IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 23, 2021, accepted April 6, 2021, date of publication April 9, 2021, date of current version April 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3072196

Blockchain-Watermarking for Compressive Sensed Images

MING LI[1,2,3,4], LEILEI ZENG[1,2,3,4], LE ZHAO[1,2,3,4], RENLIN YANG[1,2,3,4], DEZHI AN[5], AND HAIJU FAN[1,2,3,4]

[1]College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China
[2]Engineering Laboratory of Intelligence Business & Internet of Things, Henan Normal University, Xinxiang 453007, China
[3]Big Data Engineering Laboratory of Teaching Resources and Assessment of Education Quality, Henan Normal University, Xinxiang 453007, China
[4]Key Laboratory of Artificial Intelligence and Personalized Learning in Education of Henan Province, Xinxiang 453007, China
[5]School of Cyber Security, Gansu University of Political Science and Law, Lanzhou 730070, China

Corresponding author: Ming Li (liming@htu.edu.cn)

This work was supported in part by the Team Project of Collaborative Innovation in Universities of Gansu Province under Grant 2017C-16, in part by the Major Project of Gansu University of Political Science and Law under Grant 2016XZD12, in part by the National Natural Science Foundation of China under Grant 61602158, in part by the Science and Technology Research Project of Henan Province under Grant 212102210413, in part by the Key Research Projects of Henan Higher Schools under Grant 20A413007, and in part by the Doctoral Talents Research Initiation Project of Henan Normal University under Grant 20190319.

ABSTRACT With the application of multimedia big data, the problems such as information leakage and data tampering have emerged. The security of images which is one of the most typical multimedia has become a major problem facing the large-scale open network environment. This paper proposed a blockchain-watermarking scheme to protect the privacy, integrity and availability of compressed sensed images, which effectively combines multimedia watermarking, compressed sensing, Interplanetary File System (IPFS) and blockchain technologies. Based on the reliable authentication of watermarking, the confidentiality protection of compressed sensing, the secure storage of IPFS, and the decentralization and non-tamperability of blockchain, the all-round security protection of the image big data based on compressive sensing can be realized. Experiments show that the proposed scheme is effective and feasible.

INDEX TERMS Blockchain, IPFS, compressed sensing, watermarking, data hiding.

I. INTRODUCTION

With the development of informatization, the multimedia big data including images, videos, audios, etc. is growing rapidly. The application of multimedia big data is becoming more and more extensive, including social media, video surveillance, medical equipment, etc., making our lives more colorful. However, multimedia data, especially images, may face risks such as illegal theft, malicious tampering, and privacy leakage during the processes of storage, dissemination, and processing. Therefore, the issue of image security in the open network environment has addressed many attentions of researchers.

Compressed sensing [1] can use random sampling to obtain discrete samples of sparse signals under the condition much less than the Nyquist sampling rate, and then perfectly reconstruct the signal through a nonlinear reconstruction algorithm. The efficient sampling and compressed method is very suitable for the processing of multimedia big data. After incorporating cryptographic features, compressed sensing can also be used as a lightweight encryption scheme to efficiently protect the privacy of multimedia big data in an untrusted network environment [2], [3]. Zhang *et al.* [4] proposed an image encryption system based on two-dimensional compressed sensing. This study uses global random replacement to encrypt the image, and uses two-dimensional compressed sensing to compress the encrypted image to reduce the complexity of the algorithm. In addition, a two-dimensional projection image algorithm is proposed to reconstruct the image. In [5], a secure image coding scheme based on compressed sensing is proposed. The scheme uses compressed sensing to accurately restore the original information from a small number of samples. In the encoding process, a random matrix is used to compress the image into multiple linear digital measurement values. During decryption, the random matrix is used as the decryption key to recover the original signal. Experiments have proved the feasibility of the scheme. Although compressed sensing

The associate editor coordinating the review of this manuscript and approving it for publication was Larbi Boubchir.

combined with cryptographic features can guarantee the confidentiality [6] of data. However, the integrity and availability of data cannot be guaranteed. The traditional digital watermarking mechanisms [7]–[9] are the main methods to protect the integrity and availability of multimedia. Yang *et al.* [9] proposed a watermarking scheme for colorful image copyright protection and integrity verification. This method generates a feature watermark by extracting the characteristics of the host image, and then embeds the feature watermark into the host image to generate a watermark image. In the paper, the Stirmark3.1 attack is used on the watermarked image to verify the integrity, robustness and usability of the scheme. Most of the existing watermarking techniques are applied in the plaintext domain [9], [10], because the signal redundancy in the plaintext image can provide additional embedding space. However, plaintext has the risk of privacy leakage. Although watermarking technology can guarantee the integrity and availability of the host image, it cannot realize the privacy protection of multimedia data in the open network environment. Therefore, in order to ensure the confidentiality, integrity and availability of data at the same time, the application of watermarking in the encrypted domain [11], [12] is no time to delay. In order to meet the needs of ciphertext watermark embedding, Xiao *et al.* [7] proposed a robust and separable ciphertext watermarking scheme based on compressed sensing. This method first divides the image into non-overlapping blocks including important blocks and non-important blocks with edge detection, then uses traditional encryption and compressed sensing technology to encrypt them respectively, and then realizes the embedding of the watermark in the encrypted domain according to the embedding secret key. The receiving end can extract the watermark or decrypt the image based on the secret key. The experiment proves that the method has good robustness and security when resisting moderate attacks. Since compressed sensing has unique advantages in dealing with multimedia big data, the research on the combination of watermarking and compressed sensing is of great significance to the comprehensive security protection of the confidentiality, integrity and availability of multimedia big data.

The combination of compressed sensing technology and watermarking has made outstanding contributions in the field of copyright protection [13] and information leakage prevention [14]. Xiao *et al.* [15] proposed an encrypted image digital watermarking algorithm based on compressed sensing and two-dimensional discrete wavelet transform. The method first performs two-dimensional discrete wavelet transform on the image to filter out important and unimportant parts. The important parts are divided into blocks, then, the blocks are marked, and the obtained sequence is used as the secert key of the watermark position, and the other parts are processed by other selected measurement matrices. Then, the watermark is embedded in the image according to the watermark position key, and the image is scrambled to improve the security of the image. The paper shows that when a small part of the watermark image is tampered, there will be errors in the extraction of the watermark. Though the method of embedding the watermark three times in this paper reduces the embedding capacity, it improved the robustness of the watermarking scheme. Literature [16] proposed a watermarking algorithm that directly embeds information into the measured values of compressed sensing of sparse signals. This algorithm is superior to the traditional l2 and l1 minimization algorithms in term of watermark embedding capacity. In addition, the combination [15], [16] of compressed sensing and watermarking [17], [18] can also be used for multimedia tampering identification and localization [19], [20]. Wang *et al.* [21] proposed a framework based on compressed sensing and secure multi-party computing protocol for solving the privacy issues in data storage and outsourcing. In the article, the author designed a cloud computing [22], [23] environment that requires watermark detection and protection of multimedia data storage work at the same time. The multimedia data and watermark are provided to the cloud, and the watermark detection is performed in the compressed sensing domain, which protects the privacy of the watermark. Music *et al.* [24] studied the watermark detection situation under different effective coefficient numbers under compressed sensing attacking. The watermark is obtained by wavelet transform, and the watermark is stored in a specific area of the image in the form of a random sequence. Then the compressed sensing is used to attack on watermarked images. Experimental results show that using less sparseness will not reduce the watermark detected results, but it will reduce the quality of image. In these studies, as the entropy of the compressed sensing domain tends to maximum, watermarking schemes generally face the problems such as difficulty in embedding, low capacity, and poor effect.

