$
Output: results of copyright transaction
//verify the identity information according to Algorithm 3
//verify the existence of image copyright information according to Algorithm 2
//asset evaluation according to Algorithm 2 and Algorithm 3
if $OwnerName$ ! exists then
    return Consumer identity verification failed, copyright transaction failed
else if $imageID$ ! exists then
    return Image copyright information does not exist, copyright transaction failed
else if $OwnerValue < phocopyrightValue$ then
    return Payment failed, copyright transaction failed
else
    Complete and update $OwnerValue$
    return $Md5Key$
end if
```

4 Experimental Results and Performance Analysis

The system builds Fabric 2.3 network based on Hyperledger Fabric under CentOS7, writes chain code with Typescript and completes deployment, and completes image hash generation and image chaotic sequence encryption with Python. The proposed method is tested by using a self-defined data set of grotto murals, which is about 20GB in size and includes 16 kinds of images.

4.1 Performance Analysis for Digital Image Copyright Infringement Detection

At first, perform various conversion operations on any image in the data set, such as cropping, noise addition, blur (using mean blur, adjusting blur radius to 2px, 4px, 6px, 8px, 10px), sharpen (enhancing sharpness from 1 to 6), rotation(counterclockwise) and re-size, etc. The image "2.jpg" in the experimental data set is selected for these transformations, and each original image generates 37 corresponding transformed images, as shown in Figure 2.

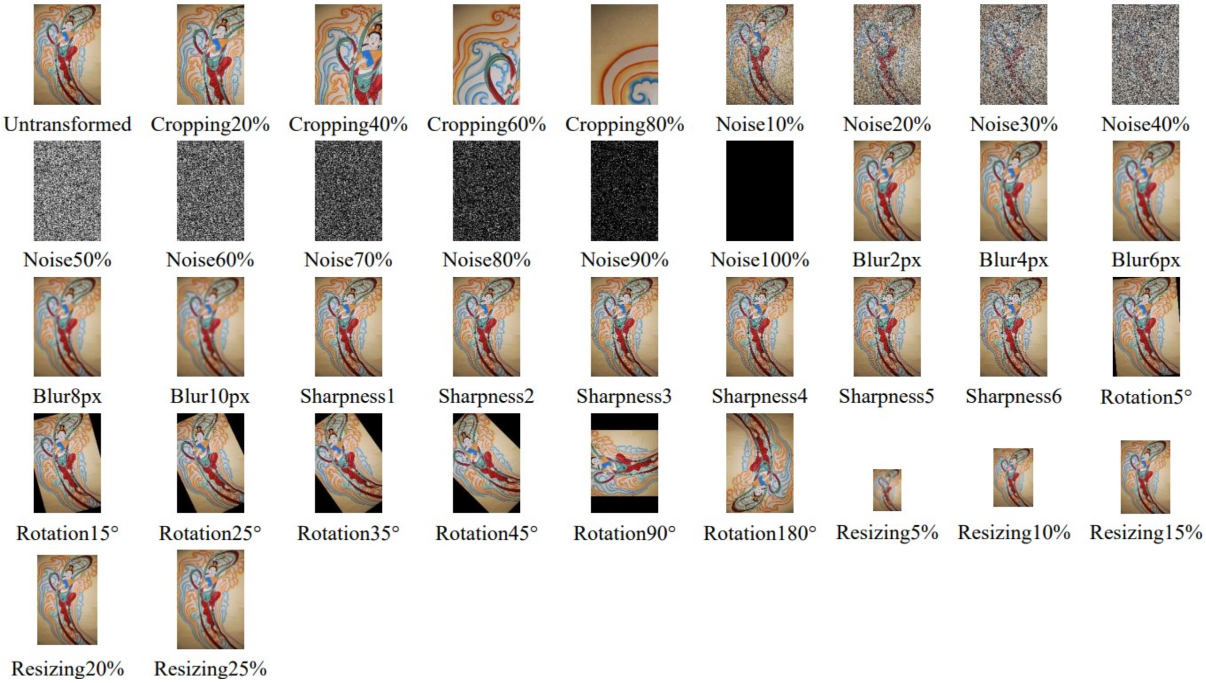


Figure 2: Operations on image 2.jpg with different modification

In order to evaluate the effectiveness of perceptual hashing in copyright infringement detection, we compare Phash, which we have used in the proposed frame work with two other techniques, Ahash and Dhash, and uses *Similarity* to measure the similarity between the original image and the modified image. The three hashing algorithms of Ahash, Dhash and Phash all return 64 bits hashes. The calculation method of *Similarity* is shown in Equation (2).

$$Similarity = (1 - \frac{Hamming\ distance}{Hashlength}) \times 100\% \quad (2)$$

where *Hamming distance* is the Hamming distance between the hash values of the two images, *Hashlength* is the length in bits of the hash value.

