Journal of Information Hiding and Privacy Protection
DOI:10.32604/jihpp.2021.026606
Article

Tech Science Press

A Image Copyright Protection Method Using Zero-Watermark by Blockchain and IPFS

Tao Chen[1], Zhao Qiu[1,*], Gengquan Xie[1], Lin Yuan[1], Shaohua Duan[1], Hao Guo[1], Dahao Fu[1] and Hancheng Huang[2]

[1]Hainan University, Haikou, 570228, China
[2]University college London, London, WC1E 6BT, UK
[*]Corresponding Author: Zhao Qiu. Email: qiuzhao@hainanu.edu.cn

Received: 31 December 2021; Accepted: 13 January 2022

Abstract: Behind the popularity of multimedia technology, the dispute over image copyright is getting worse. In the digital watermark prevention technology for copyright infringement, watermark technology is considered to be an important technology to overcome data protection problems and verify the relationship between data ownership. Among the many digital watermarking technologies, zero watermarking technology has been favored in recent years. However, the existing zero watermark technology in the implementation process often needs a trusted third party to store watermarks, which may make the data too central, data storage security is low and copyright registration costs are too high, which creates a rare problem. The decentivization and information cannot be tampered of blockchain technology's nature find new methods for image copyright protection. This paper studies the role of zero watermark algorithm in the image copyright and its complete storage and certification scheme, proposes a zero watermark image protection framework based on blockchain, and builds a system according to the framework. Combined with blockchain and zero watermarking technology, the framework uses inter IPFS (Inter Planetary File System) to solve the problem of blockchain efficient storage and sharing of large files. In addition, the application of user copyright information, image image query and image trading in the system are realized based on smart contracts, which solves the problem of lack of trusted third parties. Experiments show that the scheme is feasible and robust to various attacks.

Keywords: Zero watermarking; blockchain; IPFS; copyright protection

1 Introduction

With the rapid development of multimedia, data and information technology more and more convenient, resulting in the original image copyright cannot be guaranteed, which makes the issue of image protection has become one of the most prominent problems.

Digital watermarking is one of the most effective technologies to solve the copyright problem of digital multimedia copyright protection [1]. Its basic idea is to embed an imperceptible signal "tag" into the carrier's image, and when there is a copyright dispute, the copyright of the copyright is solved by manipulating the embedded marker to extract the copyright. According to the detection method, the digital copyright watermark can be divided into blind watermark, non-blind watermark and zero watermark three ways, in which blind watermark and non-blind watermark are embedded in the carrier image, which will destroy the transparency of the original image and data structure. Zero watermarks [2] can be done without modifying the characteristics of the original image, extract the characteristics of carrier images and copyright watermarks to generate unique zero watermark information, and finally register the resulting watermark information to a viable third-party Intellectual Property Right(IPR).This solves the problem of content completion and transparency of blind watermark and non-blind watermark.

But the security, reliability, and stability of the third-party Intellectual Property Right(IPR) have not been addressed, making it difficult for zero-watermark solutions to be applied on the ground, and the advent of blockchain technology has solved the problem. The emergence of blockchain technology has solved this problem. Blockchain has the characteristics of decentralization, high reliability and non-tamperability. It is suitable as a fully trusted third-party Intellectual Property Right(IPR), so studying zero watermarking algorithm and blockchain-based storage system can solve the problem of image copyright protection. In this article, we selected Ethereum as the blockchain and IPFS to design a framework. This framework can protect image copyright and track the transactions of image rights. It has good scalability.

The improved zero watermarking algorithm extracts key points by scale-Invariant Feature Transform, then discrete wavelet transformation(DWT) to obtain the subband coefficient, then fast Fourier transformation(FFT), and finally the KEY zero watermark key by different or computational operations By improving the zero watermark algorithm, a third-party Intellectual Property Righ(IPR) based on Ethereum blockchain is proposed to ensure the security and reliability of IPR, so as to ensure that the generated unique zero watermark information cannot be tampered with in IPR and can trace the information of image copyright transaction. Use the distributed storage system IPFS(Inter Planetary File System) to store the information of image copyright protection and ensure sufficient storage space of data.

2 Related Work

2.1 Zero-Watermark Algorithm

In order to solve the shortcomings of digital watermarking in content integrity and data structure, Chen et al. [2] first proposed a new idea and concept of digital zero-watermarking in 2010. This watermarking technology cannot modify any data of the original image, which can well solve the contradiction between the perceptibility and robustness of the digital watermark. Therefore, zero-watermark is studied and applied in image copyright protection by more and more people. In 2017, Shen et al. [3] proposed a novel time-domain zero-watermarking algorithm based on Non-Uniform Rectangular Partition. In 2009, Che et al. [4] proposed a digital watermarking algorithm based on wavelet. This algorithm has strong invisibility and can accurately determine the location of the watermark in order to improve the robustness of the zero -watermark. In 2018, Yang et al. [5] proposed a strong robust zero watermarking algorithm based on NSCT(Non-sampling Contourlet Transform domain) transform and image normalization. The scheme has good anti attack ability and imperceptibility, and can be applied in the field of zero watermark. In 2009, Chang et al. [6] proposed an adaptive copyright protection scheme that can adjust the watermark strength through the threshold. This scheme meets the requirements of data lossless and can resist various signal processing operations and geometric transformations. In 2012, Tsai et al. [7] (CAI) and others proposed a blind watermarking scheme for image copyright protection based on DWT-SVD, which uses particle optimization algorithm to calculate the watermark proportion to optimize DSS. In order to solve the shortcomings of image watermarking based on SVD, others proposed two methods: embedding the main components of the watermark into the cover image in DCT domain and embedding the image into the host image in DWT domain. Li et al. [8] proposed an improved Sobel algorithm, which changed the traditional Sobel algorithm from two directions to eight directions, so as to improve the direction of edge direction detection and make the algorithm more robust to geometry.