As a distributed network technology, blockchain has the characteristics of decentralization, traceability, transparency and non-tamperability. It has natural advantages in secure storage and information hiding. Blockchain technology is different from centralized management system. Each blockchain node has a complete ledger record. Therefore, the probability of that blockchain suffering catastrophic losses or failures, or successful hacker attacks is very small. In the existing researches on digital copyright of blockchain, Li Jingjing believed that blockchain can prevent digital copyright content from being lost and tampered, and digital copyright protection is subject to collective supervision, and the decentralization of blockchain can achieve truly by ''giving 'right' to the people'' [26]. Niu Min [27] compared the differences between centralized and decentralized copyright management models, and found the advantages of decentralized copyright management models. Meng *et al.* [25] proposed a copyright management system based on digital watermarking and blockchain, which used digital watermarking, blockchain, perceptual hash, quick response code and IPFS technologies. In the scheme, the traditional hash function and perceptual hash function are firstly used to calculate the hash value of the original image, and then the perceptual hash value of the image and the information of the

owner are packaged and uploaded to the blockchain, and the quick response code is used to generate watermark. Then, embedding the watermark into the image, and generating a watermarked image. The traditional hash function is used to calculate the hash value of the watermarked image. After that, uploading the watermarked image to the IPFS network. Thus, one can browse and download the watermarked image through IPFS. Compared with the traditional hash value of the original image, the self-authentication of the image can be realized. Although these works reflect the unique advantages of blockchain in copyright protection, there are still some problems as follows: 1. the privacy protection of files on blockchain is not considered. 2. The integrity and availability protection of the original information is not taken into account.

In response to the above problems, we propose a blockchain-watermarking scheme based on compressed sensing. The watermark is the combination of the feature watermark generated by the compressed sensing image features and the actual watermark provided by the copyright owner. The data of the blockchain-watermark is stored on IPFS, and the hash value returned by IPFS is uploaded to the blockchain. The innovations of our work are: 1. to the best of our knowledge, it is the first blockchain-watermarking scheme based on compressed sensing. 2. The problem of host image distortion caused by the watermark embedding is solved. 3. The distributed storage of watermarks is realized based on the blockchain, which effectively avoids the security problems of watermarks being attacked, stolen, and tampered.

The structure of this article is as follows. Section 2 introduces the related knowledge, including blockchain, compressed sensing and IPFS. The proposed scheme is described in Section 3. Section 4 introduces the experimental process. The conclusion is given in Section 5.

II. PRELIMINARY

A. BLOCKCHAIN

The concept of blockchain [35] first appeared in the paper ''Bitcoin: A Peer-to-Peer Electronic Cash System'' published by Satoshi Nakamoto [28]. Blockchain expounds the architectural concept of electronic cash system based on P2P network technology, encryption technology, timestamp technology, blockchain technology, etc. The blockchain is essentially a decentralized database, which includes data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [29]. The structure of blockchain is shown in Figure 1. The characteristics of blockchain are decentralization, openness, independence, security, and anonymity [30]. Among them, decentralization, security and anonymity have unique advantages in anti-tampering and privacy protection [31], [32]. Decentralization is the most prominent and essential feature of the blockchain [30], which means that the blockchain technology does not need to rely on additional trusted third-party institutions, and each node in the network stores all the transaction data in the entire network. Information is transferred between various nodes, and transactions in the network are verified. Each node in the blockchain does not know others, and transactions between nodes are open and transparent, preventing the risk of collusion and tampering. Blockchain obeys the majority rule. Only when at least fifty-one percent of the nodes in the network agree to tamper the data, can the data be tampered, but the price paid is huge. Another feature of blockchain is that the transactions packaged on the blockchain cannot be modified. The blockchain is composed of blocks connected one by one. Each block is packaged by transactions. Each block contains a block header and a block body. The block header contains the Block Version Number, Parent-Block Hash Value, Merkle Root Value, Timestamp Value, Difficulty Target Value and Nonce Value. The Parent-Block Hash Value refers to the hash value calculated by SHA-256 of the previous block of the current block, and the blocks are connected by the hash value of the Parent-Block to create a blockchain. The Timestamp Value provides a time reference for all nodes in the blockchain to form a temporal order. The block body is packaged by transactions. One of the features of hash algorithm is that even if the string is changed slightly, the hash value will change greatly. Therefore, once the transaction in the blockchain is tampered, the hash value will change. That is, the blockchain will not be connected by the hash value of the Parent-Blocks, which ensures that the data on the chain will not be tampered. Some features of the blockchain, such as the hash of the parent block, the timestamp, and the capability of tamper proof of packed transactions on the blockchain, are particularly suitable for privacy protection.

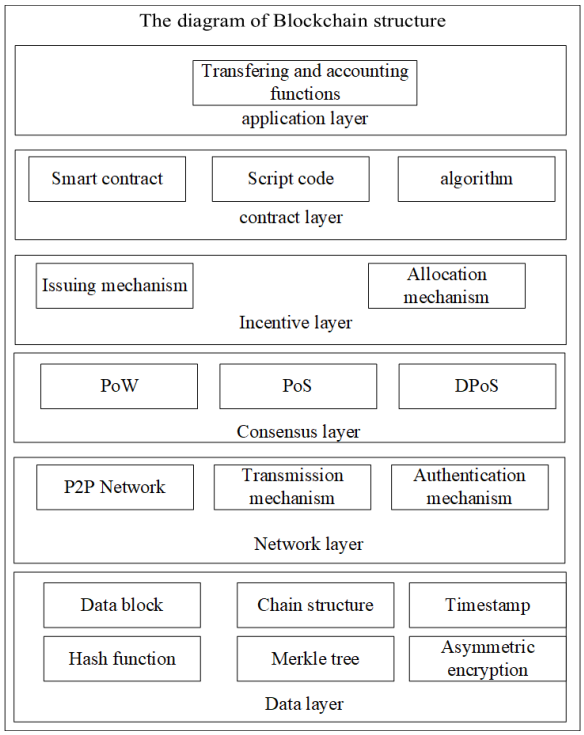

FIGURE 1. Blockchain structure diagram.