Considering that the image data of grotto frescoes have bright colors, many portraits, damaged, similar and noisy, two similar but different the original images (1.jpg and 2.jpg) are selected to calculate their similarity under different hash algorithms. Figure 3 shows the similarity between the image 1.jpg and 2.jpg under different hash algorithms. Figure 3(a) shows the image 1.jpg and 2.jpg. Figure 3(b) shows the similarity between the two images under three different hash algorithms.

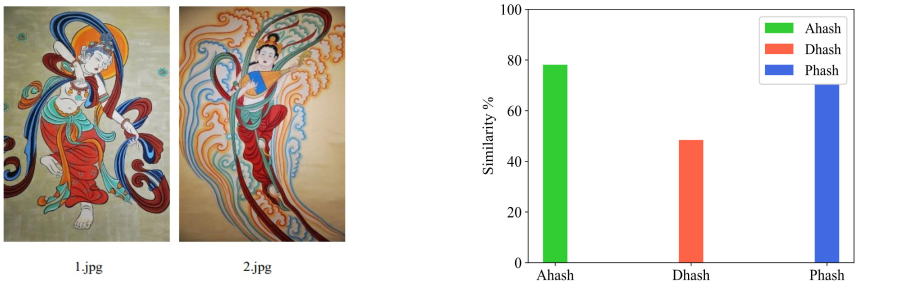
The similarity of different images is lower, the better the implementation effect of perceptual hashing algorithm. As shown in Figure 3(b), the similarity of similar but different images calculate by the Ahash, Dhash and Phash are 78.12500%, 48.43750% and 70.31250% respectively. The difference hash effect is relatively good.

In order to further evaluate the effectiveness of the three hashing algorithms for infringement detection, the original image 2.jpg is subjected to a series of image processing operations, and then the similarity between the processed images of 1.jpg and 2.jpg under different hashing algorithms is calculated again. Figure 4 shows the similarity measurement between the original image 1.jpg and the original image 2.jpg after clipping, adding noise, blurring, sharpening, rotating and resizing. Except for the noise addition, the performance of the three hashing algorithms under other image processing is: Dhash >Phash >Ahash.

Compared with the copied images and published edition in the market, the murals have higher noise which obtained by shooting, and the image effect tends to the image after noise addition processing, so it is more necessary to consider the selection of hash algorithm under noise addition processing. As shown in Figure 4(b), the similarity between Ahash and Dhash for different degrees of noise processing is quite different. Relatively speaking, Phash is more stable in the case of image noise addition processing, so Phash is used to measure the similarity of images. Although the image similarity value of Phash is relatively stable, the accuracy of similarity judgment is low. Therefore, this scheme effectively solves the problem of low accuracy by improving the perceptual hashing algorithm. Figure 5 shows the similarity measurement results of the image 1.jpg and similar image 2.jpg using improved perceptual hashing algorithm, Ahash and Dhash.

As shown in Figure 5, for similar but different images, the similarity of the improved perceptual hashing algorithm is 47.65625%. Compared with 70.31250% of the unimproved perceptual hashing algorithm and 48.43750% of the Dhash algorithm, the accuracy of similarity measurement has been greatly improved.

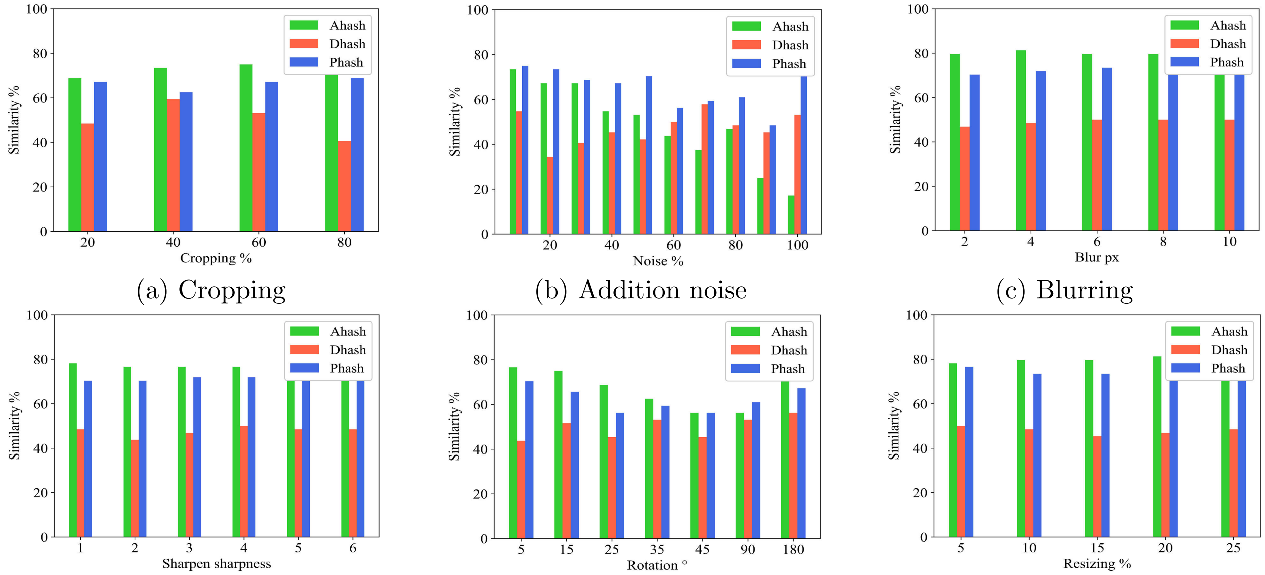
After clipping, noising, blurring, sharpening, rotating



(a) The image1.jpg and 2.jpg

(b) The similarity between the two images

Figure 3: The similarity under different hash algorithms



(a) Cropping

(b) Addition noise

(c) Blurring

(d) Sharpening

(e) Rotation

(f) Resizing

Figure 4: Before the improvement of perceptual hashing algorithm, the image 2.jpg after various transformation processing and the image 1.jpg similarity measurement.

