Hindawi
Security and Communication Networks
Volume 2021, Article ID 6493306, 16 pages
https://doi.org/10.1155/2021/6493306

Research Article

A Novel Video Copyright Protection Scheme Based on Blockchain and Double Watermarking

Jingjing Zheng,[1] **Shuhua Teng**,[2,3] **Peirong Li**,[4] **Wei Ou**,[4] **Donghao Zhou**,[5] **and Jun Ye**[4]

[1]*School of Computer Science and Technology, Hainan University, Haikou 570228, Hainan, China*
[2]*Hunan Communications Research Institute Co., LTD., Changsha 410015, Hunan, China*
[3]*School of Information Science and Engineering, Hunan First Normal University, Changsha 410205, Hunan, China*
[4]*School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, Hainan, China*
[5]*School of Computer, National University of Defense Technology, Changsha 410073, Hunan, China*

Correspondence should be addressed to Wei Ou; ouwei@hainanu.edu.cn

Received 13 September 2021; Revised 17 October 2021; Accepted 11 November 2021; Published 13 December 2021

Academic Editor: Honghao Gao

With the continuous development of multimedia, more and more digital works such as videos are spread, stored, and used in the network. In recent years, digital copyright infringement disputes have occurred frequently. The traditional copyright protection system has some problems, such as difficulty confirming copyright, monitoring infringement, and obtaining evidence for rights protection. To this end, we have designed and implemented a novel video copyright protection scheme based on the blockchain and double watermarking technology. We use the image correlation coefficient method to extract video keyframes. And we combine with Contourlet Transform domain, QR decomposition, and SIFT algorithm to improve the robustness of watermark against geometric attacks on the premise of invisibility. After that, we use Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation to encrypt the robust watermark and strengthen the security. Moreover, based on the characteristics of the fragile watermarking, we accurately locate the attacked video's tamper position and complete the integrity authentication of the watermarked video. In addition, the hash digest of the video watermark and the user ID of the copyright owner is signed by SM2 and uploaded to the blockchain. The user can register the copyright after passing the identity authentication. We conduct tests and security analysis on the blockchain performance of the system, the performance of the commercial cryptography algorithm, and the security of the watermarking system. The experimental results show that the blockchain used in this system conforms to the industry standard, the performance of SM2 and SM3 is better than ECC-256 and SHA-256, and the system security is well guaranteed.

1. Introduction

With the advent of the Internet era, the new media industry is growing at high speed worldwide [1], resulting from the integration of network technology and cultural industry. The number of video resources that people are exposed to in their daily life is rapidly expanding. And the number of online video users in China is gradually increasing in proportion to the total number of netizens. As of June 2019, the number of online video users had reached 759 million [2]. In the case of China, the short video industry, such as Tik Tok, Kuaishou, and other platforms, currently has more than 600 million active users and a market volume of more than 10 billion CNY [3]. The official data survey on video infringement cases shows the severe and rampant infringement phenomenon behind the prosperous video industry in China. From January 2019 to October 2020, the 12426 Copyright Monitoring Centre monitored more than 100,000 original short video authors, the National Copyright Administration's early warning list, short video clips of key film, and other works. The number of works covered exceeded 10 million, and a total of 30,095,200 suspected infringing short videos were monitored, which involved up to 2.72 trillion clicks.

The frequent occurrence of video copyright infringement is also related to the characteristics of the video, such as easy modification and hard distinguishment. A large amount of video information is exchanged and transmitted on the network [4, 5], and the video can be easily modified by various means [6], such as interception, copy, tamper, and redistribution [7]. Pirated video resources can be found everywhere on the Internet. It is difficult to distinguish the authenticity of video information, and there are many disputes over copyright issues [8]. The commercialization of the video business is severely hampered, resulting in severe economic damage [9]. The Internet brings not only opportunities to the field of video works but also the problem of industry copyright disorder. This problem is the challenge in this field. If it cannot be solved in time, it will be a significant obstacle for the development of China's online video works copyright industry [10]. Copyright protection in the field of video has become a matter of urgency and cannot be delayed.

Along with the acceleration of technology application and innovation in the emerging markets of intellectual property rights (IPR) capitalization, a large number of international investment treaties have included IPRs in the scope of investment [11–13]. China's policies related to IPR protection have also continued to increase. IPR has been mentioned many times in the document "Outline of the 14th Five-Year Plan and 2035 Vision for National Economic and Social Development of the People's Republic of China." China is actively promoting digital industrialization and industrial digitization, and the digital economy has become a new variable to improve the quality and efficiency of the Chinese economy [14, 15].

Traditional video digital watermarking technology has the following problems [16–18]: Firstly, the algorithm's robustness is poor. The vector of the video watermarking algorithm is video. For video attacks, in addition to image attacks, there are also frame average, frame deletion, frame reassembly, and other attacks. Therefore, for video watermarking technology, it is required to resist the attacks mentioned above. Moreover, the robustness of geometric attacks, compression attacks, and other attacks still needs to be improved. Secondly, the balance of the video watermarking scheme is poor. Video single watermarking algorithm is mutually constrained in terms of robustness and vulnerability. The robust watermarking ensures that the watermark information confirming the copyright can still be extracted after the video is attacked. The fragile watermarking can locate and quantify the tampered location when tampering is detected. Furthermore, the single watermarking systems often cannot balance robustness and vulnerability. Thirdly, traditional digital copyright protection systems use centralized central databases. So, the security of data is easily threatened. Nowadays, with the rapid development of the Internet, there are more and more copyright protection issues. And the centralized databases are no longer meet the growing demand for copyright protection on the Internet. Fourthly, the watermark is poorly associated with its owner. In order to protect their IPR, individuals or groups often embed the watermark of relevant information with certainty and confidentiality into the resources they want to protect. However, when their watermarks are not notarized by trusted third-party certification bodies, the relationship between them and individuals or groups cannot be guaranteed, which leads to the watermark's poor relevance to the owner. Usually, the authentication steps of third-party certification bodies are tedious and costly.

Given the above problems, we propose and implement a video copyright protection system based on the blockchain and double watermarking technology. We are committed to protecting video copyright and solving traceability and other needs. The system makes use of SM2 to sign the digest of robust watermark and user ID and then uploads the signature to the blockchain platform. The consensus mechanism of the blockchain can effectively guarantee the authenticity of the data. During the uploading procedure, we also verify the user's identity to confirm that the user is who he claims to be. The combination of Contourlet Transform domain, QR decomposition, and SIFT algorithm makes the robust watermark improve the robustness against geometric attacks under the premise of invisibility. The watermark is encrypted by using Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation and pinpoints the location of the tampered location by using the fragile watermarking.

2. Background

Due to the increasing number of disputes caused by video copyright issues, people's awareness of video copyright protection is growing, and the demand for video copyright protection has become intense. Digital watermarking technology has emerged. In 1993, Tirkel et al. first proposed the expression "watermark." In 1994, Tirkel et al. [19] proposed "a digital watermark," detailed the definition of digital watermarking, and described the application areas of digital watermarking. As a result, many famous universities and institutions at home and abroad have started to devote themselves to the research of digital watermarking technology, and the research results are widely used in real life. Video digital watermarking technology can be mainly divided into video watermarking based on the spatial domain (pixel domain) and video watermarking based on the transform domain [20]. Most video watermarking based on spatial domain has poor robustness, such as the LSB algorithm, which embeds the watermark in the least significant bit of data [21]. It is easy to be removed and challenging to resist attacks. The transform domain-based video watermarking technology can transform the spatial domain to the transform domain, perform image operations on the transform domain, and finally inverse transform to the spatial domain. The above operations can spread the transform to each pixel point in the spatial domain to enhance the robustness.