2.2 Blockchain

Blockchain technology was first proposed in Bitcoin: A Peer-to-Peer Electronic Cash System [9] published by Ben Cong in mid-2008. Since it was proposed, it has been pursued by many scholars and researchers. Although bitcoin is one of the most successful cases of the current commercialization of blockchain technology, it can only be used for bitcoin transactions, and there are few other application scenarios. Ethereum can be applied in finance, education, medical treatment, logistics and other fields. It is one of the most widely used and successful technologies in the blockchain. Ethereum is a universal and completely distrusted platform, which is open and programmable. It has the characteristics of decentralized, data tamper proof, traceability and permanent storage.

In order to better store data, some schemes using blockchain have been proposed. Tian et al. [10] (Medical System) proposed a lightweight and scalable blockchain framework, which adopts loose coupling design to provide integrity and effectiveness verification for evidence. In 2020, Liang et al. [11] (Medical System) and others proposed a blockchain technology scheme that can solve data storage and recovery methods, which can encode and repair network data storage. In recent years, more and more blockchain storage platforms have begun to appear, such as IPFS [12], Storj [13], SIA [14], Swarm [15], and they are all distributed. The IPFS(Inter Planetary File System) is a point-to-point distributed file system, which allocates a unique hash value to each stored file through content addressing and is one of the most widely used storage platforms. It solves the problems of insufficient centralized storage, network data storage and data distribution, and can save data safely and faster, which plays an important role in the construction of blockchain. So, many blockchain based schemes use IPFS network as the storage phase for decentralized storage. In 2020, Sun et al. [16] proposed an encryption scheme based on attribute EMR, which stores the data in IPFs to ensure the data security in EMR. In 2018, Zheng et al. [17] proposed to reduce the data storage size in the blockchain by using IPFs network. This scheme has good results in storage space and security. In 2017, Chen et al. [18] proposed a scheme to combine IPFs storage with sawtooth storage model with blockchain, which solves the problem of high throughput of individual users in IPFS.

Inspired by the above literature, we propose a scheme of zero watermark image copyright protection based on Ethereum blockchain. We link the zero-watermark information and upload it to IPFS, and the whole storage and research process are recorded by Ethereum.

3 Preliminary

We will cover some preliminary knowledge and related technology in this section.

3.1 Zero-Watermark

3.1.1 Scale-Invariant Feature Transform

SIFT(Scale-Invariant Feature Transform) is a computer vision feature extraction algorithm used to detect and describe local features in images. In essence, it searches for key points (feature points) in different scale spaces and calculates the direction of the key points. The key points found by SIFT are some very prominent points that will not change due to factors such as illumination, affine transformation and noise, such as corner points, edge points, bright spots in dark areas, and dark points in bright areas.

The SIFT algorithm is broken down into the following four steps:

1). Extremum detection in scale space: Search for image positions on all scales. The Gaussian differential function is used to identify potential points of interest that are invariant to scale and rotation.

$$G(x,y,\sigma)=\frac{\frac{1}{2\pi\sigma^2}e^{-(x^2+y^2)}}{2\sigma^2 L} \tag{1}$$

$$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y) \tag{2}$$

* represents the convolution operation, (x, y) represents the pixel position of the image. σ is a scale space factor. The smaller the value, the less the image is smoothed, and the smaller the corresponding scale. The large scale corresponds to the general features of the image, and the small scale corresponds to the detailed features of the image.

$$D(x,y,\sigma)=\big(G(x,y,k\sigma)-G(x,y,\sigma)\big)*I(x,y)=L(x,y,k\sigma)-L(x,y,\sigma) \tag{3}$$

Construct DOG scale-space, the difference of the Gaussian function can be calculated using two similar scales, separated by a constant multiplier k. Feature points are composed of local extreme points in DOG space. In order to find the extreme points of the DOG function, each pixel must be compared with all its neighbors to see if it is larger or smaller than its neighbors in the image domain and scale domain.

2). Key point location: At each candidate location, a fine-fitting model is used to determine the location and scale. The selection of key points depends on their degree of stability.

3). Direction determination: Based on the local gradient direction of the image, one or more directions are assigned to each key point position. All subsequent operations on the image data are transformed relative to the direction, scale and position of the key points, thereby providing invariance to these transformations. the modulus formula and the gradient direction formula are as follows:

$$m = \sqrt{\left(L_{x+1,y} - L_{x-1,y}\right)^2 - \left(L_{x,y+1} - L_{x,y-1}\right)^2} \tag{4}$$

$$\theta = \arctan\left(\frac{L_{x,y+1} - L_{x,y-1}}{L_{x+1,y} - L_{x-1,y}}\right) \tag{5}$$

4). Key point description: In the neighborhood around each key point, measure the local gradient of the image on the selected scale. These gradients are transformed into a representation that allows relatively large local shape deformation and illumination changes.