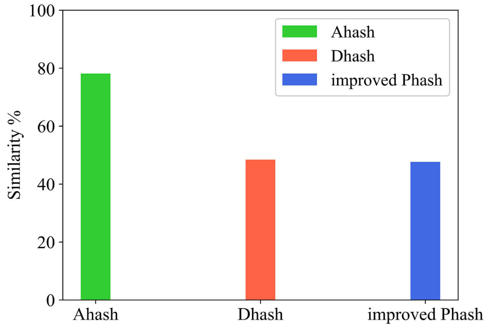


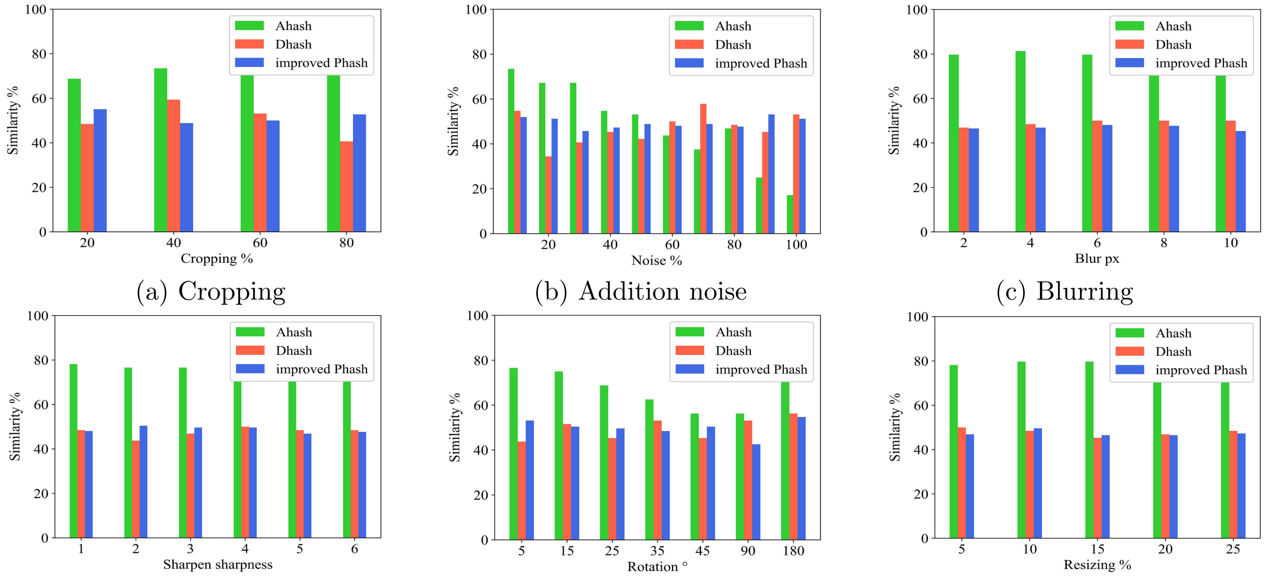
Figure 5: Similarity measurement between image 1.jpg and similar image 2.jpg under three hash algorithms

and resizing the original image 2.jpg, the similarity measurement with the original image 1.jpg is done by using the improved perceptual hash algorithm. Figure 6 shows the similarity measurement of infringement detection under different hash algorithms.

As shown in Figure 6, the accuracy of similarity measurement using the improved perceptual hashing algorithm has been greatly improved. The performance of the improved perceptual hashing algorithm is relatively stable in different degrees of noise addition processing. Except for noise addition, other image processing methods use the improved perceptual hashing algorithm to measure image similarity, which is better than Ahash and Dhash. Therefore, this scheme sets the similarity threshold to 47.65625%, selects the improved perceptual hashing algorithm to process the image data, uploads the generated hash value to the blockchain, and measures the similarity in the smart contract to realize the infringement detection of the image copyright.

4.2 Performance Analysis for Image Encryption Algorithm

In order to enhance the security of the images uploaded to IPFS, a unique chaotic sequence encryption initial value X_0 is determined for each image by MD5 algorithm, and the images are encrypted. Figure 7 shows the compari-



(a) Cropping (b) Addition noise (c) Blurring

(d) Sharpening (e) Rotation (f) Resizing

Figure 6: After improved perceptual hashing algorithm, the image 2.jpg after various transformation processing and the image 1.jpg similarity measurement of infringement detection.