Currently, the ordinary and practical watermarking algorithms embed the watermark in the transform domain, such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and other methods. However, the two-dimensional wavelet has limited directionality and cannot represent image contours and edge information in the most efficient sparse form. The Contourlet Transform has been proposed to solve this problem. Literature [22] proposed a zero watermarking algorithm based on Contourlet Transform, which constructs a zero watermarking without changing the video content, and the algorithm is also more robust to most attacks. Zhang et al. [23] proposed a block adaptive compressed sensing reversible watermarking algorithm based on the trade-off between high embedding capacity and invisibility of digital image reversible watermark. Literature [24] proposed robust reversible watermarking technology based on an independent embedding threshold and robust reversible watermarking technology based on the JND threshold in the frequency domain. Naskar and Chakraborty [25] developed a statistical modeling technique to derive a reversible watermarking algorithm based on pixel prediction. The exported metrics and performance trends are apparent, and the developed model is accurate and consistent. Literature [26] proposed a visual watermarking algorithm, which has better transparency and antiattack.

In recent years, with the continuous improvement of digital watermarking technology. The research of the video watermarking algorithm has become the main direction, and a large number of video watermarking algorithms have been proposed. Shukla and Sharma [27] extracted the keyframes of scene changes and embedded the watermark in the low-frequency subband of the three-level DWT. The method has good watermark invisibility, but the watermark embedding capacity needs to be improved. Moreover, the watermark embedding position is always fixed in the low-frequency subband of the video frame. The robustness against various attacks has much room for improvement. Bao and Yang [28] designed a blind video watermarking algorithm combined with DWT-Schur decomposition. The experimental results show that the method has good robustness against noise attacks and video attacks, but the watermark embedding position is fixed. Wang [29] proposed a video watermarking algorithm in the DWT domain based on extreme learning machines, which have better watermark invisibility and can effectively resist multiple attacks. However, the watermark embedding capacity is too small, and the watermark embedding position has been fixed in the low-frequency subband.

For a long time, the research on the algorithm based on video watermarking mainly focused on a single watermarking. The advantages of a single watermarking algorithm are good transparency and clear functions, but a single watermarking sometimes cannot meet different requirements of users. The research of video double watermarking algorithm arises. The video double watermarking algorithm has the characteristics of high transparency and good security, and the double watermarking algorithm in the transform domain has higher transparency and robustness. Therefore, the transform domain double watermarking algorithm has been more widely used.

In literature [30], the whole wavelet transform is first applied to the carrier image, embedding a robust watermark in the low-frequency subband and a fragile watermark in the high-frequency subband. The literature [31] first embeds the robust watermark into the discrete wavelet coefficients of the image YCbCr color space. Moreover, it embeds the fragile watermark into the least significant bit of the image RGB color space. However, the extraction effect of the two watermarks is not very well. The literature [32] performs DWT on the image, then selects some coefficients to do singular value decomposition, and embeds the robust watermark in the singular values. Finally, they perform quaternion DCT on the image and embed the fragile watermark in the least significant bit of its coefficients. However, this algorithm does not resist crop attacks and rotation attacks well.

Blockchain technology was proposed by Satoshi Nakamoto in a Bitcoin paper, which has attracted widespread attention. It provides an effective solution to solve the digital copyright challenge [33–35]. Blockchain technology and digital copyright protection have a natural fit. Firstly, the blockchain can establish a hard link between user addresses and data objects, which realize data identification and clear ownership of rights and interests. Secondly, the characteristics of tamper-proof, forgery-proof, and traceable data on the chain can provide evidential proof and solidify evidence for digital works.

The current digital copyright protection based on blockchain has been studied in the academic field. The literature [36] designed a digital copyright protection and trading system based on blockchain technology. It uses the consortium blockchain technology to provide full-service digital copyright protection and trading services, such as digital content copyright registration, tracking, authentication, query, and trading. However, this literature only mentions depositing the eigenvalues of digital content into the blockchain. It does not explain for different types of works which digital content eigenvalue extraction technology is used. The literature [37] designed a digital copyright transaction system model based on the consortium blockchain, which can guarantee the immutability and traceability of copyright information. However, it does not describe too much about copyright registration. The literature [38] proposed a Hyperledger-based digital copyright registration model based on blockchain technology, which is mainly for the registration of works in the form of text as the carrier and focuses on the part of copyright registration. The paper [39] proposed a federated audio and video copyright blockchain system based on the improved Practical Byzantine Fault Tolerance algorithm. The literature [40] proposed a distributed digital copyright management mechanism based on a blockchain credit system, which focuses on the copyright transaction process. The scheme achieves the irreversibly encrypted record of the copyright transaction process and makes lightweight adjustments to the data structure of the distributed ledger. In addition, scholars in the literature [41, 42] have proposed new digital rights management schemes by combining digital watermarking technology and blockchain.

3. Video Double Watermarking Copyright Protection Scheme

3.1. Architecture. The architecture of the system is shown in Figure 1, which is mainly divided into client-side, video copyright protection platform, blockchain network, and server-side.

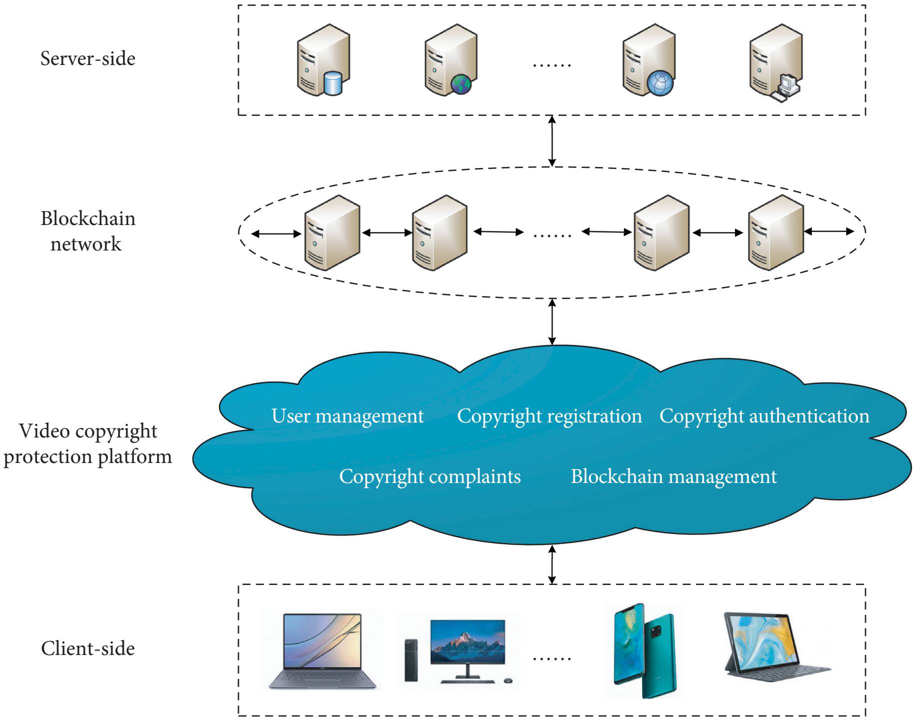


Figure 1: Architecture.