3.1.2 Discrete Wavelet Transform (DWT)

DWT is to discretize the scale and translation of the basic wavelet. In image processing, dyadic wavelet is often used as the wavelet transform function, that is, the integer power of 2 is used for division. Wavelet transform (WT) is also used to process signal, it is mainly to sample the wavelet in discrete intervals. The wavelet transform can reflect the space of the image as well as the frequency domain information of the image.

Decomposition formula:

$$C_{j+1,k} = \sum_{n \epsilon Z} C_{j,n} \overline{h}_{n-2k} \quad k \epsilon Z \tag{6}$$

$$d_{j+1,k} = \sum_{n \epsilon Z} C_{j,n} \overline{g}_{n-2k} \quad k \epsilon Z \tag{7}$$

Reconstruction formula:

$$C_{j,k} = \sum_{n \epsilon Z} C_{j+1,n} h_{k-2n} + \sum_{n \epsilon Z} d_{j+1,n} g_{k-2n} \quad k \epsilon Z \tag{8}$$

3.1.3 Fast Fourier Transform (FFT)

FFT is a discrete Fourier transform (DFT) algorithm that can be completed in O(nlogn) time. The DFT of a finite discrete signal x(n), n=0, 1,..., N-1 is defined as

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn} \quad k = 0,1,\dots,N-1,\ W_N = e^{-j\frac{2\pi}{N}} \tag{9}$$

DFT needs to calculate about N2 multiplications and N2 additions. FFT is improved on the basis of DFT and the calculation time is improved to NlogN. Using the symmetry and periodicity of WN, the N-point DFT is decomposed into two N/2-point DFTs, so that the total calculation amount of the two N/2-point DFTs is only half of the original, that is (N/2)2 + (N/2)2 = N2/2, so that the decomposition can continue, and then N/2 is decomposed into two N/4-point DFTs. In this way, the amount of calculation can be reduced to (N/2) log2N multiplications and Nlog2N additions.

3.2 Ethereum

3.2.1 Blockchain

The infrastructure of blockchain is shown in Fig. 1. It is composed of five layers: data layer, network layer, consensus layer, control layer and application layer. Although each layer has different functions, it can support each other to realize a decentralized trust mechanism. The data layer describes the physical form of blockchain technology, including Merkle tree, block storage and timestamp. It is the basic layer of blockchain architecture. The network layer is a distributed network without the supervision of a third-party central organization. In essence, it is a P2P network. Each node not only receives information, but also generates information. Nodes maintain communication by maintaining a common blockchain. Such a distributed network determines that each node has all the information of the system, and the attack on a single node will not affect the normal operation of the system. The consensus layer enables highly decentralized nodes to efficiently reach consensus on the effective of block data in a decentralized system, which is the key to ensure the good performance of the blockchain network. Among the common consensus mechanisms, it mainly includes PoW(Proof of Work) [19], PoS(Proof of Stake) [20] and PBFT(Practical Byzantine Fault Tolerance) [21]. The contract layer mainly refers to various script codes, algorithm mechanisms and smart contracts. It is the key layer to realize the programmability of the blockchain. Smart contracts can be deployed to the blockchain according to their own needs and are automatically executed by the platform. The application layer is the layer of application sequence derived from blockchain, which encapsulates various application scenarios and cases of blockchain. In this basic model, each level has its own role and implementation method, which can flexibly apply the blockchain to various use scenarios.

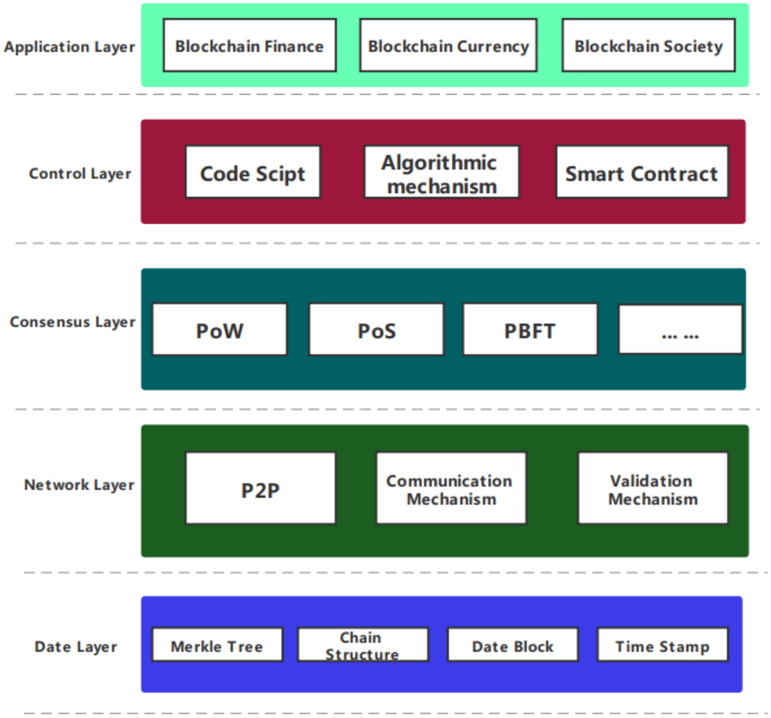


Figure 1: Infrastructure of blockchain

3.2.2 Ethereum

Bitcoin only brings the concept of blockchain and realizes the application of blockchain technology in digital currency. There is almost no general blockchain application development platform, so Ethereum came into being. Ethereum is the product of Blockchain 2.0 Architecture. Compared with bitcoin project, Ethereum is much younger. However, the emergence of Ethereum expands the application scope of blockchain technology. It aims to build a system with a wide range of applications and support complete blockchain application development.