son of the original image, encrypted image and decrypted image of the image 1.jpg.

(a) Original (b) Encrypted (c) Decrypted

Figure 7: The comparison of the original image, encrypted image and decrypted image of the image 1.jpg

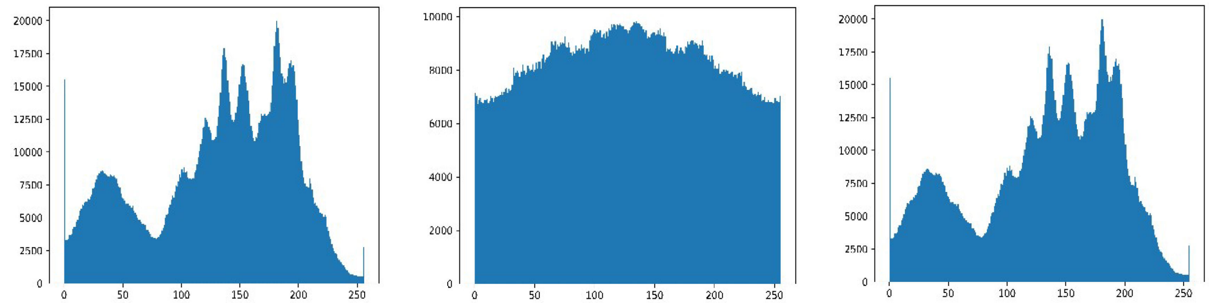
The performance of image encryption algorithm is analyzed by histogram analysis in statistical analysis, and the generated gray histogram of the image 1.jpg is shown in Figure 8.

As shown in Figure 8, the gray histogram of the original image shows obvious statistical laws, and is vulnerable to statistical analysis attacks. The distribution of gray histogram of the encrypted image is uniform, which is completely different from the original image. It is proved that the encryption scheme in the proposed method is secure, and can resist statistical analysis attacks well.

4.3 Performance Comparison with Existing Copyright Protection Schemes

Table 2 shows the comprehensive performance comparison results between proposed scheme and the existing multimedia content copyright protection schemes in [10, 13, 19, 20, 23, 32].

As shown in Table 2, the existing digital copyright protection schemes based on blockchain mostly realize automatic infringement detection through smart contracts, thus ensuring the privacy and security of digital copyright. The DRM system proposed in scheme [10] takes into account the characteristics of online educational multimedia resources, uses three smart contracts to realize copyright protection, and conducts infringement detection through watermark extraction and hash digest. Although the accuracy rate is improved, the verification is complicated and the system is not scalable. Scheme [13, 20] detects infringement by perceptual hashing, which ensures the verification effect and reduces the verification complexity, but the ownership of users is not treated. Scheme [19, 32] uses the consensus mechanism of blockchain to realize full-cycle copyright protection by smart contract, but does not consider the infringement detection and data security of digital copyright content itself. Scheme [23] ensures the security of multimedia copyright protection through improved watermarking algorithm, but there are still security and ownership problems due to the restriction of digital watermarking algorithm and single contract. By analyzing the problems existing in the above copyright protection technologies, this scheme improves the traditional perceptual hashing algorithm, and improves the judgment accuracy while ensuring the low verification complexity. Meanwhile, using the scheme [10] for reference, the double smart contract is used to solve the problem that the user's rights in a single contract are unclear. In the smart contract 1, the infringement detection module is combined with the copyright information registration process to realize automatic infringement detection. At the same time, the correlation key and chaotic sequence encryption are combined to encrypt the image data to be uploaded to



(a) Original (b) Encrypted (c) Decrypted

Figure 8: The gray histogram of the image 1.jpg

Table 2: Performance comparison with existing copyright protection schemes

Authors	Scalability	Privacy	Security	Double smart contract	Infringement detection
Ref. [20]	✓	✓	✓	×	wavelet hash
Ref. [10]	×	✓	✓	×	watermark/hash digest
Ref. [13]	✓	✓	✓	×	perceptual hashing
Ref. [19]	×	✓	✓	×	none
Ref. [32]	×	✓	✓	×	none
Ref. [23]	✓	✓	✓	×	watermark
Proposed	✓	✓	✓	✓	perceptual hashing

IPFS, which improves the security of digital images of grotto murals.

5 Example Simulation Results

5.1 Digital Image Copyright Infringement Detection

In order to verify the realization of the infringement detection part in the smart contract 1, after the copyright information creation of the image 2.jpg is successfully completed, the images processed with different degrees of noise are uploaded, Table 3 shows the creation results of corresponding copyright information of processed images.