(1) Client-side: this part has encapsulated the complex and abstract transaction logic into a concise and beautiful visual interface to present to users, which has understandable operation logic and well interaction and user operation experience.

(2) Video copyright protection platform: the platform includes five functional modules, comprising user management, copyright registration, copyright authentication, copyright complaints, and blockchain management. The following is the system process:

(i) The users register and become legal users.

(ii) The users upload the video to be registered. And the system performs the copyright audit of the video, which uses similarity detection to determine whether the video is registered and whether the watermark meets the requirements. The G component of the video keyframes is processed with the second-level Contourlet Transform. Then, the QR decomposition is performed on the low-frequency subband, and the R matrix is selected as the robust watermark embedding carrier. And the fragile watermark is embedded in the least significant bit of the B component of the video keyframes. After passing the authentication, the signature of the watermark hash digest value and user ID generated by SM2 are uploaded to the blockchain to generate the block. After that, the copyright registration is completed.

(iii) The users upload the video to be authenticated and perform copyright detection after extracting keyframes. The platform compares the user watermark with the watermark hash value on the blockchain to realize the binding of user identity and robust watermark. We achieve the matching of the robust watermark with the embedded video by comparing the user watermark with the NC value of the extracted watermark. After that, the copyright authentication is completed.

(iv) When users find others have preregistered their videos, they can submit credible proof. If the administrator approves, the platform will transfer the video copyright, upload the transaction information, update the database, and after that complete the copyright complaints.

(3) Blockchain network: this part is responsible for the erection and management of the Fabric network, including distributed ledger, smart contract, consensus mechanism, and other components, which is the basis for the well operation of blockchain services.

(4) Server-side: it is the foundation of the platform application services, which are responsible for the client's transactions logic processing and communication with the blockchain network. It includes the processing and execution of functional modules of blockchain management and other services. In addition, it includes MySQL local database and provides security services such as identity authentication and permission management for the platform. We use an enterprise application framework for development, with good security and coupling degree and through the way as "Java back-end to SDK to

blockchain" to achieve efficient communication with the Fabric network.

3.2. Copyright Registration. Copyright registration mainly includes copyright audit, watermark embedding, and identity authentication functions. The process is shown in Figure 2.

(1) Copyright audit:

In copyright registration, keyframes are first extracted from the video. Then, the keyframes are audited for similarity by using the perceptual hash algorithm. User watermarks are also audited in the same way. It is divided into four steps: ① scaling the image; ② converting the grayscale image; ③ calculating DCT; ④ shrinking DCT; ⑤ calculating the difference value; ⑥ calculating the fingerprint. After getting the pHash value of the picture, we compare the hamming distance of the pHash value of the two pictures. Usually, a group of pictures with hamming distance less than 10 is commonly considered as similar pictures.

(2) Watermark embedding:

Users register, become legal users, and then log in to this system. They need to provide the video for copyright registration and the watermark containing personal information, which is the video to be embedded with the watermark and the robust watermark. Firstly, the keyframes of the video to be registered are extracted using the image correlation coefficient method to prepare for embedding the digital watermark. Secondly, the robust watermark is encoded with the hamming code. Thirdly, we embed the robust watermark in the video by using the Contourlet-based digital double watermarking technology, and the fragile watermark is generated by the robust watermark. Furthermore, the video with a double watermark is obtained.

(i) Video keyframe extraction

The image correlation coefficient method is used to measure the similarity of adjacent image frames in the video to realize the extraction of keyframes. Suppose that the video has a total of NOF frames and $i = 1$; then the keyframe extraction steps are as follows:

Step 1: Obtain matrix A by reading frame i of the video.

Step 2: Read the next frame, namely, the matrix B of frame $i + 1$.

Step 3: Use A and B matrixes of the same size to calculate the similarity r of adjacent image frames. If the difference value is greater than a certain threshold, frame i is selected as the keyframes and output i.

Step 4: If $i + 1$ >NOF, all keyframes of the video have been extracted, otherwise $i = i + 1$, and go back to Step 1.

(ii) Robust watermark preprocessing

Set the binary image W_1 of size $m \times n$ as the robust watermark image. The preprocessing steps are as follows:

Step 1: Transform the binary image W_1 into matrix A with 4 columns and $m \times n/4$ rows (zero padding).

Step 2: Each row of matrix A is coded with (7, 4) hamming code to obtain the matrix A' containing error correction codes, namely, the robust watermark image W_1^*.

(iii) Robust watermark embedding

Set the color image I of size $M \times N$ as the carrier image, and the process of robust watermark embedding is shown in Figure 3.

Detailed steps are as follows:

Step 1: Separate components R, G, and B in the RGB color space model of the color carrier image I. Then, we perform the second-level Contourlet Transform on the component G to extract the second-level low-frequency subband.

Step 2: Divide the second-order low-frequency subband into 4×4 blocks. And we perform QR decomposition of each small block to obtain $(M \times N)/256$ Q matrixes and $(M \times N)/256$ R matrixes.

Step 3: Select element (C_{12}) in row 1 and column 2 as the coefficient value of the embedding position and embed the watermark there.

Step 4: Perform Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation for the robust watermark W_1^* to form an encrypted robust watermark, denoted as $W_1^{* *}$.

Step 5: Set the quantization step L as the optimal value 50 obtained in the previous experiment. Then, divide the coefficient value C_{12} at the above embedding position by L to get the quantization value, namely, $q = C_{12}/L$. And then, we embed the robust watermark $W_1^{* *}$ into the R matrix to get the matrix R' with robust watermark.

Set the quantization value as q and the pixel value of the encrypted robust watermark as w. If $w = 0$, then the coefficient value C_{12}' of the element (C_{12}) in row 1 and column 2 of R matrix after embedding the watermark is

$$C_{12}' = \left\{ \begin{array}{ll} q \times L & \mathrm{mod}\,(q, 2) = 0 \\ (q - 1) \times L & \mathrm{mod}\,(q, 2) = 1 \end{array} \right\}. \tag{1}$$

If $w = 1$, then the coefficient value C_{12}' of the element (C_{12}) in row 1 and column 2 of R matrix embedded with watermark is

$$C_{12}' = \left\{ \begin{array}{ll} (q + 1) \times L & \mathrm{mod}\,(q, 2) = 0 \\ q \times L & \mathrm{mod}\,(q, 2) = 1 \end{array} \right\}. \tag{2}$$