Ethereum is a decentralized blockchain platform, in which each node in the network can send “transactions” or “bookkeeping”, that is, record and execute “transactions” sent on the network. These nodes can reach data consistency through the consensus mechanism, it can form a whole. At the same time, compared with bitcoin architecture, Ethereum has faster speed and more advanced reward mechanism. Moreover, Ethereum supports smart contracts. Users can define their own digital assets and circulation logic. Any calculation can be performed through Ethereum, so Ethereum can be used as a more general blockchain platform to support various decentralized applications. The so-called smart contract is actually an EVM executable code. No matter publishing or calling the smart contract, the information of the smart contract is attached to the "transaction" and published to the network in the form of transaction. Therefore, after the nodes in the Ethereum network receive the transaction, EVM will execute the corresponding contract code. Finally, all nodes reach a consensus through the consensus algorithm, and the content and status of the contract will be consistent throughout the network.

3.2.3 IPFS

IPFS is a content addressed, distributed and new hypermedia transmission protocol, which can share files. It is also more suitable as a third-party Intellectual Property Right(IPR). IPFS supports the creation of fully distributed applications. It aims to make the network faster, safer and more open. IPFS is a distributed file system. Its goal is to connect all computing devices to the same file system, so as to become a national unified storage system.

IPFS and Ethereum work together, which can supplement the two defects of low storage efficiency and high cost in Ethereum, and the coordination and difficult coordination between different chains across the chain. For the first defect, IPFS is used to store file data, and the only permanently available IPFS address is placed in the blockchain, instead of putting the data itself in the blockchain. For the second defect, IPFs can assist different blockchain networks to transfer information and files.

During file storage, IPFs first decomposes a file into multiple data blocks, and then calculates hash values for these data blocks. In each node, these hash values calculated by a file are stored in a hash table. If multiple nodes are stored in the hash value of this file in the hash table, the file hash value is maintained in the distributed hash table. When obtaining a file, you can send the corresponding hash value to the IPFS file system for request. IPFS file system assigns a unique hash value to each file, which enables IPFS to support content-based addressing.

4 The Proposed Framework

In this section, we will introduce the proposed framework in Fig. 2 for zero watermark image copyright protection, and describe its main structure. More design details will be given in the next section.

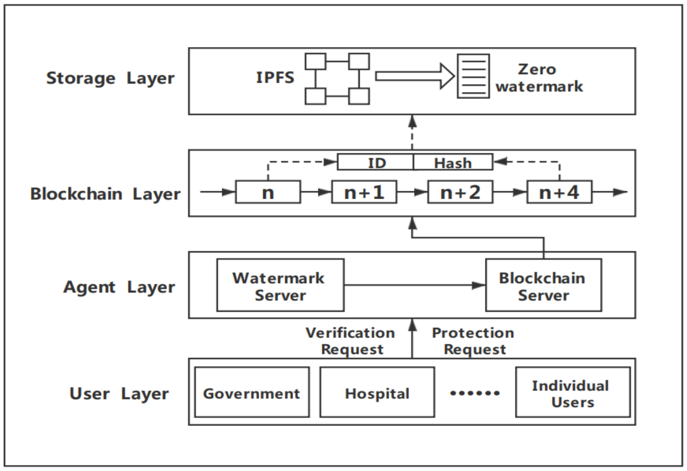


Figure 2: The proposed framework

4.1 Architecture Overview

The blockchain links the zero watermark information and stores the zero watermark data in IPFS. Specifically, after the image of each organization in the entity layer is protected by the verification request, the verification request will be uploaded to the watermark server. In the agent layer, the watermark server generates a zero watermark according to the image and uploads it to the blockchain server. In the blockchain layer and storage layer, store the zero watermark data in IPFS, and then return a unique hash value in IPFS according to the uploaded zero watermark information, and store the hash value in the blockchain to save the storage space in the block and save the gas consumption in the blockchain.

4.2 User Layer

The user layer consists of hospitals, governments, remote sensing images and hospitals. The images generated by these mechanisms will be uploaded to the watermark server, and zero watermark information will be generated in the watermark server. When it is necessary to verify whether the image is the image of the organization, it is only necessary to send a verification request to verify the zero watermark information uploaded to the blockchain. When the verification is successful, the server will feed back a message that is the same picture as the organization; when the verification fails, a message that is not the same picture as the organization will be fed back.

4.3 Agent Layer

The agent layer mainly includes two agent servers: watermark server and blockchain server.

1) Watermark server: When an organization uploads an image for copyright protection, it will carry out a series of watermark processing on the uploaded original image to extract the zero watermark in each image, which can still extract the zero watermark in the image for geometric attacks and conventional attacks, so as to strengthen the robustness of the digital watermark.