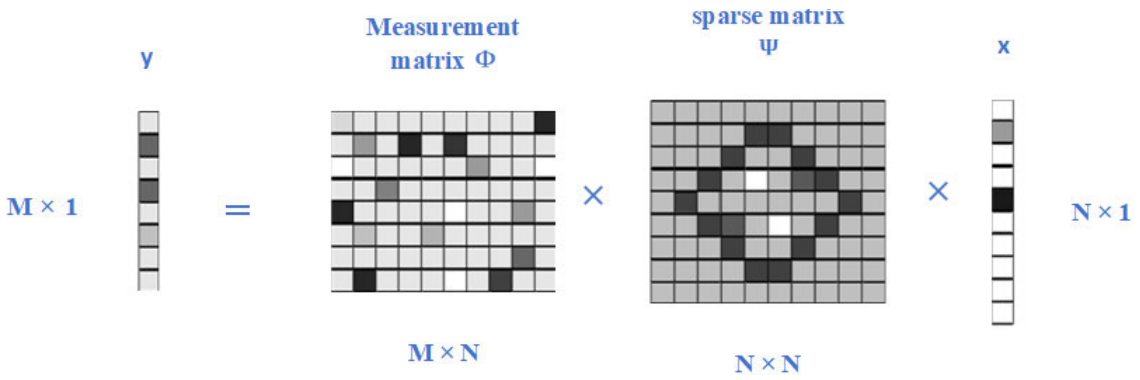

FIGURE 2. Principle diagram of compressed sensing.

B. COMPRESSED SENSING

Compressed sensing is a sampling method proposed by Candes, Rober, Donoho [1] and Tao, and it is widely used in signal processing. Compared with the traditional Nyquist sampling theorem, compressed sensing technology is superior. First of all, the traditional technology can only compress the signal after sampling; while compressed sensing can sampling while compressing. Secondly, if someone want to use the traditional Nyquist sampling method to accurately restore the original signal, the sampling frequency must be greater than twice the highest frequency of the original signal; but compressed sensing only requires a small amount of measurement values to restore the original signal. In addition, compressed sensing also reduces signal processing, storage, and transmission costs [33]. Compressed sensing can be regarded as an encryption scheme. Comparing with traditional encryption schemes, it has many advantages such as low computational cost of encryption process, simultaneous encryption and compression, and robustness of ciphertext. The basis of compressed sensing includes two aspects: one is the sparsity of the signal. The other is irrelevance. The sampling method of compressed sensing is to correlate the signal with another set of determined waveforms which are not related to the sparse space where the signal is located.

Supposing there is a finite-length one-dimensional discrete signal $x(x \in R^N)$, the length is N, the sparse basis vector is $\Psi_i(i = 1, 2, \ldots, N)$, and the original signal is sparsely transformed by:

$$x = \sum_{i=1}^{N} \alpha_i \Psi_i \quad \text{or } x = \alpha\Psi \tag{1}$$

The key factor of the compressed sensing technology is whether the signal is sparse. If the number of non-zero values is only $K(K \ll N)$ in (1), then the signal is sparse, that is, compressed sensing can be performed. The commonly used sparse bases in images are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) [1]. After confirming that the signal can be compressed sensed, it is necessary to design an $M \times N(M \ll N)$ dimensional measurement matrix that is not related to the transform base to measure the signal, and finally obtaining a measurement result y with the size of $M \times 1$. The N-dimensional signal is compressed into M-dimensional signals, realizing signal's compression. The signal can be reconstructed based on the measurement result y. The measurement matrices commonly used in compressed sensing mainly include random Gaussian matrix, Hadamard matrix, Binary Random matrix, Toeplitz matrix, etc. The principle of compressed sensing is shown in Figure 2, where x is the original signal with the length of $N \times 1$.

In the process of compression sampling, a sparse matrix with the size of $N \times N$ is first applied to the original signal x to sparse the original signal. Then, using the measurement matrix that is not related to the sparse basis and the sparse signal to obtain the observation result$y$ with a length of only $M \times 1$ dimensions, where $M \ll N$.

The measurement result can be obtained by the following formulas:

$$y = \Phi\Psi x = \Theta x \tag{2}$$

$$\Theta = \Phi\Psi \tag{3}$$

After the observed result is obtained, the original signal can be reconstructed.

The reconstruction algorithm selected in this paper is Orthogonal Matching Pursuit (OMP), and its algorithm steps are shown in Table 1, where, r_t represents the residual; t represents the number of iterations; $\varnothing$ represents the empty set; Λ_t represents the index set of the t-th iteration; λ_t represents the index found in the t-th iteration; α_j represents the j-th column of matrix A; A_t represents the column set of matrix A selected by index Λ_t; θ_t is the column vector with the size of $t \times 1$.

C. INTERPLANETARY FILE SYSTEM

The Interplanetary File System (IPFS) [34] is a network transmission protocol for distributing storage and sharing of files. As a point-to-point distributed file system, IPFS aims to connect all computing devices to the same file system. It has the following features: 1. content addressing. That is, all data stored in IPFS has a specific hash value, which is unique, and content can be searched through the hash value.

TABLE 1. OMP algorithm.

Input:
1.Sensor matrix $A = \Psi\Phi$ with the size of $M \times N$;
2.Observation vector y with the size of $N \times 1$;
3.Signal sparsity k.
Output:
1.Signal sparsity indicates coefficient estimation θ';
2.The residual $r_k = y - A_k\theta'_k$ with the size of $N \times 1$.
Process:
1. Initializing the $r_0 = y$, $\Lambda_0 = \varnothing$,$A_0 = \varnothing$,$t = 1$;
2. Finding the index λ_t, making the $\lambda_t = arg \max_{j=1,2,\ldots,N} |< r_{t-1}, \alpha >|$;
3.Let $\Lambda_t = \Lambda_{t-1} \cup \{\lambda_t\}$, $A_t = A_{t-1} \cup \alpha$;
4.Finding the least squares solution of the $y = A_t\theta_t, \theta'_t = arg \min_{\theta'_t} \| y - A_t\theta_t \| = (A_t^T A_t)^{-1} A_t^T y$;
5.Updating residual $r_t = y - A_t\theta'_t = y - A_t(A_t^T A)^{-1} A_t^T y$;
6.$t = t + 1$, if t $\leq$ K,then return to step 2, otherwise, stoping the iteration and go to step 7;
7.The reconstructed θ' has a non-zero term at Λ_t , and its value is the θ'_t that obtained in the last iteration.