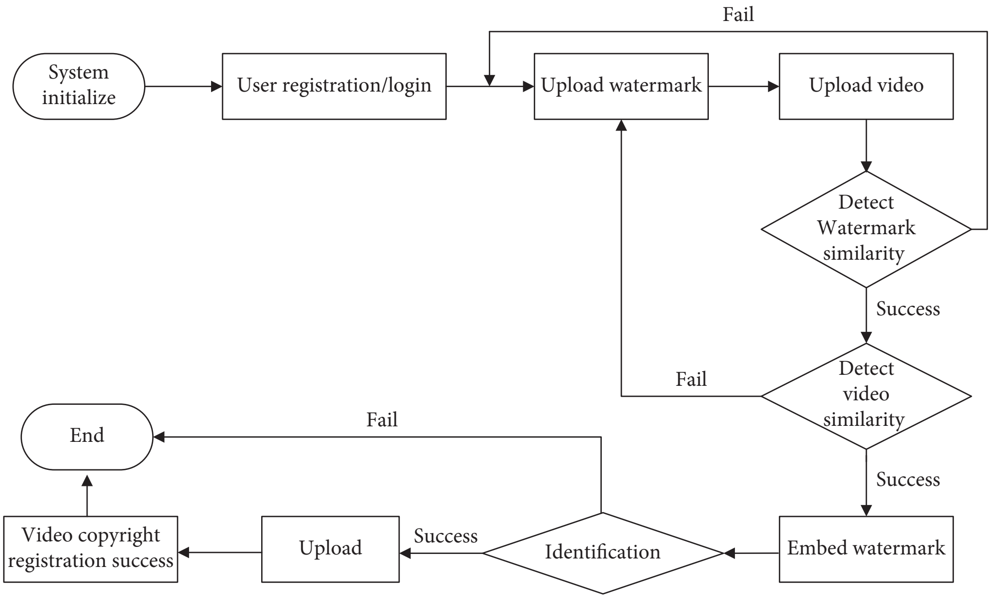


Figure 2: Copyright registration.

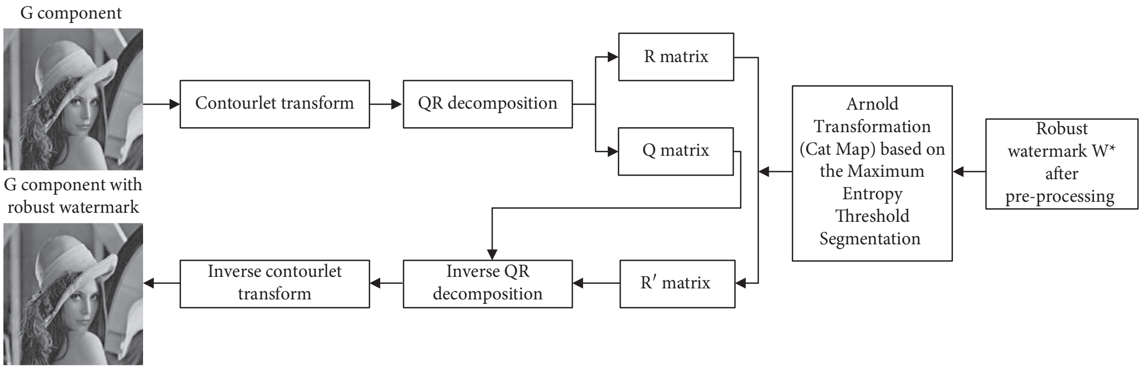

G component
Contourlet transform
QR decomposition
R matrix
Q matrix
Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation
Robust watermark W* after pre-processing
G component with robust watermark
Inverse contourlet transform
Inverse QR decomposition
R′ matrix

Figure 3: Embed robust watermark.

Step 6: perform Inverse QR decomposition on matrix R' embedded with robust watermark. Moreover, the Inverse Contourlet Transformation is performed to obtain component G containing robust watermark, denoted as G^*.

(iv) Fragile watermark embedding

Use the components R and B separated in the robust watermark embedding process and the component G^* containing the robust watermark for the formation and embedding of the fragile watermark. The process of embedding fragile watermarks is shown in Figure 4.

Detailed steps are as follows:

Step 1: Set the least significant bit of the gray value of component B to 0, denoted as B'.

Step 2: Divide the components R, G^*, and B' into 2×2 blocks and calculate the mean value of the three components. The value is changed into 8-bit binary numbers. And the highest 4 bits is extracted to form a 2×2 small matrix to form the fragile watermark W_2.

Step 3: The fragile watermark W_2 is correspondingly embedded into the least significant bit of the B' component and obtain the B' component containing the fragile watermark, denoted as B^*.

Step 4: Components R and G^* containing robust watermark and B^* containing fragile watermark are combined to form a color image I^* containing double watermark.

(3) Identity authentication:

After the watermark is embedded, SM3 is used to hash the robust watermark and the user ID, respectively. Then, we use the digest value of the user ID as the private key, and SM2 is used to generate the corresponding public key. The robust watermark digest value and user ID are signed with the private key. The public key is used for verification before uploading to the blockchain. If the ID obtained by

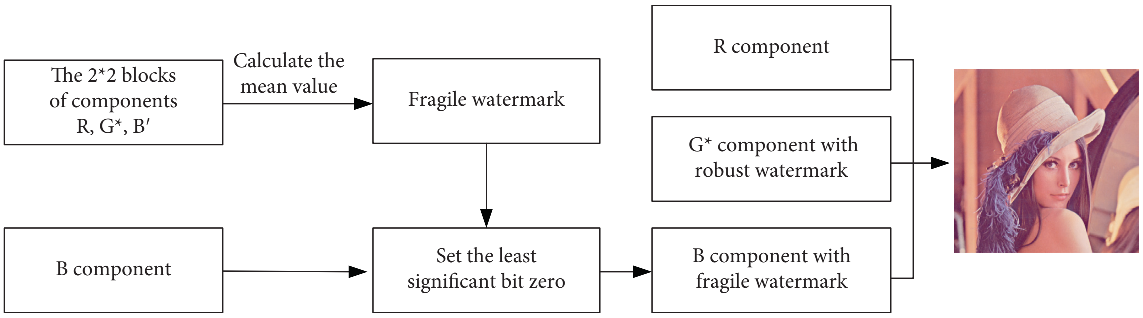

The 2*2 blocks of components R, G*, B′
Calculate the mean value
Fragile watermark
R component
G* component with robust watermark
B component
Set the least significant bit zero
B component with fragile watermark

Figure 4: Embed fragile watermark.

decryption matches the user's identity, the authentication is passed. And then, the system uploads the signature to the blockchain platform. After that, the copyright registration is completed. On the contrary, it will be refused to upload to the blockchain, failing to complete the copyright registration. The specific process is shown in Figure 5.

3.3. Copyright Authentication. Copyright authentication requires proving the watermark's relevance with the video and the watermark's relevance with the individual. Suppose it is proved that the user's watermark is embedded in the video and the user watermark is owned by the user. Then, the video is also owned by the user. The copyright registration module mainly includes watermark extraction, watermark owner authentication, and video owner authentication. The process is shown in Figure 6.

(1) Watermark extraction

When the users upload the video to be detected, we call the SIFT algorithm to process the video to be detected. Then, we carry out the reverse process of the watermark embedding algorithm. If the extraction fails, it means that the video has not been registered on this platform. If the extraction succeeds, the watermark in the video to be detected is obtained. Whether the watermark is the user's watermark requires further authentication.

The blind watermarking algorithm is used to extract fragile watermark and robust watermark. The process of extracting fragile and robust watermark is shown in Figure 7.