2) Blockchain server: The zero watermark information generated in the watermark server is chained to the blockchain. This makes the zero watermark that originally needed the third-party intellectual property right no longer need the copyright protection center. It can solve the problem of centralized storage of the original zero watermark, realize decentralized storage, and make the storage of zero watermark traceable. The non tamperability cannot be realized before the zero watermark is realized, which ensures the security of the zero watermark information and makes the zero watermark more credible.

4.4 Blockchain Service Layer

The block structure in the blockchain is shown in the Fig. 3 below. It is a distributed ledger. The block is composed of two parts: block header and block header. The block header stores the original information of the block. It is used to identify, verify and explain the content of the block. In the block body, all transactions in the block are packaged and integrated. Organizing blocks into chains can effectively reduce the possibility of existing block data being changed or deleted, which is also a major feature of the blockchain itself.

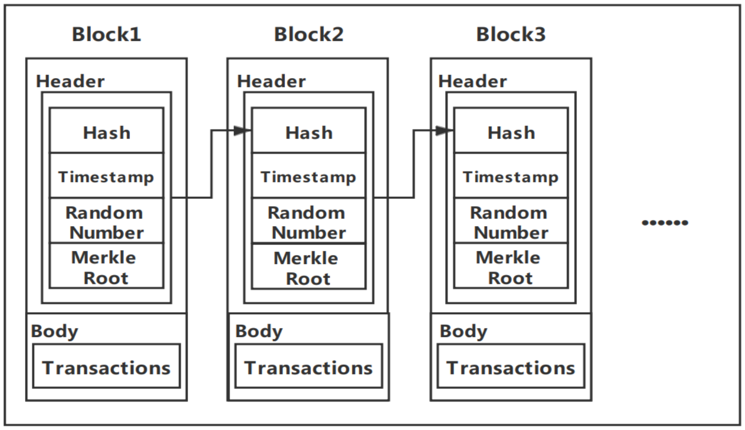


Figure 3: The block structure

4.5 Storage Layer

The zero watermark information and some correction information stored in the storage layer are stored in IPFS outside the chain. When the entity layer sends an authentication request, it needs to store the information in IPFS. In order to protect the zero watermark information from malicious modification and save the storage space in the blockchain, the files stored in IPFS will be hashed and the hash value will be written to the blockchain. Therefore, the entity layer will obtain the corresponding unique watermark information stored in IPFS through the hash value in the block, and then compare it with the zero watermark generated by the image in the verification request, so it is easy to verify the authenticity of the data.

5 Zero-Watermark Algorithm Design

Our framework is flexible and scalable and can be combined with most zero-watermark algorithms. However, after considering a number of features, we have improved the traditional zero-watermark and suggested a more suitable zero-watermark algorithms for Blockchain.

Since most hash algorithms, such as perceptual hash algorithms, can resist scaling attacks, but it is difficult to resist geometric attacks such as rotation and translation, zero watermark technology is adopted. This paper uses Scale-Invariant Feature Transform to extract feature values, discrete wavelet transform (DWT) to obtain sub-band coefficients, fast Fourier transform (FFT) to reduce the amount of calculation, and finally performs exclusive OR operation to obtain the KEY zero watermark key. Our zero-watermark algorithm consists of two parts: zero-watermark generation part and zero-watermark validation part.

1) The generation part is show in Fig. 4:

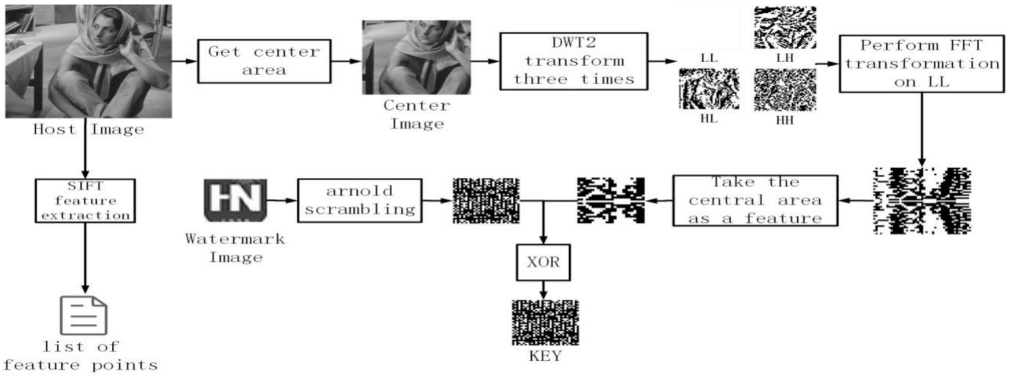


Figure 4: The generation part

Step 1: Extract the central area of the original image E(i,j) to obtain CE(i,j).

Step 2: Perform SIFT transformation [22] on the original image E(i,j) to obtain the key point description.

Step 3: Perform DWT2 transformation on the transformed image CE(i,j) to obtain subband coefficients {LL,HL,LH,HH}.

Step 4: Perform FFT transformation on the subband coefficient LL to extract the middle region matrix D(i,j).

Step 5: Perform arnold scrambling on the watermark image W(i,j) to obtain EW(i,j).