Table 3: The copyright information creation results of the image 2.jpg

Noise addition (%)	Similarity with image 1.jpg (%)	Acceptance result
10	51.95312	Rejected
20	51.17188	Rejected
30	45.70312	**Accepted**
40	47.26562	**Accepted**
50	48.82812	Rejected
60	48.04688	Rejected
70	48.82812	Rejected
80	47.65655	Rejected
90	53.12500	Rejected
100	51.17188	Rejected

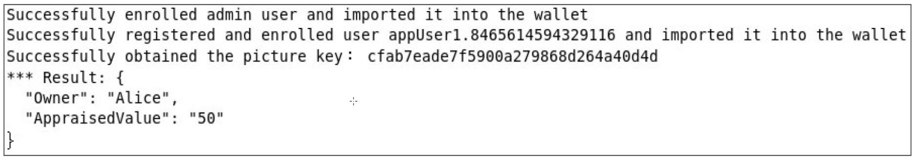
As shown in Table 3, the images with different proportions of noise addition (except for 30% and 40% of noise addition) failed to pass the infringement detection created by copyright information, which proves that using the improved perceptual hashing algorithm to judge the similarity can effectively identify the infringing images and realize the copyright protection of grotto mural images.

5.2 Image Copyright Transaction

In order to obtain the required image, consumers need to purchase the image copyright and obtain the $Md5Key$ to decrypt the encrypted image downloaded by IPFS. Copyright transaction mainly includes three parts: verification of consumer identity information, verification of the existence of image copyright information and asset evaluation. The copyright transaction process is completed by calling double smart contracts. The copyright transaction success interface is shown in Figure 9.

5.3 Upload and Download of Files in IPFS

The copyright owner completes the uploading of encrypted images and part of copyright information on IPFS. Before uploading, put the image and copyright information to be uploaded into a folder (the folder is named after the $imageID$ and contains encrypted image data and copyright information), and then upload the folder through IPFS network. After success, the encrypted image data hash value, copyright information hash value and folder hash value will be generated at the same time. Ac-



```
Successfully enrolled admin user and imported it into the wallet
Successfully registered and enrolled user appUser1.8465614594329116 and imported it into the wallet
Successfully obtained the picture key： cfab7eade7f5900a279868d264a40d4d
*** Result: {
  "Owner": "Alice",
  "AppraisedValue": "50"
}
```

Figure 9: The copyright transaction success

cording to the configured IPFS URL, port number and generated folder hash value, you can directly view the contents of phocopyright1 folder in the browser, and all nodes in IPFS can download the uploaded files according to the hash value generated when uploading the folder. The process of uploading and downloading IPFS files is shown in Figure 10.

As shown in Figure 10(a), the copyright owner stores the grotto murals encrypted image (1-encrypt.jpg) and part of the copyright information text file (phocopyright-info.txt) in the folder (phocopyright1). As shown in Figure 10(b), the copyright owner uses the IPFS file upload command to complete the upload of phocopyright1. After successful upload, IPFS hash of phocopyright1, 1-encrypt.jpg and phocopyroght-info.txt are generated respectively. At this time, the uploaded phocopyright1 can be viewed in the browser, and the results displayed in the browser are shown in Figure 10(c), (d) and (e). The consumer uses the IPFS file download command to get the folder named after the IPFS hash value of phocopyright1, and the successful download interface is shown in Figure 10(f).

6 Conclusions

In order to realize the copyright protection of digital images of grotto murals, and solve the problems that copyright information is easy to tamper and cannot be traced, a digital image copyright protection method based on blockchain and perceptual hashing was proposed by combining perceptual hashing, image encryption, blockchain and IPFS. The proposed method improves the existing perceptual hashing algorithm to solve the problems of missing image details in feature capture and low accuracy in image infringement detection, and redefines the frequency domain spatial sampling in image data hashing, which greatly improves the accuracy of image similarity threshold. In addition, combining image hash and MD5 to generate a unique and random key for chaotic encryption reduces the possibility of users stealing copyright information. Through smart contracts, copyright owner and consumers can register first and then upload/download, and the security of copyright trading process is enhanced through triple judgment when double smart contract are called. Copyright owners only upload encrypted images and part of copyright information to IPFS, which also improves the security of copyright data to a certain extent, effectively expands the storage space of blockchain and reduces the storage cost. The simulation results show that the proposed method can effectively protect the copyright of digital images of grotto murals, and can be further applied to other multimedia data copyright protection fields.

In this paper, the chaotic sequence encryption key generation method is simple, and the key space is small, which ensures the security and improves the encryption efficiency. However, there is a risk of being cracked, and there are still shortcomings in fine-grained access control of copyright transactions. The further research plan is to further improve the security of DRM by improving the key generation method, combining zero trust mechanism, searchable encryption and other technologies.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61862041). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] A. Abrar, W. Abdul and S. Ghouzali, "Secure image authentication using watermarking and blockchain," *Intelligent Automation and Soft Computing*, vol. 28, no. 2, pp. 577–591, 2021.