The detailed process of extracting the fragile watermark and robust watermark is as follows:

(i) Fragile watermark extracting:

Step 1: Separate the color channels R, G, and B of the color image with double watermark of size from each other. And we extract the least significant bit of component B and set it to zero to form a fragile watermark matrix W_2' of size $M \times N$.
Step 2: Divide the components R, G, and B into 2×2 blocks and calculate the mean value. Moreover, the maximum 4 bits of the mean value are extracted and form a 2×2 small matrix, denoted as $T_k\,(k = 1, 2, \ldots, M \times N/4)$.
Step 3: Divide fragile watermark matrix W_2' into 2×2 blocks, denoted as $W_{2k}''\,(k = 1, 2, \ldots, M \times N/4)$. If W_{2k}'' and T_k are equal, then the kth $(k = 1, 2, \ldots, M \times N/4)$ small matrix of the positioning matrix L is the null matrix. Otherwise, it is the matrix of all ones.

(ii) Robust watermark extracting

Step 1: Separate the color channels R, G, and B of the color image with double watermarks of size $M \times N$. And we perform a second-level Contourlet Transform on the G component and extract its low-frequency subbands.
Step 2: The low-frequency subbands are divided into 4×4 blocks, and QR decomposition is performed to obtain $(M \times N)/256$ matrix Q' and $(M \times N)/256$ matrix R'.
Step 3: Calculate the quantization value $q' = \mathrm{round}\,(C_{12}'/L)$ of the coefficient value C_{12}' in row 1 and column 2 of the matrix R'. Among them, L is the quantization step. Furthermore, the extraction of the robust watermark W_{1T} is performed. A pixel value w_{1T} of the extracted robust watermark W_{1T} (undecrypted and with supervision code) is

$$w_{1T} = \left\{ \begin{array}{ll} 0 & \mathrm{mod}\,(q', 2) = 0 \\ 1, & \mathrm{mod}\,(q', 2) = 1 \end{array} \right\}. \tag{3}$$

Step 4: Firstly, the matrix W_{1T} is decrypted by inverse Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation. Then, the robust watermark matrix W_{1T}' containing only the supervisory code is obtained.
Step 5: Transform the robust watermark matrix W_{1T}' with supervisory code into A' with 7 columns and calculate the correctors of each row in the matrix A'.
Step 6: Correct the element values in each row of matrix A'. Then, we extract the first 4 columns of elements in matrix A' and turn them

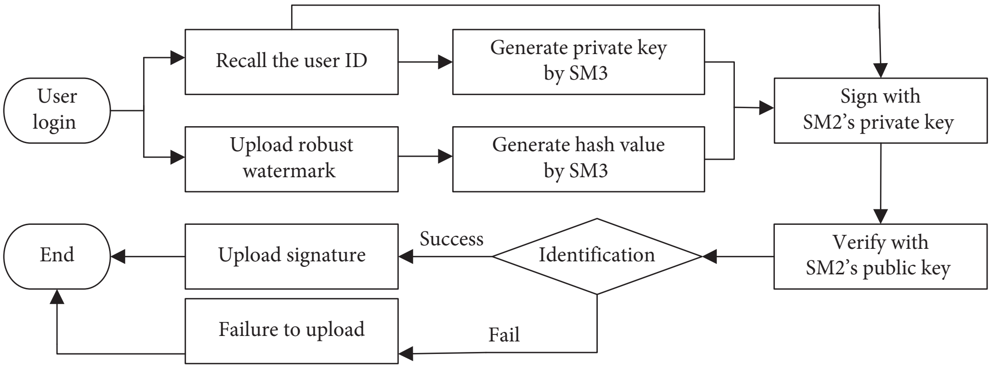


Figure 5: Identity authentication.

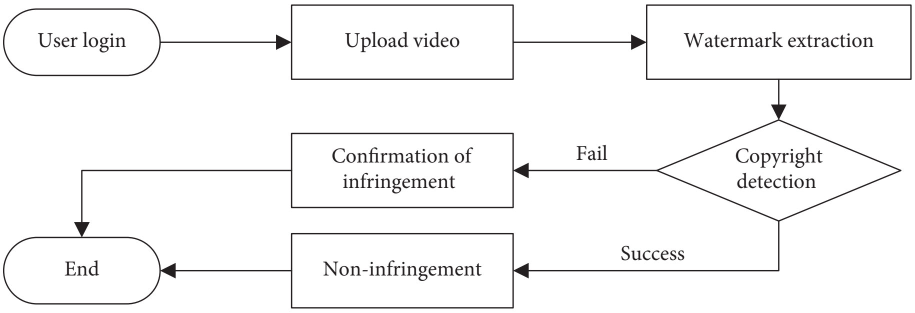


Figure 6: Copyright authentication.

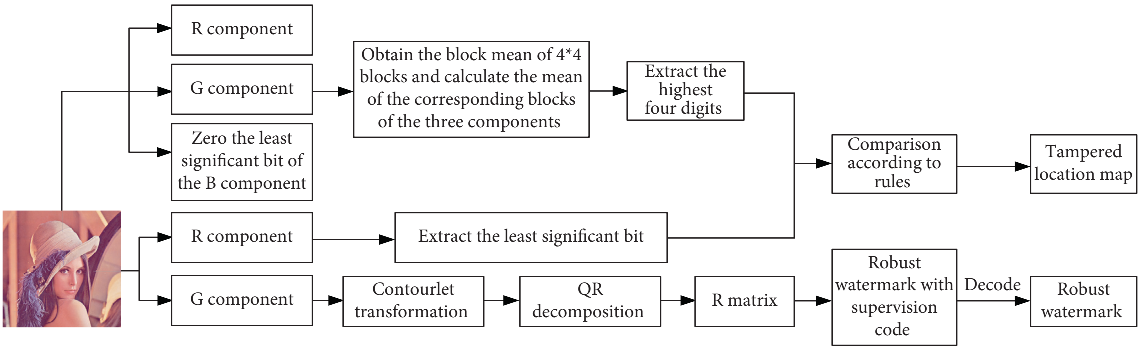

R component
G component
Zero the least significant bit of the B component
Obtain the block mean of 4*4 blocks and calculate the mean of the corresponding blocks of the three components
Extract the highest four digits
Comparison according to rules
Tampered location map
R component
Extract the least significant bit
G component
Contourlet transformation
QR decomposition
R matrix
Robust watermark with supervision code
Decode
Robust watermark

Figure 7: Extract watermark.

into a square matrix denoted as W_1'. The robust watermark was finally extracted and restored.

(2) Watermark owner authentication:

Blockchain digital copyright registration mainly relies on the timestamp and the hash value. The timestamp is the added time of data content, once generated, that cannot be falsified and synchronized to the connected block. It is not possible to modify a newly generated block record unless the attackers have at least 51% of the total network capacity, but it is impossible. Consequently, it could ensure the heterogeneity and reliability of the information before and after. We call the corresponding public key through the user ID to verify the signature on the blockchain and obtain the digest value of the watermark and the user ID. Hence, the user watermark is owned by the user, which proves the correlation between the watermark and the user.

(3) Video owner authentication:

Copyright authentication module requires users to provide the user watermark and the video to be authenticated. If the user stores the user watermark, it is easy to lose. Besides, storing for a long time or after the transmission can easily cause a certain degree of distortion of the watermark image. Therefore, we use the database directly to retrieve the corresponding user watermark. The platform compares the normalized correlation coefficient between the extracted watermark and the user watermark. If the watermark passes the threshold value, it indicates that the watermark in the video is on the blockchain, proving the correlation between the video and the watermark.