2. Tamper-proof. The tampering of data in IPFS can be detected. 3. Elimination of redundancy. The same files in the IPFS network will only be stored once, saving storage space. In the IPFS network, we can download files based on the unique hash value generated by the uploaded file.

III. THE PROPOSED METHOD

The overall processing of the proposed method is shown in Figure 3. We firstly perform compressed sensing on the original image to obtain a compressed and encrypted image. Then, generate a feature watermark based on the encrypted image after the compressed sensing process, and combine the feature watermark with the actual watermark to generate the blockchain watermark, which is uploaded to the IPFS network. IPFS will return a string of hash values, and the hash values are stored on the blockchain to realize watermarking. The storage structure of the blockchain can realize the safe storage of uploading data [38]–[40], preventing the leakage of information and the occurrence of infringement incidents, and realize tamper proof of the compressive sensed images.

A. GENERATION AND UPLOADING OF THE WATERMARK

First, the image is processed by compressed sensing. Then, the compressed and encrypted image is divided into blocks,

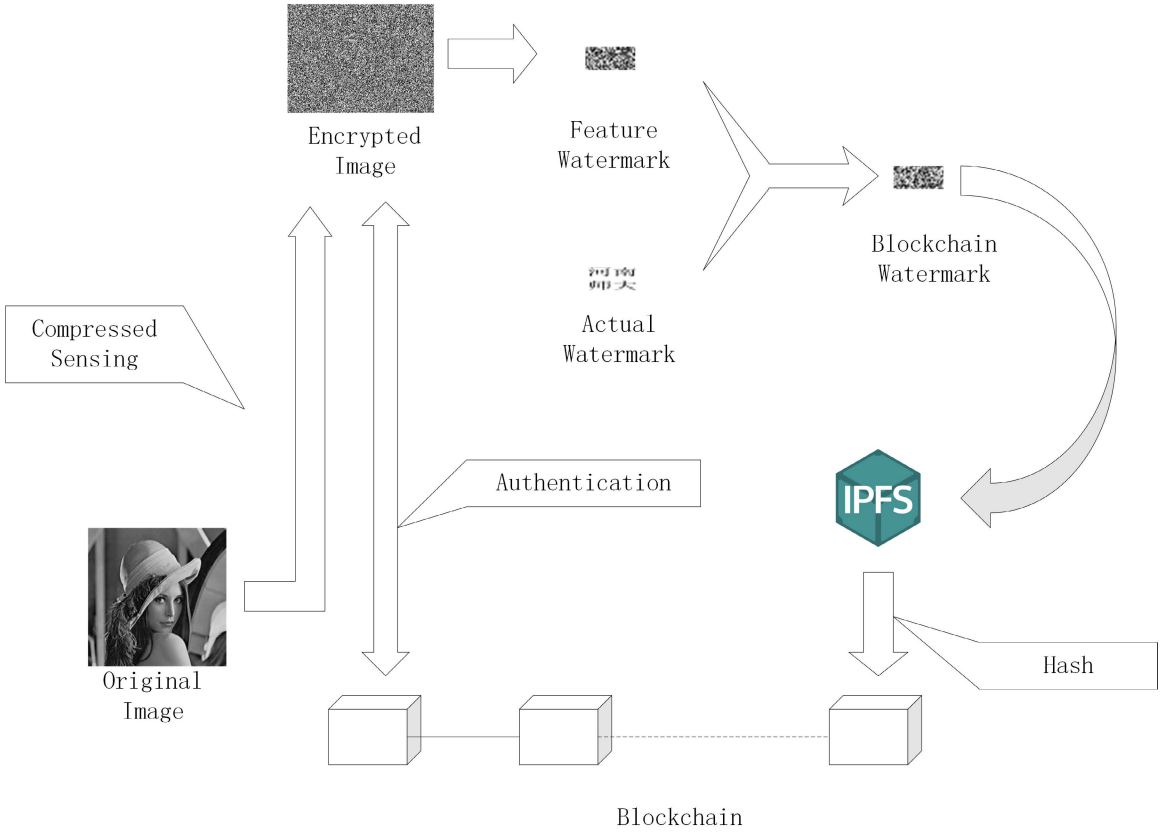

FIGURE 3. Schematic diagram of the process.

and the feature values are extracted from each block to generate a feature watermark. Designing an actual watermark with the same size as the feature watermark, and combining the actual watermark with the feature watermark to obtain the blockchain-watermark. In order to reduce the space complexity of the blockchain watermarks, the generated watermark is first uploaded to IPFS. IPFS will return a string of hash values, and then uploading the hash values to the blockchain. The steps are as follows:

1. Compressed sensing: Performing wavelet transform on the original image to make it sparse, and then perform compressed sensing on the sparse image to obtain the compressed and encrypted image.

2. Block division: Dividing the encrypted image into un-overlapping blocks with the size of 8×8.

3. Feature watermark generation: Converting each block into a 1×64 row vector. Then, using a chaotic sequence to randomly generate a 64×1 column vector. Multiplying the row vector and the column vector to obtain a random feature value of each block. Obtaining a feature matrix of each block's eigenvalues. The feature watermark is generated directly from the feature matrix.

4. Actual watermark generation: Designing and generating an actual watermark by the copyright owner. The size of the feature watermark is the same as that of the actual watermark.

5. Blockchain watermark generation: Combining the actual watermark with the feature watermark to generate a blockchain watermark.

6. IPFS uploading: Uploading the blockchain watermark to IPFS and returning a string of hash values.

7. Blockchain uploading: Uploading the returned hash value to the blockchain to protect the information in the ciphertext state.

B. EXTRACTION AND DETECTION OF THE WATERMARK

By a smart contract, the file is uploaded to the blockchain, and a string of hash values will be generated. The hash value is the contract address of the transaction. When extracting files in the blockchain, entering the contract address to find the corresponding contract, and downloading the uploaded blockchain watermark from the IPFS network through the hash value of the uploaded file stored in the contract. The actual watermark can be obtained by combining the blockchain watermark and the feature watermark computed from the compressed and encrypted image. The integrity and availability of the compressive sensed image are tested by comparing the extracted actual watermark and the original actual watermark. The steps of the extraction and detection methods are as follows:

1. Hash value extraction: Finding the corresponding contract through the contract address generated by the transaction, and finding the hash value generated by uploading the file in the contract file.