Step 6: D(i,j) and EW(i,j) are XORed to obtain the KEY zero-watermark key.

2) The validation part is show in Fig. 5:

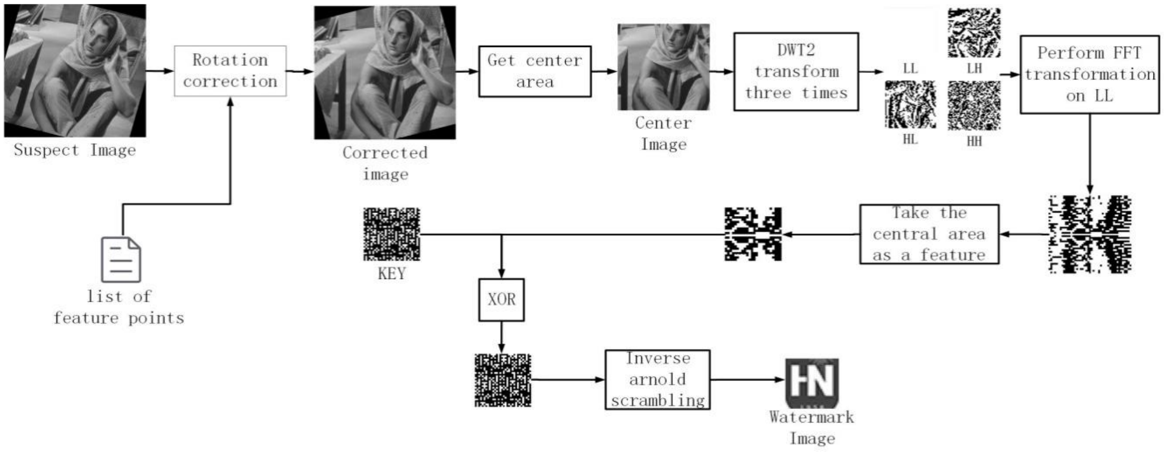


Figure 5: The validation part

Step 1: Extract the central area of the original image E(i,j) to obtain CE(i,j).

Step 2: Perform SIFT transformation on the original image E(i,j) to obtain the key point description.

Step 3: Perform DWT2 transformation on the transformed image CE(i,j) to obtain subband coefficients {LL,HL,LH,HH}.

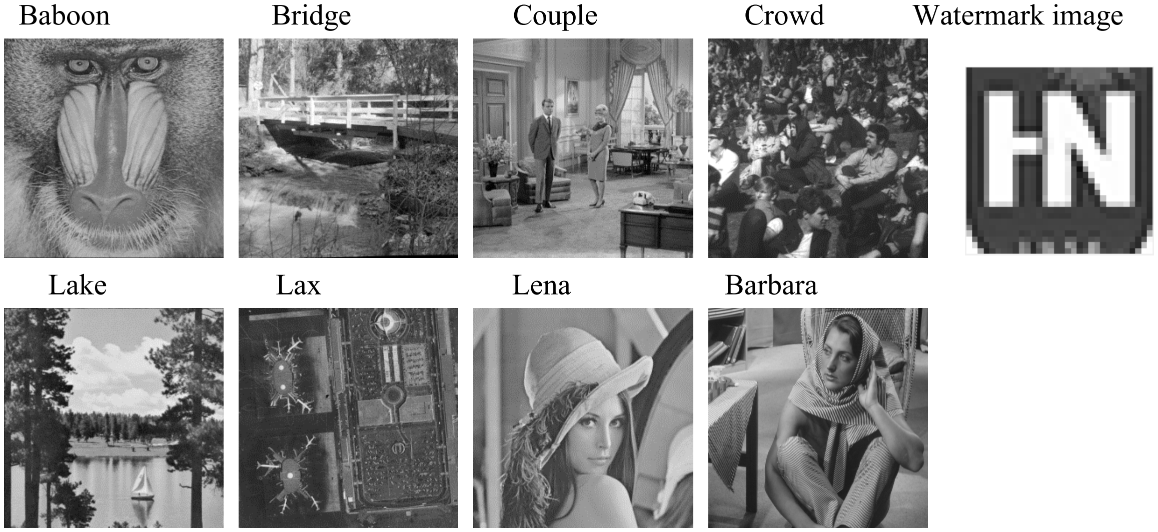
Step 4: Perform FFT transformation on the subband coefficient LL to extract the middle region matrix D(i,j).

Step 5: Perform arnold scrambling on the watermark image W(i,j) to obtain EW(i,j).

Step 6: D(i,j) and EW(i,j) are XORed to obtain the KEY zero watermark key.

6 Experiments and Analysis

In order to evaluate our proposed scheme, this article selected eight famous gray images from the USC-SIPI image database including Baboon, Bridge, Couple, Crowd, Lake, Lax, Lena, Barbara. The standard 256 × 265 gray image is select as the host image and the watermark is 32 × 32 binary image. They are shown in Fig. 6.


Baboon Bridge Couple Crowd Watermark image

Lake Lax Lena Barbara

Figure 6: Original host images and a watermark image

6.1 Algorithm Perform Test

Table 1 shows the algorithm perform against some typical and JPEG-compression attack. For the recovered watermarks, the NCs are lager than 0.83. The high robustness against some typical and JPEG-compression attack of the proposed algorithm is verified here.