3.4. Blockchain Management. We use Hyperledger Fabric to construct the blockchain module. Fabric is a consortium blockchain with features such as permissioned networks, confidential transactions, and pluggable architecture. Only individuals approved to join the blockchain network can participate in transactions. It offers a unique approach to the consensus that enables performance at scale while preserving privacy and can meet the needs of building a video copyright protection platform. Blockchain management is shown in Figure 8.

Node configuration: when building the blockchain, it is required to set the configuration information of different nodes. This module carries out CA authentication for nodes and sets basic configurations such as consensus algorithm and block size in the blockchain configuration file. When necessary, the number of nodes can be dynamically added through node configuration and allowing nodes certified by CA to join the blockchain to build the video copyright protection ecology together.

Channel creating: the channel feature in the Fabric can be used to separate the data of different channels in the ledgers shared by different nodes according to their requirements. In this system, it only needs to complete the basic node configuration and build a channel.

Smart contract deployment: the smart contract in the blockchain needs to be deployed at every node in the channel to be effective. So, the watermark information uploaded to the blockchain needs to be written into the smart contract. And the smart contract needs to be deployed and instantiated.

Copyright information uploading: when the users provide a robust watermark, the video platform will call the copyright information uploading function in the smart contract. And it uploads the signature of the watermark hash digest value and user ID generated by SM2 to the blockchain and generates a block.

When the video platform receives the uploading request, it will issue information to the blockchain module. The blockchain workflow is as follows: ① The transmitting node broadcasts the new watermark digest information to the whole blockchain network. ② The receiving node checks the record information of received data, such as whether the record information is legitimate. After passing the inspection, the data record will be included in a block. ③ All receiving nodes in the whole network perform the consensus algorithm for the block. ④ The block is formally incorporated into the blockchain after processing the consensus algorithm, and each network node achieves agreement on the incorporation of the block. The method of acceptance is to regard the random hash value of the block as the latest block hash value. And the manufacture of new blocks will be extended based on this blockchain.

In the way of uploading data to the blockchain, we choose to adopt the digital signature to store proof. The signature is the hash value of the robust watermark signed by SM2. Its hash value, also known as "digital fingerprint," can be obtained by hashing the robust watermark. We use SM2 to sign the hash of the robust watermark and the user ID together and upload the signature to the blockchain.

4. Experiment and Analysis

In order to make the experimental results more accurate, we collected and organized 50 different videos in uncompressed MP4 format from the network to carry out the test, mainly taking the "landscape map" video as an example. The frame image is RGB color space with a size of 720×1280, the data rate is 20,604 kpbs, the total bit rate is 20,604 kpbs, the frame rate is 25.00 frames/sec, the audio sampling frequency is 44.100 kHz, the video size is 41.7 MB, the total number of video frames is 413 frames, and the duration is 17 seconds. The size of the watermark is a 9×12 binary image. The system uses MySQL8.0.22 as the back-end database. Bootstrap is used as the component development framework in the front-end, and the double watermarking processing is mainly implemented in MATLAB. Moreover, Hyperledger Fabric2.3 is used to build the blockchain platform, and the back-end uses IDEA for debugging. Table 1 shows the software and hardware environment.

4.1. Experiment

4.1.1. Blockchain Performance. We use Caliper to test the performance of our blockchain network. Caliper is a blockchain performance testing framework that can test the performance of a blockchain network with a defined set of tests and generate test reports. Caliper supports the tests of transaction success rate, transactions per second (TPS), transaction latency, and resource consumption performance metrics. The blockchain industry standards are shown in Table 2.

The results of the blockchain test are shown in Figure 9. The transaction success rate of this test is 100%, the average transaction delay is 0.71 s (the maximum transaction delay is 2.54 s, and the minimum transaction delay is 0.07 s), and the throughput is 221.2 transactions/second.

The test results show that it conforms to the industry standard.

4.1.2. Commercial Cryptography Algorithm Performance. This system combines SM2 and SM3 with blockchain technology and is mainly applied to the digital signature of transactions. SM3 and SHA-256 are both hash algorithms. SM2 is a public key cryptography algorithm based on the discrete logarithm problem on the elliptic curve, and its key length is 256 bits. To compare SM2 with the international mainstream cryptography algorithm, we select ECC-256, the public key cryptography with the same key length as the comparison object. During the process of digital signature and signature verification, SM2 and ECC use SM3 and SHA-256 to perform hash operations, respectively. Therefore, we will design test experiments on SM2 and ECC to compare the advantages of the blockchain using the commercial cryptography algorithm compared with the ordinary blockchain architecture.

(1) Test environment:

The two algorithms use elliptic curves based on the prime number field, and the equation on the prime number field F_p is

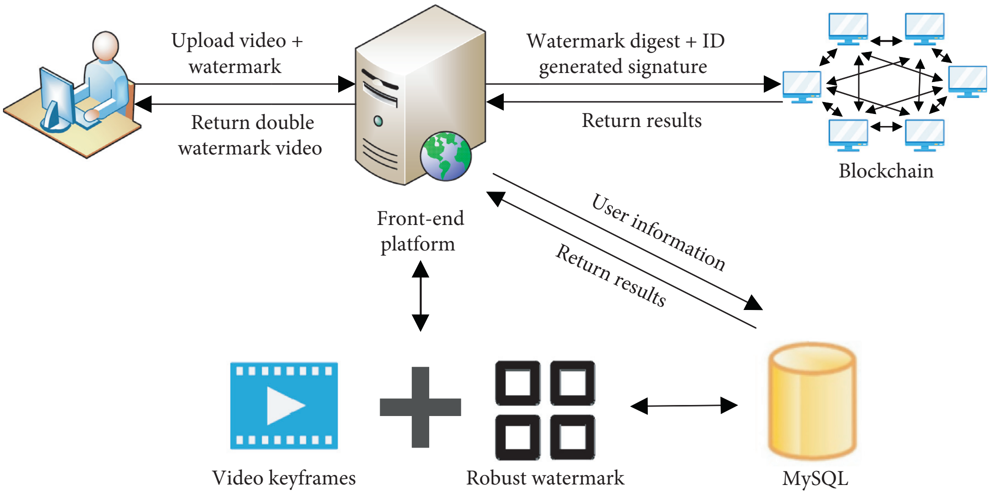


FIGURE 8: Blockchain management.

TABLE 1: Software and hardware environment.

Name	Environment
CPU	i7-10875H
GPU	RTX2080SMQ
Memory	32G
OS	Ubuntu18.04
Blockchain	Fabric2.3
Database	MySQL8.0.22
Watermarking development tool	MATLAB R2018b
Server-side debugging tools	IDEA
Front-end debugging tool	Visual studio code

TABLE 2: Blockchain industry standards.