2. Blockchain watermark downloading: Downloading the blockchain watermark file in the IPFS network through the hash value stored in the contract file.

3. Actual watermark extraction: Combining the downloaded blockchain watermark and the feature watermark obtained from the compressive sensed image to form the actual watermark.

4. Tamper detection: Comparing the obtained actual watermark with the original actual watermark, the tampered area can be found.

IV. EXPERIMENTS

A. PROOF OF VALIDITY

1) BLOCKCHAIN WATERMARK GENERATION

The original image selected in this experiment is shown in Figure 4(a), which is a two-dimensional grayscale image with a size of 256×256. First, performing wavelet transform on the image to make it sparse and generating the wavelet transform matrix. Then, we design a random measurement matrix R that is not related to the wavelet transform matrix, and its size is 120×256,the sampling rate is 46.87 percent. Then, the compressed and encrypted image can be obtained according to formula (4).

$$y = R \times X1 \tag{4}$$

Distributing the compressed matrix values between $0 \sim 255$ uniformly, the obtained encrypted image is shown in Figure 4(b), the size of which is 120×256. The compressed image is divided into blocks, and each block is a matrix with a size of 8×8. The feature value is extracted from each block to generate the feature watermark. In extraction, each block is converted into a 1×64 row vector, and the chaotic sequence is then used to randomly generate a 64×1 column vector. Multiplying the row vector and the column vector to get a random number as the feature value. Calculating the eigenvalues of each block in turn, and finally get a feature matrix $C1$. The feature watermark is generated from the feature matrix, as shown in Figure 4(c). The actual watermark is shown in Figure 4(d). This actual watermark is combined with the feature watermark to obtain the blockchain watermark, as shown in Figure 4(e). The extracted actual watermark Figure 4 (f) can be obtained by performing XOR operation between Figure 4 (e) and (c). The experimental results show that the extracted watermark is consistent with the actual watermark. Since blockchain watermark is obtained by combining feature watermark and actual watermark, and the feature watermark is a liner operation based on the size of the image, the time complexity of blockchain watermarking is $O(m \times n)$, $m \times n$ is the size of the encrypted image. In the proposed scheme,the experimental equipment we used was Lenovo, i7-8700, 8G, and 240G SSD. The encrypted image is generated by performing compressed sensing on the original image, the elapsed time is 0.235 seconds. Dividing the encrypted image into blocks, for each block, a feature value is generated and generating a feature watermark, which takes 0.183 seconds. And the elapsed time is 0.000007 seconds to generate a blockchain watermark by combining feature watermark and actual watermark. The elapsed time is also negligible when uploading blockchain watermark to IPFS

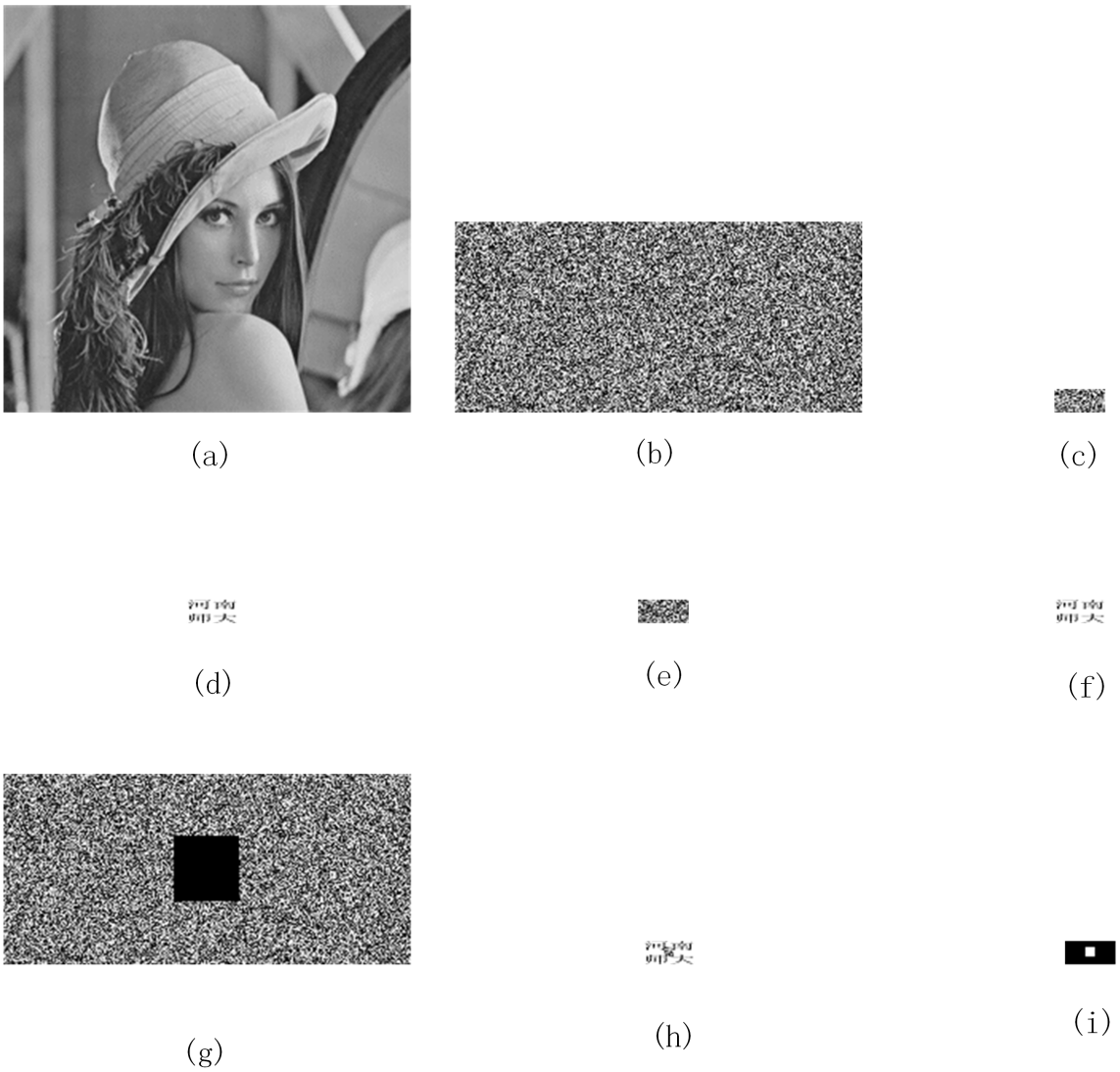

FIGURE 4. Experimental results. (a). The original image; (b). the encrypted image; (c). the feature watermark; (d). the actual watermark; (e). the blockchain-watermark; (f). the actual watermark extracted from (b); (g). the tampered encrypted image; (h). the actual watermark extracted from (g); (i). the Tampered area in encrypted image.

network and blockchain, but gas is consumed in the process of uploading to blockchain. In our scheme, the elapsed time is little, and the image will not be distributed if the watermarking process is not complete.