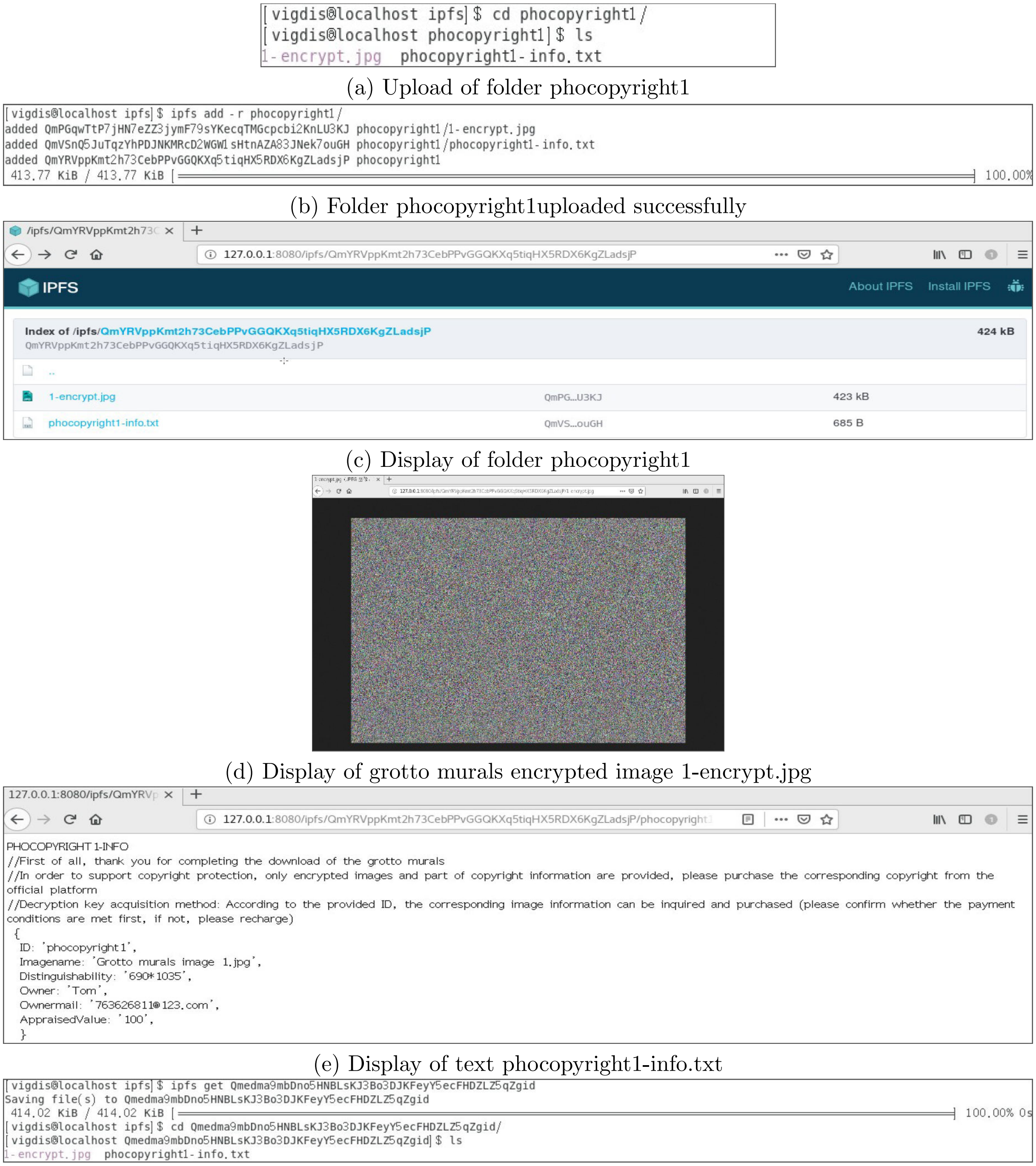
[2] C. C. Chang, K. F. Hwang, M. S. Hwang, "A digital watermarking scheme using human visual effects", *Informatics*, vol. 24, no. 4, pp. 505–511, Dec. 2000.

[3] C. C. Chang, K. F. Hwang, M. S. Hwang, "A block based digital watermarks for copy protection of images," in *Fifth Asia-Pacific Conference on Communications*, vol. 2, pp. 977-980, 1999.

[4] C. C. Chang, K. F. Hwang, M. S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics", *IEE Proceedings-Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43-50, 2002.

[5] R. A. Dobre, R. O. Preda, R. A. Badea, *et al.*, "Blockchain-based image copyright protection system using jpeg resistant digital signature," in *2020 IEEE 26th International Symposium for Design and Technology in Electronic Packaging(SIITME)*, IEEE, Pitesti, Romania, pp. 206–210, Oct. 2020.