Table 1: Algorithm perform

Attack	Baboon	Bridge	Couple	Crowd	Lake	Lax	Lena	Barbara
Non-Attack	1	1	1	1	1	1	1	1
Lossy JPEG (QF = 90%)	0.9941	0.9970	0.9970	1	0.9985	0.9911	0.9985	0.9970
Lossy JPEG (QF = 50%)	0.9749	0.9852	0.9911	1	0.9970	0.9794	0.9925	0.9882
Lossy JPEG (QF = 20%)	0.9461	0.9881	0.9763	0.9925	0.9911	0.9678	0.9719	0.9767
Gaussian noise (0.1%)	0.9721	0.9823	0.9897	0.9941	0.9897	0.9780	0.9752	0.9868
Gaussian noise (2%)	0.8748	0.9514	0.9181	0.9593	0.9596	0.9019	0.9006	0.9231
Gaussian noise (5%)	0.8299	0.9152	0.8936	0.9482	0.9267	0.8867	0.8641	0.9069
Salt-pepper noise (0.1%)	0.9707	0.9911	0.9852	1	0.9896	0.9882	0.9838	0.9881
Salt-pepper noise (2%)	0.9206	0.9632	0.9514	0.9782	0.9868	0.9385	0.9509	0.9650
Salt-pepper noise (10%)	0.8495	0.9330	0.9035	0.9333	0.9223	0.9011	0.8855	0.8861
Speckle noise (0.1%)	0.9821	0.9912	0.9911	0.9985	0.9985	0.9868	0.9897	0.9911
Speckle noise (10%)	0.8490	0.9349	0.9412	0.9684	0.9421	0.9263	0.9017	0.9117
Average filter 3 × 3	0.9780	0.9882	0.9911	0.9970	0.9896	0.9825	0.9794	0.9912
Average filter 4 × 4	0.9266	0.9692	0.9692	0.9781	0.9579	0.9469	0.9624	0.9647
Median filter 3 × 3	0.9565	0.9780	0.9837	0.9897	0.9822	0.9425	0.9823	0.9868
Median filter 4 × 4	0.8956	0.9574	0.9622	0.9707	0.9527	0.9242	0.9610	0.9619
Motion filter 3 × 3	0.9810	0.9823	0.9941	0.9970	0.9911	0.9825	0.9823	0.9882
Motion filter 4 × 4	0.9694	0.9794	0.9853	0.9970	0.9911	0.9738	0.9707	0.9838
Rotation 0.5	0.8818	0.9396	0.9270	0.9440	0.9168	0.8974	0.9010	0.9222
Scaling 0.25	0.9494	0.9706	0.9810	0.9941	0.9868	0.9639	0.9576	0.9882
Scaling 0.9	0.9882	0.9970	0.9882	0.9911	0.9927	0.9854	0.9941	0.9970
Scaling 1.1	0.9416	0.9777	0.9689	0.9794	0.9737	0.9607	0.9839	0.9719
Scaling 2	0.9912	1	1	1	1	0.9941	0.9970	1

Table 2: Algorithm perform

Attack	Scheme [3]		Proposed Scheme	
	BER	NC	BER	NC
Lossy JPEG (QF = 90%)	0.0078	0.9893	0.0019	0.9970
Lossy JPEG (QF = 70%)	0.0127	0.9827	0.0020	0.9970
Lossy JPEG (QF = 50%)	0.0166	0.9775	0.0078	0.9882
Lossy JPEG (QF = 30%)	0.0361	0.9522	0.0078	0.9882
Lossy JPEG (QF = 10%)	0.1094	0.8681	0.0273	0.9590
Gaussian noise (5%)	0.0791	0.9010	0.0635	0.9069
Salt-pepper noise (1%)	0.0283	0.9621	0.0225	0.9664
Median filter 3 × 3	0.0488	0.9365	0.0088	0.9868
Gaussian LPF 3 × 3	0.0186	0.9749	0.0019	0.9970

It can be seen from Table 2 that the proposed scheme is more robust than Scheme [3]. We can see that the effect from NC or BER is better than Scheme [3]. For the recovered watermarks, NCs are lager than 0.90 and BER are less smaller than 0.027. Through experiments, it can be concluded that the proposed scheme is proved to be effective. Users can protect image copyright and make sure security of zero-watermark related information, and this can enhance algorithm.

6.2 Security Analysis

Our paper proposes decentralized image copyright protection method using zero-watermark. We use IPFS and blockchain to achieve decentralization and protect the security of zero-watermark information. Compared with the traditional zero-watermark scheme, our scheme is more secure and focuses on the protection of zero-watermark information. We remove the trusted third party in the traditional zero-watermark, put all zero-watermark information in IPFS for storage, and then return the hash value generated by IPFS and put it in the blockchain. This ensures the reliability and security of the data.

7 Conclusion

In the increasingly serious image copyright disputes, image copyright protection is becoming more and more important. The solution of zero-watermark combined with blockchain can solve the related disputes of image copyright protection. Although the zero-watermark requires a third-party storage platform, which will cause the storage of the zero-watermark information center to be insecure, the emergence of the blockchain solves this problem and can guarantee the security of the zero-watermark information. This article studies the copyright protection and traceability of images, so that Zero Watermark does not require a trusted third-party platform. Putting it on the blockchain and IPFS effectively solves the shortcomings of untrustworthy watermarks.