2) BLOCKCHAIN WATERMARKING

The example of blockchain watermarking algorithm is given in Table 2. The first step in Table 2 is to upload the blockchain watermark to the IPFS network, the IPFS network returns a string of unique hash value; the second step is to upload the hash value to the blockchain by writing a smart contract. And the information generated during the uploading process including the File Name, the Hash value returned by the IPFS network, Transaction Hash, uploaded account address, Execution and Transaction cost and so on. The watermark on blockchain is well protected and cannot be modified. After watermark extraction from the blockchain, the blockchain watermark and the feature watermark are combined to obtain the extracted actual watermark as shown in Figure 4(f). It can be seen that the extracted watermark is the same as the original actual watermark.

3) TAMPER DETECTION

When the compressive sensed image is illegally tampered, the blockchain watermark can be used to detect and locate the tampered area. Since the watermark is obtained by image block processing, each watermark bit corresponds to the corresponding position of the blocks of the compressive sensed image. The test results are also shown in Figure 4. When the compressed and encrypted image is tampered as shown in Figure 4(g), where the black area denotes the tampered area, the extracted actual watermark is shown as Figure 4(h).

TABLE 2. The upload process and transaction information.

Process	*Information*
1.Uploading the blockchain watermark to IPFS, and a string of hash value will be returned.	'Name': 'blockchain watermark.png'; 'Hash': 'QmdABkC8MTRQwLshDf6a3VwmU1bmBJ25t8fSBipn7ioDxB' 'size': '593'
2. Uploading the hash value to the blockchain by writing a smart contract.	Status: 0x1 Transaction mined and execution succeed Transaction Hash:0xe0f915b420d75441aa37577f1c788d1228ba21695694a209016450182274a051 From:0x5B38Da6a701c568545DcfcB03FcB875f56beddC4 To: water.uploads(string) 0xd9145CCE52D386f254917e481Eb44e9943F39138 Gas: 3000000 gas Transaction cost: 86653 gas Execution cost: 61797 gas hash:0xe0f915b420d75441aa37577f1c788d1228ba21695694a209016450182274a051; input: 0x94e. . . 00000; decoded input:{"string temp": " QmSD3HYvRwTcXB5Xea4pNNo2vqyhG6rqHQNfRqYGU8wrsm"} decoded output:{} logs: [] value: 0wei

TABLE 3. Comparison with other schemes.

Scheme	*Encrypted domain*	*Compressed sensing*	*IPFS*	*Temper detection*	*Temper localization*	*Modification on host media*	*External security*	*Third-party*
Our scheme	Y	Y	Y	Y	Y	Out	Y	N
[11]	Y	N	N	N	N	In	N	Y
[10]	N	N	N	N	N	In	N	Y
[17]	N	N	N	Y	Y	In	N	Y
[18]	N	N	N	Y	Y	In	N	Y
[19]	N	Y	N	Y	Y	In	N	Y
[20]	N	Y	N	Y	Y	In	N	Y
[4]	Y	Y	N	N	N	In	N	Y
[5]	Y	Y	N	N	N	In	N	Y
[25]	N	N	Y	N	N	Out	Y	N
[31]	Y	N	N	N	N	Out	Y	N
[32]	Y	N	N	N	N	Out	Y	N

By comparing Figure 4(h) and the original actual watermark Figure 4(d), the tampered area can be deduced, as shown in Figure 4(i), the tampered area Figure 4 (i) can be obtained by performing XOR operation between Figure 4 (d) and (h). It can be seen that the deduced tampered area in Figure 4(i) is nearly the same as the original tampered area in Figure 4(g), indicating that the tampered area can be detected and located through the watermark. The main characteristic of the proposed scheme is fragility. However, the robustness is also equipped to some extent since the text in the actual watermark extracted from the tampered encrypted image can be recognized, as shown in Figure 4 (h).

The image watermark capacity refers to the maximum amount of information that can be hidden in the host image. In the proposed scheme, we did not embed the watermark in the host image. We performing compressed sensing and block processing on the original image (256×256) to generate a feature watermark with the size of 15×32, then combining it with the actual watermark and finally generate a blockchain watermark with the same size. So the actual watermark capacity that can be accommodated is also 15×32.

B. COMPARISON

The method proposed in this paper is compared with other similar methods, as shown in Table 3. The evaluation indicators mainly including encrypted domain, compressed sensing, IPFS, tamper detection, tamper localization, Modification on host media, external security, and third-party. Among them, external security refers to the fact that whether it will be attacked outside; third-party participation refers to the need of participation of third-party's servers. According to Table 3, it can be seen that in the schemes without the need of participation of a third-party, only the proposed method can realize tamper detection and localization, and only our scheme can process compressive sensed signal. Similarly, in the schemes which processed in the encrypted domain, only the proposed scheme can perform tamper detection and localization.

TABLE 4. Performance comparison with other solutions.

Scheme	*PSNR*	*BER*	*SSIM*	*NC*
Our scheme	∞	0	1	1
[36]	55.34	0	0.9999	0.9121
[37]	59.24	0	0.9999	Inadequate

In order to assess the distortion caused by watermark embedding, we have compared the quality of watermarked image with other state-of-the-art schemes [36], [37] in terms of peak signal-to-noise ratio (PSNR), bit error rate (BER), structural similarity (SSIM) and normalized correlation

TABLE 5. Performance comparison with other schemes.

Scheme	dimension of water-mark/signature	transaction cost	complexity	tampering localization performance	resistance to non-malicious operations	detection of malicious operation
Our scheme	2	Low	$O(m \times n)$	Good	brightness adjustment (<0.4), contrast adjustment (<1.002)	crop, copy-past, geometry transfor-mation, etc.
[38]	1	Normal	$O(m \times n)$	N/A	N/A	crop, copy-past, geometry transfor-mation, etc.
[39]	1	Normal	$O(p \times T)$	N/A	N/A	crop, copy-past, geometry transfor-mation, etc.

coefficient (NC) according formulas (5-9).

$$PSNR(f, f_w) = 10log_{10}\frac{255^2}{MSE} \tag{5}$$

$$MSE = \frac{1}{N^2}(\sum_{i=1}^{N}\sum_{j=1}^{N}[f_w(i,j) - f(i,j)]^2) \tag{6}$$

$$BER = \frac{B_{error}}{l} \tag{7}$$

$$SSIM(f, f_w) = \frac{\sigma_{ffw} + C1}{\sigma_f \sigma_{fw} + C1} \tag{8}$$

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}[W(i,j)xw''(i,j)]}{\sum_{i=1}^{N}\sum_{j=1}^{N}[W(i,j)]^2} \tag{9}$$

where, f is the original ciphertext image, f_w is the ciphertext image that the blockchain watermarking is generated; σ_f and σ_{fw} are the standard variance of f and f_w; σ_{ffw} is the covariance between f and f_w; and $C1$ is a constant; l denotes the dimensions of the watermark image; B_{error} refers to the number of incorrectly extracted bits; W is the original watermark. w'' is the extracted watermark.