Rule requirements	Rule item	Requirements
Test scenarios	Stress test	The number of transactions received per second is basically the same as the number of uploads, and the success rate of uploads is higher than 95%
	Spike test	The number of transactions received per second is significantly higher than the number of uploads, and the success rate of uploads is higher than 75%
	Stability test	Low-load operation with no system crashes
Results	Performance indicators	Upload success rate (95%) TPS (>200) average delay time (<0.5 s)

$$y^2 = x^3 + ax + b. \tag{4}$$

Among them, SM2 adopts the commercial cryptography standards, and the parameters are as follows:

$a = 0xFFFFFFFEFFFFFFFFFFFFFFFFFFFFF$
$FFFFFFFFFFF00000000FFFFFFFFFFFFFFFC$

$b = 0x28E9FA9E9\ D9F5E344\ D5\quad A9E4BCF6509$
$A7F39789F515AB8F92\ DD\ BCB\ D\ 414\ D940E93$

ECC adopts the secp256k1 curve, and the parameters are as follows:

$a = 0x0000000000000000000000000000000000000$
$000000000000000000000000000$

$b = 0x0000000000000000000000000000000000000$
$0000000000000000000000007$

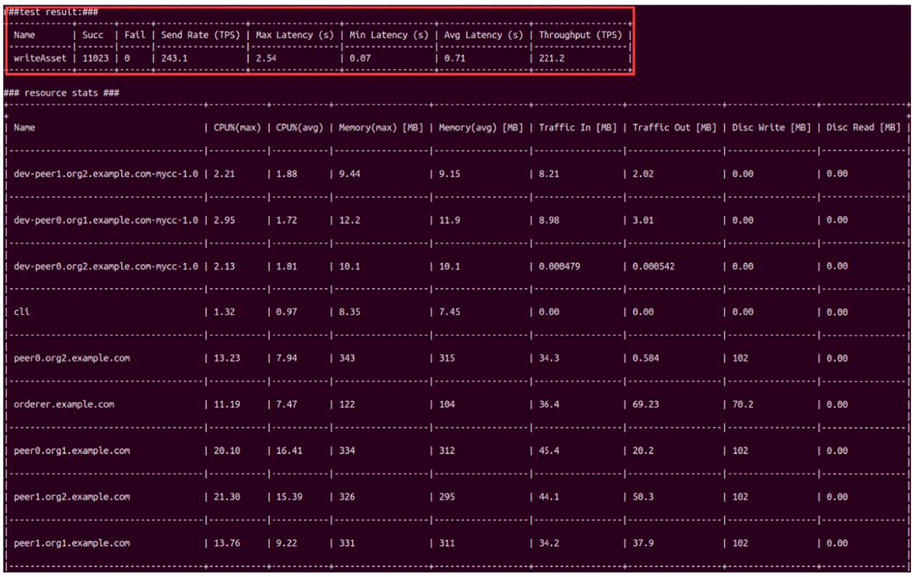
(2) Test method:

We, respectively, use SM2 and ECC to complete 10,000 signing and verifying operations and calculate the time and memory costs of the signing and verifying for 32-byte, 64-byte, and 128-byte strings.

(3) Test results:

(i) Time overhead

As can be seen from Table 3, the SM2 signing and verifying have a faster execution speed. It saves about 20% time compared with the secp256k1 curve adopted in Bitcoin.



```
###test result:###
+-----------+-------+------+------------------+------------------+------------------+------------------+------------------+
| Name      | Succ  | Fail | Send Rate (TPS)  | Max Latency (s)  | Min Latency (s)  | Avg Latency (s)  | Throughput (TPS) |
|-----------|-------|------|------------------|------------------|------------------|------------------|------------------|
| writeAsset | 11023 | 0   | 243.1            | 2.54             | 0.07             | 0.71             | 221.2            |
+-----------+-------+------+------------------+------------------+------------------+------------------+------------------+

### resource stats ###
+-----------------------------------+-----------+-----------+-------------------+-------------------+-----------------+------------------+-----------------+-----------------+
| Name                              | CPU%(max) | CPU%(avg) | Memory(max) [MB]  | Memory(avg) [MB]  | Traffic In [MB] | Traffic Out [MB] | Disc Write [MB] | Disc Read [MB]  |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| dev-peer1.org2.example.com-mycc-1.0 | 2.21    | 1.88      | 9.44              | 9.15              | 8.21            | 2.02             | 0.00            | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| dev-peer0.org1.example.com-mycc-1.0 | 2.95    | 1.72      | 12.2              | 11.9              | 8.98            | 3.01             | 0.00            | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| dev-peer0.org2.example.com-mycc-1.0 | 2.13    | 1.81      | 10.1              | 10.1              | 0.000479        | 0.000542         | 0.00            | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| cli                               | 1.32      | 0.97      | 8.35              | 7.45              | 0.00            | 0.00             | 0.00            | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| peer0.org2.example.com            | 13.23     | 7.94      | 343               | 315               | 34.3            | 0.584            | 102             | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| orderer.example.com               | 11.19     | 7.47      | 122               | 104               | 36.4            | 69.23            | 70.2            | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| peer0.org1.example.com            | 20.10     | 16.41     | 334               | 312               | 45.4            | 20.2             | 102             | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| peer1.org2.example.com            | 21.30     | 15.39     | 326               | 295               | 44.1            | 50.3             | 102             | 0.00            |
|-----------------------------------|-----------|-----------|-------------------|-------------------|-----------------|------------------|-----------------|-----------------|
| peer1.org1.example.com            | 13.76     | 9.22      | 331               | 311               | 34.2            | 37.9             | 102             | 0.00            |
+-----------------------------------+-----------+-----------+-------------------+-------------------+-----------------+------------------+-----------------+-----------------+
```

FIGURE 9: Blockchain performance test.

(ii) Memory overhead

As shown in Table 4, the signing and verifying by SM2 + SM3 take up less memory than the ECC-256 + SHA-256, which saves about 10% of the memory.

TABLE 3: Signing and verifying time of SM2 and ECC-256.

Algorithm	Signing time/s	Verifying time/s
SM2	981	1975
ECC-256	1145	2321

TABLE 4: Memory overhead of the signing and verifying of SM2 and ECC-256.

Algorithm	ROM/Byte	RAM/Byte
SM2	10895	3015
ECC-256	10157	3202

4.1.3. *Security*.

(1) Test indicators

(i) Invisibility:

The test of invisibility of the watermark is described by the peak signal-to-noise ratio (PSNR). The larger the PSNR, the smaller the difference between the two. Conversely, the more significant the difference between the two, the smaller the PSNR. The calculation formula of PSNR is as follows:

$$\mathrm{PSNR}\,(F, F') = 10\,\log_{10}\left(\frac{hw255^2}{\sum_{i=1}^{h}\sum_{j=1}^{w}\left(F_{i,j} - F'_{i,j}\right)^2}\right), \tag{5}$$

where F and F' represent two images and h and w, respectively, represent the number of rows and columns of the image. Generally, if the PSNR is greater than 35 dB, the visual quality of the original video frame is not significantly different from the watermark video frame.

(ii) Robustness:

The NC value can be used to evaluate the robustness of the watermark. After analyzing and summarizing a large number of traditional watermarks related literature data, we conclude that, in the scenario of assuring image quality (the PSNR is greater than 35 dB), if the NC of the watermark information is higher than 0.85, then this watermarking algorithm could be considered to have robustness.

$$\mathrm{NC}\,(i, j) = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N} T\,(m,n)S^{ij}\,(m,n)}{\sqrt{\sum_{m=1}^{M}\sum_{n=1}^{N} T^2\,(m,n)\sum_{m=1}^{M}\sum_{n=1}^{N}\left(S^{ij}\,(m,n)\right)^2}}. \tag{6}$$

Among them, $T\,(m,n)$ is the nth line from the bottom and the mth pixel value of the template image. $S\,(i,\,j)$ is the part covered by the template, which is called the search subgraph, i and j are the image point coordinates in the lower-left corner of the search subgraph in the reference graph S.