Acknowledgement: First of all, I would like to thank my tutor Professor Qiu Zhao for his care and support for me. He patiently guided me to revise my thesis until it was completed. My mentor’s open-minded and modest personality left me a deep impression and benefited a lot. Second, I want to thank my classmates Wang, Duan, Fu and Li for their help. Many ideas were formed in the fierce discussion with my classmates. Thirdly, I would like to thank my parents for their support. Finally, I would like to thank School of Computer Science and Technology, Hainan University. It gives me a good research environment to enable me to complete this article so successful.

Funding Statement: This work is supported by Hainan Provincial Key Research and Development Program (No. ZDYF2020018), Haikou Key Research and Development Program (No. 2020-049) and Hainan Provincial Natural Science Foundation of China (No. 2019RC100).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. S. Wang and W. C. Chen, “A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography,” *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 757–762, 2009.

[2] H. Chen, T. Luo, M. Yu, G. Jiang, H. Zhou *et al.,* “A zero-watermark method based on texture characteristic of image blocks for stereo images,” in *2012 Int. Conf. on Industrial Control and Electronics Engineering*, pp. 490–493, 2012.

[3] Z. Shen and U. Kintak, “A novel image zero-watermarking scheme based on non-uniform rectangular,” in *2017 Int. Conf. on Wavelet Analysis and Pattern Recognition (ICWAPR)*, pp. 78–82, 2017.

[4] S. Che, B. Ma, Z. Che and Q. Huang, “A wavelet-based method of zero-watermark,” in *2009 Int. Conf. on Wavelet Analysis and Pattern Recognition*, pp. 293–297, 2009.

[5] K. Yang, W. Wang, Z. Yuan and W. Zhao, “Strong robust zero watermarking algorithm based on NSCT transform and image normalization,” in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conf. (IAEAC)*, pp. 236–240, 2018.

[6] C. C. Chang and P. Y. Lin, “Adaptive watermark mechanism for rightful ownership protection,” *Journal of Systems and Software*, vol. 81, no. 7, pp. 1118–1129, 2008.

[7] H. H. Tsai, Y. J. Jhuang and Y. S. Lai, “An SVD-based image watermarking in wavelet domain using SVR and PSO,” *Applied Soft Computing*, vol. 12, no. 8, pp. 2442–2453, 2012.

[8] L. Li, S. Wang, W. Zeng nd F. Qin, “Research on zero watermarking technique based on improved Sobel operator,” in *2021 IEEE Int. Conf. on Artificial Intelligence and Industrial Design (AIID)*, pp. 594–597, 2021

[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, 21260, 2008.

[10] Z. Tian, M. Li, M. Qiu, Y. Sun and S. Su, “Block-DEF: A secure digital evidence framework using blockchain,” *Information Sciences*, vol. 491, pp. 151–165, 2019.

[11] W. Liang, Y. Fan, K. C. Li, D. Zhang and J. L. Gaudiot, “Secure data storage and recovery in industrial blockchain network environments,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020.

[12] J. Benet, “IPFS-content addressed, versioned, P2P file system,” *arXiv preprint arXiv*:1407.3561, 2014.

[13] S. Wilkinson, T. Boshevski, J. Brandoff and V. Buterin, “Storj a peer-to-peer cloud storage network,” [Online]. Available: https://www.storj.io/storjv2.pdf, 2014.

[14] D. Vorick and L. Champine, “Sia: Simple decentralized storage,” [Online]. Available: https://blockchainlab.com/pdf/whitepaper3.pdf, 2014.

[15] L. Acampora, “Swarm,” *The Missouri Review*, vol. 35, no. 3, pp. 64–80, 2012.

[16] J. Sun, X. Yao, S. Wang and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS,” *IEEE Access*, vol. 8, pp. 59389–59401, 2020.

[17] Q. Zheng, Y. Li, P. Chen and X. Dong, “An innovative IPFS-based storage model for blockchain,” in *2018 IEEE/WIC/ACM Int. Conf. on Web Intelligence (WI)*, pp. 704-708, 2018.

[18] Y. Chen, H. Li, K. Li and J. Zhang, “An improved P2P file system scheme based on IPFS and blockchain,” in *2017 IEEE Int. Conf. on Big Data (Big Data)*, pp. 2652–2657, 2017.

[19] A. Biryukov and I. Pustogarov, “Proof-of-work as anonymous micropayment: Rewarding a Tor relay,” in *Int. Conf. on Financial Cryptography and Data Security*, pp. 445–455, 2015.

[20] A. Kiayias, A. Russell, B. David and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Annual Int. Cryptology Conf.*, pp. 357–388, 2017.

[21] G. Xu, Y. Liu, J. Xing, T. Luo, Y. Gu *et al.,* “SG-PBFT: A secure and highly efficient blockchain PBFT consensus algorithm for Internet of vehicles,” *arXiv preprint arXiv*:2101.01306, 2021.

[22] S. Duan, H. Wang, Y. Liu, L. Huang and X. Zhou, “A novel comprehensive watermarking scheme for color images,” *Security and Communication Networks*, vol. 2020, no. 4, pp. 1–12, 2020.