The comparison results are shown in Table 4. It can be found that our scheme has the highest image quality in every index, which is because the watermark is embedded on the blockchain rather than the image using the proposed method, and the distortion of the host image can be totally avoided.

In order to show the performance of our scheme, we compare our scheme with other schemes in terms of the dimension of the watermark/signature, the transaction cost, the complexity, the tampering localization performance, resistance to non-malicious operations and detection of malicious operation. The comparison results are shown in Table 5, where $m \times n$ represents the size of the image, and in paper [39], p is the number of divided blocks of user image's sensing data, T is the entire cycle. It can be seen from Table 5 that our scheme has lower transaction cost and good tampering localization performance. In terms of non-malicious operation, only our solution can resist slightly brightness (<0.4) and contrast (<1.002) adjustments, which is mainly due to the robustness of compressive sensing. In contrast, the hash value or signature in papers [38], [39] is sensitive to any non-malicious operation performed on the original image. In terms of malicious operation, a variety of attacks including crop, copy-past, geometry transformation, etc., can be detected successfully by all the compared schemes.

C. SECURITY ANALYSIS

1) IMAGE TAMPER-PROOF

The image tamper-proof is relied on the watermark. The tampered area can be deduced from the extracted actual watermark, as shown in Figure 4 (h), and it can be clearly seen from the XOR result that shown in Figure 4 (i). If the image is precious and any modification is not allowed, the appearance of tampered area denotes that the image is not usable anymore. If some distortion of the image is allowed, one can judge the usability of the image by observing the extent of modification on the watermark.

2) WATERMARK TAMPER-PROOF

The watermark which is vital to the image security is well protected by the technologies of blockchain and IPFS. The blockchain watermark is first uploaded to the IPFS network, then a string of specific hash value returned by the IPFS network is uploaded to the blockchain. Since both IPFS and blockchain are distributed storage, IPFS has the characteristics of content addressing and tamper-proof, that is, all data in the IPFS network has a specific and unique hash value, and the content can be searched through the hash value.And when the data in the IPFS network is tampered, IPFS can detect and prompt. The characteristics of blockchain are decentralization and security, the blockchain technology does not need to rely on additional trusted third-party institutions, and each node in the network stores all the transaction data in the entire network. Blockchain obeys the majority rule. Only when at least 51% of the nodes in the network agree to tamper the data, can the data be tampered, but the price paid is huge. The features of the IPFS network and blockchain ensure the safety of uploaded data.

V. CONCLUSION

This study proposed a novel watermarking scheme, which combines the compressed sensing and blockchain technologies, to protect the privacy, the integrity and the availability of the image big data simultaneously. The security of the watermark is ensured by the blockchain. The original content of images is concealed by compressive sensing, and the watermarking is processed in the encrypted domain. The tampered area on the compressive sensed images can be detected and located by the blockchain watermark. Experiments and analysis show that the proposed method is effective and feasible, and the performance is superior to other state of the art works.