[6] T. Feng, R. Y. Yang and R. B. Gong, "Digital copyright protection system for oil and gas knowledge achievements based on blockchain," *Interna-*



```
[vigdis@localhost ipfs]$ cd phocopyright1/
[vigdis@localhost phocopyright1]$ ls
1-encrypt.jpg  phocopyright1-info.txt
```

(a) Upload of folder phocopyright1

```
[vigdis@localhost ipfs]$ ipfs add -r phocopyright1/
added QmPGqwTtP7jHN7eZZ3jymF79sYKecqTMGcpcbi2KnLU3KJ phocopyright1/1-encrypt.jpg
added QmVSnQ5JuTqzYhPDJNKMRcD2WGW1sHtnAZA83JNek7ouGH phocopyright1/phocopyright1-info.txt
added QmYRVppKmt2h73CebPPvGGQKXq5tiqHX5RDX6KgZLadsjP phocopyright1
 413.77 KiB / 413.77 KiB [══════════════════════════════════════════════════╡ 100.00%
```

(b) Folder phocopyright1uploaded successfully

/ipfs/QmYRVppKmt2h73C
127.0.0.1:8080/ipfs/QmYRVppKmt2h73CebPPvGGQKXq5tiqHX5RDX6KgZLadsjP
IPFS
About IPFS
Install IPFS

Index of /ipfs/QmYRVppKmt2h73CebPPvGGQKXq5tiqHX5RDX6KgZLadsjP 424 kB
QmYRVppKmt2h73CebPPvGGQKXq5tiqHX5RDX6KgZLadsjP

..		
1-encrypt.jpg	QmPG...U3KJ	423 kB
phocopyright1-info.txt	QmVS...ouGH	685 B

(c) Display of folder phocopyright1

(d) Display of grotto murals encrypted image 1-encrypt.jpg

127.0.0.1:8080/ipfs/QmYRVp
127.0.0.1:8080/ipfs/QmYRVppKmt2h73CebPPvGGQKXq5tiqHX5RDX6KgZLadsjP/phocopyright1

```
PHOCOPYRIGHT 1-INFO
//First of all, thank you for completing the download of the grotto murals
//In order to support copyright protection, only encrypted images and part of copyright information are provided, please purchase the corresponding copyright from the
official platform
//Decryption key acquisition method: According to the provided ID, the corresponding image information can be inquired and purchased (please confirm whether the payment
conditions are met first, if not, please recharge)
 {
  ID: 'phocopyright1',
  Imagename: 'Grotto murals image 1.jpg',
  Distinguishability: '690*1035',
  Owner: 'Tom',
  Ownermail: '763626811@123.com',
  AppraisedValue: '100',
  }
```

(e) Display of text phocopyright1-info.txt

```
[vigdis@localhost ipfs]$ ipfs get Qmedma9mbDno5HNBLsKJ3Bo3DJKFeyY5ecFHDZLZ5qZgid
Saving file(s) to Qmedma9mbDno5HNBLsKJ3Bo3DJKFeyY5ecFHDZLZ5qZgid
 414.02 KiB / 414.02 KiB [═════════════════════════════════════════════════╡ 100.00% 0s
[vigdis@localhost ipfs]$ cd Qmedma9mbDno5HNBLsKJ3Bo3DJKFeyY5ecFHDZLZ5qZgid/
[vigdis@localhost Qmedma9mbDno5HNBLsKJ3Bo3DJKFeyY5ecFHDZLZ5qZgid]$ ls
1-encrypt.jpg  phocopyright1-info.txt
```

(f) Folder phocopyright1 download successfully

Figure 10: Upload and download of files in IPFS

tional Journal of Network Security, vol. 23, no. 4, pp. 631–641, 2021.

[7] T. Gaber, A. Ahmed and A Mostafa, "Privdrm: A privacy-preserving secure digital right management system," in*Proceedings of the Evaluation and Assessment in Software Engineering*, ACM, Trondheim, Norway, pp. 481–486, Apr. 2020.

[8] J. T. Gao, H. Y. Yu, X. Q. Zhu, *et al.*, "Blockchain-based digital rights management scheme via multi-authority ciphertext-policy attribute-based encryption and proxy re-encryption," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5233-5244, 2021.

[9] A. Garba, A. D. Dwivedi, M. Kamal, *et al.*, "A digital rights management system based on a scalable blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2665–2680, 2021.

[10] J. Q. Guo, C. Y. Li, G. Z. Zhang, *et al.*, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimedia Tools and Applications*, vol. 79, no. 15, pp. 9735–9755, 2020.

[11] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–555, Jan. 2000.

[12] M. Kripa, A. Nidhin Mahesh, R. Ramaguru, *et al.*, "Blockchain framework for social media drm based on secret sharing," in *2020 International Conference on Information and Communication Technology for Intelligent Systems*, Springer, Singapore, pp. 451–458, Oct. 2020.

[13] R. Kumar, R. Tripathi, N. Marchang, *et al.*, "A secured distributed detection system based on ipfs and blockchain for industrial image and video data security," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 128–143, 2021.

[14] T. Li, H. Wang, D. B. He, *et al.*, "Blockchain-based privacy-preserving and rewarding private data sharing for iot," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15138–15149, 2022.