REFERENCES

[1] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[2] W. Xue, C. Luo, R. Rana, W. Hu, and A. Seneviratne, "CScrypt: A compressive-sensing-based encryption engine for the Internet of Things: Demo abstract," in *Proc. 14th ACM Conf. Embedded Netw. Sensor Syst. (CD-ROM)*, Nov. 2016, pp. 286–287.
[3] Y. Zhang, P. Wang, L. Fang, X. He, H. Han, and B. Chen, "Secure transmission of compressed sampling data using edge clouds," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6641–6651, Oct. 2020.
[4] B. Zhang, D. Xiao, Z. Zhang, and L. Yang, "Compressing encrypted images by using 2D compressed sensing," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun.; IEEE 17th Int. Conf. Smart City; IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Zhangjiajie, China, Aug. 2019, pp. 1914–1919.
[5] G. Zhang, S. Jiao, and X. Xu, "Application of compressed sensing for secure image coding," in *Proc. Int. Conf. Wireless Algorithms, Syetems, Appl. (WASA)*. Berlin, Germany: Springer, 2010, pp. 220–224.
[6] Y. Zhang, Q. He, G. Chen, X. Zhang, and Y. Xiang, "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7566–7578, Dec. 2020.
[7] D. Xiao, M. Deng, and Y. Zhang, "Robust and separable watermarking algorithm in image based on compressive sensing," *J. Electron. Inf. Technol.*, vol. 37, no. 5, pp. 1248–1254, 2015.
[8] L. Y. Xiang, Y. Li, W. Hao, P. Yang, and X. B. Shen, "Reversible natural language watermarking using synonym substitution and arithmetic coding," *Comput. Mater. Continua*, vol. 55, no. 3, pp. 541–559, 2018.
[9] C. Yang, X. Luo, J. Lu, and F. Liu, "Extracting hidden messages of MLSB steganography based on optimal stego subset," *Sci. China Inf. Sci.*, vol. 61, no. 11, pp. 237–239, Nov. 2018.
[10] N. Tarhouni, M. Charfeddine, and C. Ben Amar, "Novel and robust image watermarking for copyright protection and integrity control," *Circuits, Syst., Signal Process.*, vol. 39, no. 10, pp. 5059–5103, Oct. 2020.
[11] S. Liu, B. M. Hennelly, C. Guo, and J. T. Sheridan, "Robustness of double random phase encoding spread-space spread-spectrum watermarking technique," *Signal Process.*, vol. 109, pp. 345–361, Apr. 2015.
[12] L. Jiang, Z. Xu, and Y. Xu, "Commutative encryption and watermarking based on orthogonal decomposition," *Multimedia Tools Appl.*, vol. 70, no. 3, pp. 1617–1635, 2014.
[13] H. Huang and F. Chang, "Robust image watermarking based on compressed sensing techniques," *J. Inf. Hiding Multimedia Signal Process.*, vol. 5, no. 2, pp. 275–285, Apr. 2014.
[14] T.-S. Chen, K.-N. Hou, W.-K. Beh, and A.-Y. Wu, "Low-complexity compressed-sensing-based watermark cryptosystem and circuits implementation for wireless sensor networks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 11, pp. 2485–2497, Nov. 2019.
[15] D. Xiao, Y. Chang, T. Xiang, and S. Bai, "A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9265–9296, Apr. 2017.
[16] M. Yamac, C. Dikici, and B. Sankur, "Robust watermarking of compressive sensed signals," in *Proc. 21st Signal Process. Commun. Appl. Conf. (SIU)*, Haspolat, Turkey, Apr. 2013, pp. 1–4.
[17] M. Fan and H. Wang, "An enhanced fragile watermarking scheme to digital image protection and self-recovery," *Signal Process., Image Commun.*, vol. 66, pp. 19–29, Aug. 2018.
[18] C. Qin, P. Ji, X. Zhang, J. Dong, and J. Wang, "Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy," *Signal Process.*, vol. 138, pp. 280–293, Sep. 2017.
[19] G. Valenzise, M. Tagliasacchi, S. Tubaro, G. Cancelli, and M. Barni, "A compressive-sensing based watermarking scheme for sparse image tampering identification," in *Proc. 16th IEEE Int. Conf. Image Process. (ICIP)*, Cairo, Egypt, Nov. 2009, pp. 1265–1268.
[20] W. Lu, Z. Chen, L. Li, X. Cao, J. Wei, N. Xiong, J. Li, and J. Dang, "Watermarking based on compressive sensing for digital speech detection and recovery," *Sensors*, vol. 18, no. 7, p. 2390, Jul. 2018.
[21] Q. Wang, W. Zeng, and J. Tian, "A compressive sensing based secure watermark detection and privacy preserving storage framework," *IEEE Trans. Image Process.*, vol. 23, no. 3, pp. 1317–1328, Mar. 2014.
[22] Y. Zhang, X. Xiao, L.-X. Yang, Y. Xiang, and S. Zhong, "Secure and efficient outsourcing of PCA-based face recognition," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1683–1695, Oct. 2020.
[23] Y. Zhang, H. Huang, L.-X. Yang, Y. Xiang, and M. Li, "Serious challenges and potential solutions for the industrial Internet of Things with edge intelligence," *IEEE Netw.*, vol. 33, no. 5, pp. 41–45, Sep. 2019.
[24] J. Music, I. Knezevic, and E. Franca, "Wavelet based watermarking approach in the compressive sensing scenario," in *Proc. 4th Medit. Conf. Embedded Comput. (MECO)*, Budva, Montenegro, Jun. 2015, pp. 315–318.
[25] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, Jul. 2018, pp. 359–364.
[26] J. Li and Z. Wang, "Digital copyright protection promoted by blockchain technology," *Youth Journalist*, no. 10, pp. 25–28, 2017.
[27] M. Niu, "Research on the management mode of digital copyright protection based on blockchain," M.S. thesis, Dept. Technol., BIGC, Beijing, China, 2017.
[28] S. Nakamoto. (2009). *Bitcoin: A Peer-to-peer Electronic Cash System*. [Online]. Available: https//bitcoin.org.bitcoin.pdf
[29] Q. Zhu, S. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Application of distributed ledger technologies to the Internet of Things: A survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–34, Nov. 2019.
[30] C. Xu and X. Li, "Data privacy protection method of block chain transaction," *Comput. Sci.*, vol. 47, no. 3, pp. 281–286, Mar. 2020.
[31] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," *Entropy*, vol. 22, no. 2, p. 175, Feb. 2020.
[32] N. Wang, Y. Chen, Y. Yang, Z. Fang, and Y. Sun, "Blockchain private key storage algorithm based on image information hinding," in *Proc. Int. Conf. Artif. Intell. Secur. (ICAIS)*, 2019, pp. 542–552.
[33] J. Zhao, "Research on image information hiding scheme based on compressed sensing," M.S. thesis, Dept. Technol., CQU, Chongqing, China, 2018.
[34] J. Benet, "IPFS-content addressed, versioned, P2P file system," Jul. 2014, *arXiv:1407.3561*. [Online]. Available: https://arxiv.org/abs/1407.3561
[35] E. Zhang, M. Li, S.-M. Yiu, J. Du, J.-Z. Zhu, and G.-G. Jin, "Fair hierarchical secret sharing scheme based on smart contract," *Inf. Sci.*, vol. 546, pp. 166–176, Feb. 2021.
[36] K. M. Hosny and M. M. Darwish, "Resilient color image watermarking using accurate quaternion radial substituted Chebyshev moments," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 2, pp. 1–25, Jun. 2019.
[37] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invariant quaternion Legendre-Fourier moments," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24727–24750, Oct. 2018.
[38] P. W. Khan and Y. Byun, "Blockchain-based secure image encryption scheme for the industrial Internet of Things," *Entropy*, vol. 22, no. 2, p. 175, 2020.
[39] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the Internet of Things," *Sensors*, vol. 20, no. 3, p. 916, 2020.
[40] R. A. Dobre, R. O. Preda, C. C. Oprea, and I. Pirnog, "Authentication of JPEG images on the blockchain," in *Proc. Int. Conf. Control, Artif. Intell., Robot. Optim. (ICCAIRO)*, Prague, Czech Republic, May 2018, pp. 211–255.

MING LI received the master's degree in science from the College of Physics and Information Engineering, Henan Normal University, Henan, China, in 2010, and the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. He is currently an Associate Professor with the College of Computer and Information Engineering, Henan Normal University. His research interests include multimedia security, information hiding, and compressive sensing.

LEILEI ZENG received the B.S. degree from the Department of Computer and Information Engineering, Henan Normal University, Xinxiang, China, in 2019, where he is currently pursuing the M.S. degree in computer science and technology. His research interests include multimedia security and information hiding.

LE ZHAO received the B.S. degree from the Department of Computer and Information Engineering, Henan Normal University, Xinxiang, China, in 2019, where she is currently pursuing the M.S. degree in computer science and technology. Her research interest includes privacy protection for machine learning.

RENLIN YANG received the B.S. degree from the Department of Computer and Information Engineering, Henan Normal University, Xinxiang, China, in 2019, where he is currently pursuing the M.S. degree in computer science and technology. His research interests include secret sharing and private set intersection.

DEZHI AN is currently a Professor with the School of Cyber Security, Gansu University of Political Science and Law, Lanzhou, China. His research interests include network security, public opinion analysis, and data mining.

HAIJU FAN received the master's degree in science from the College of Electronic Information Engineering, Beihang University, Beijing, China, in 2005, and the Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2017. She is currently an Associate Professor with the College of Computer and Information Engineering, Henan Normal University. Her research interests include multimedia security, information hiding, and compressive sensing.