[15] W. Li, Y. Zhu, L. Tian, *et al.*, "FPGA-based hardware acceleration for image copyright protection system based on blockchain," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, New York, NY, USA, pp. 234–239, Aug. 2020.

[16] X. B. Li, M. Darwich, M. A. Salehi,*et al.*, "A survey on cloud-based video streaming services," *Advances in Computers*, vol. 123, pp. 193–244, 2021.

[17] L. Liu, W. Shang, W. Lin, *et al.*, "A decentralized copyright protection, transaction and content distribution system based on blockchain 3.0," in *2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter)*, IEEE, Ho Chi Minh City, Vietnam, pp. 45–50, Jan. 2021.

[18] L. Liu, W. Zhang and C. Han, "A survey for the application of blockchain technology in the media," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3143–3165, 2021.

[19] Y. Liu, J. Zhang, S. Wu, *et al.*, "Research on digital copyright protection based on the hyperledger fabric blockchain network technology," *PeerJ Computer Science*, vol. 7, p. e709, 2021.

[20] R. Mehta, N. Kapoor, S. Sourav, *et al.*, "Decentralised image sharing and copyright protection using blockchain and perceptual hashes," in *2019 11th International Conference on Communication Systems Networks(COMSNETS)*, IEEE, Bengaluru, India, pp. 1–6, Jan. 2019.

[21] D. Mishra, A. Kasi, M. S. Obaidat, *et al.*, "Construction of lightweight content key distribution framework for drm systems," in *2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, Arad, Romania, pp. 863–868, Dec. 2021.

[22] J. Nan, Q. Liu and V. Sugumaran, "A blockchain-based code copyright management system," *Information Processing & Management*, vol. 58, no. 3, p. 102518, pp. 1-17, 2021.

[23] I. Natgunanathan, P. Praitheeshan and L. X. Gao, "Blockchain-based audio watermarking technique for multimedia copyright protection in distribution networks," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 18, no. 3, pp. 1–23, 2022.

[24] J. S. Pan, X. X. Sun, S. C. Chu, *et al.*, "Digital watermarking with improved sms applied for qr code," *Engineering Applications of Artificial Intelligence*, vol. 97, p. 104049, 2021.

[25] S. Rana and D. Mishra, "Provably secure authenticated content key distribution framework for iot-enabled enterprise digital rights management systems," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 36, no. 3, pp. 131–140, 2021.

[26] N. Ren, Y. Z. Zhao, C. Q. Zhu, *et al.*, "Copyright protection based on zero watermarking and blockchain for vector maps," *ISPRS International Journal of Geo-Information*, vol. 10, p. 294, pp. 1–20, 2021.

[27] J. Y. Shen, "Blockchain technology and its applications in digital content copyright protection," in *Proceedings of the 4th International Conference on Economic Management and Green Development*, Springer, Singapore, pp. 18–25, Jan. 2021.

[28] J. Shi, D. Yi and J. Kuang, "A blockchain and sift based system for image copyright protection," in *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, ACM, Xi'an, China, pp. 1–6, Dec. 2019.

[29] M. Sultana, A. Hossain and F. Laila, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Medical Informatics and Decision Making*, vol. 20, p. 256, pp. 1–10, 2020.

[30] B. Wang, S. Jiawei, W. Wang, *et al.*, "A blockchain-based system for secure image protection using zero-watermark," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, IEEE, Delhi, India, pp. 62–70, Dec. 2020.

[31] C. Wang, B. Ma, Z. Xia, *et al.*, "Geometric resistant polar quaternion discrete fourier transform and its application in color image zero-hiding," *ISA transactions*, vol. 125, pp. 665–680, 2022.

[32] Z. Wang and T. Li, "Research on image copyright confirmation and protection model based on blockchain," in *2021 2nd International Conference on Control, Robotics and Intelligent System*, ACM, Qingdao, China, pp. 230–234, Aug. 2021.

[33] N. I. Wu, M. S. Hwang, "A novel LSB data hiding scheme with the lowest distortion", *The Imaging Science Journal*, vol. 65, no. 6, pp. 371–378, 2017.

[34] Z. Yan, "The color and artistic features of murals in dunhuang cave 465 in mogao grottoe," in *The 6th International Conference on Arts, Design and*

Contemporary Education (ICADCE2020), Atlantis Press, Moscow, Russia, pp. 56–62, Jan. 2021.

[35] D. Zhang, X. J. Wu, T. Xu, *et al.*, "Watch: Two-stage discrete cross-media hashing," *IEEE Transactions on Knowledge and Data Engineering*, https://doi.org/10.1109/TKDE.2022.3159131, pp. 1–13, 2022.

Biography

Qiu-yu Zhang Researcher/Ph.D. supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research center, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.

Guo-rui Wu is currently a master student of the School of Computer and Communication, Lanzhou University of Technology, China. She received the BS degrees in network engineering from Lanzhou Institute of Technology, Gansu, China, in 2020. Her research interests include network and information security, multimedia data security, blockchain.