(2) Attack tests

(i) Invisibility:

We embedded watermarks on different video frames and tested their PSNR. The detailed results are shown in Table 5.

Table 5: Detailed effect display.

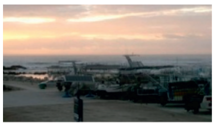
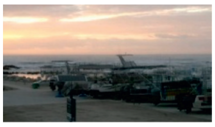
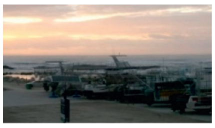
Original video frame	Embedded watermark video frame
	 PSNR: 45.706 dB
Original video frame 	Embedded watermark video frame PSNR: 45.4470 dB
Original video frame 	Embedded watermark video frame PSNR: 45.9029 dB

Table 6: The effect of extracting watermark after the attack.

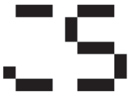
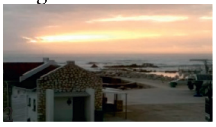
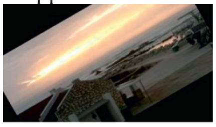
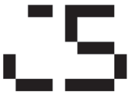
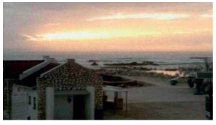
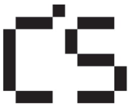
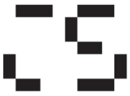
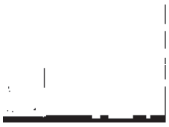
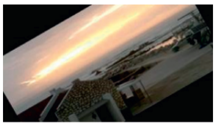
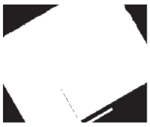
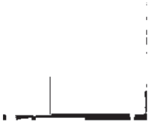
Original video frame	Embedded watermark	Embedded watermark video frame	Clipped video frame	Extracted watermark
				 NC: 0.9840
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9761
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9940
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9826

Table 6: Continued.

Original video frame	Embedded watermark	Embedded watermark video frame	Clipped video frame	Extracted watermark
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark NC: 0.9941

Table 7: Statistics of precision rate and recall rate.

Embedded watermark video frame	Embedded watermark video frames after clipping attacks	Location map
	 Precision rate: 95.22%	 Recall rate: 90.68%
Embedded watermark video frame 	Embedded watermark video frames after rotation attacks  Precision rate: 96.81%	Location map  Recall rate: 92.63%
Embedded watermark video frame 	Embedded watermark video frames after sharpening Precision rate: 85.73%	Location map  Recall rate: 82.66%

As shown in Table 5, the results of PSNR all exceed 45 dB, which indicates that the difference between video frames before and after watermark embedding is slight and the invisibility is well.

(ii) Robustness:

Attacks can be used to detect the actual performance of a system. There are two types of attacks in the actual transmission process: unintentional and intentional. Traditional image attack methods include gamma correction, median filtering, shear attack, rotation attack, histogram equalization, Gaussian noise, motion blur, contrast ratio adjustment, and sharp attack. The attacks against video include frame deletion and frame displacement. Table 6 shows the different attack methods used on video frames, and the NC and PSNR values are tested.

As shown in Table 6, NC values all exceed 0.9. It indicates that the extracted watermark and embedded watermark have high similarity and well robustness.

(iii) Tampering location:

The system adopts double watermarking technology, in which the fragile watermark can realize the tamper location function. Experiments on deleting, replacing, and adding malicious tampering are carried out to the watermark videos, respectively.

The precision rate and recall rate are used to evaluate and analyze the tamper location results.

$$\begin{aligned} \text{precision rate} &= \frac{\mathrm{AB}}{A} \times 100\%, \\ \text{recall rate} &= \frac{\mathrm{AB}}{B} \times 100\%. \end{aligned} \tag{7}$$

Among them, A is the area of the location area of the experimental results, B is the area of the real tampering area, and AB is the intersection of *A* and *B*. Table 7 shows the statistics of precision and recall rate.

As shown in Table 7, for physical attacks, the precision rate is above 95%, and the recall rate is about 90%, which well realizes the tamper location function of the fragile watermark.

4.2. Analysis. Confidentiality. When watermark and video are uploaded to the system, they need to pass similarity detection. After that, performs the hash operation on user ID by SM3 before uploading it to the blockchain platform. The user ID hash is used as the private key, which is used to sign the robust watermark hash and ID and upload the signature to the blockchain. When a copyright query or authentication is performed, the data can be obtained only by decrypting it with its corresponding public key, which realizes the confidentiality of user data. The confidentiality of the system is thus realized.

Integrity. After the user watermark is uploaded to the system, the user watermark and user ID are first hashed, and the user ID hash is used as the private key. The private key is used to sign the robust watermark and ID. Before uploading the signature to the blockchain platform, it needs to be decrypted with its public key to prevent the data from being tampered with and ensure the integrity of the system.

Authenticity. When users register for copyright, they must pass identity authentication before uploading the robust watermark information. Users use the SM2 algorithm to sign the information to be uploaded to the blockchain. The public key is invoked to verify the signature before uploading to the blockchain, ensuring that the user's identity matches the claimed identity.

Nonrepudiation. Blockchain has the characteristics of tamper-proof, openness, and transparency to achieve nonrepudiation. Transactions on the blockchain are organized through the Merkle tree. If any transactions are modified, it will cause some change in the hash value of the Merkle root. Furthermore, the timestamp can prove the order between blocks. Each data in the timestamp is secondary encryption. To tamper with the data, not only break the hash algorithm but also change the timestamp.

5. Conclusion

This paper is based on the double watermarking algorithm on Contourlet and blockchain technology. We generate a fragile watermark based on the robust watermark and embed both in the video. The double watermarking algorithm improves the robustness under the premise of ensuring the invisibility of the watermark and implements the tampering locating function. This system generates the digest value of the robust watermark based on SM3 and signs the digest value and the user ID using SM2. The signature is uploaded to the blockchain after passing the identity authentication, which significantly improves the credibility of the authentication and the security of the system. In the first part, we explain the wide application of video copyright protection and analyze the security threats faced by video copyright and the solutions. The second part introduces the current research status on video copyright protection at home and abroad. In the third part, we propose a video copyright protection system based on blockchain and double watermarking technology for the shortcomings of the traditional video copyright protection system using digital watermarking technology, such as low security, poor balance, poor robustness, and watermark not bound to individuals. In the fourth part, we test the performance of blockchain and commercial cryptography algorithms. Besides, we test the security of double watermarking and analyze the watermarking systems' confidentiality, integrity, authenticity, and nonrepudiation. The combination of blockchain and watermarking technology optimizes the traditional copyright protection scheme. The adoption of the commercial cryptography algorithm ensures the confidentiality and autonomy of the system. The improvement of the robust watermarking scheme improves the robustness, security, and self-adaptability of the watermark. Moreover, the adoption of improved fragile watermarking realizes the watermarked video integrity identification. The next steps of our job are as follows:

(1) In view of the low efficiency of the blockchain system itself, the multinode server is adopted to improve the efficiency of the video copyright protection system.

(2) We will find the best embedding point of the robust watermark to achieve the maximum energy and further improve the robustness of the robust watermark against geometric attacks.

(3) We will improve the copyright transfer module to realize copyright transactions.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Hainan Provincial Natural Science Foundation of China (621RC508 and 620RC563), the Science Project of Hainan University (KYQD(ZR)-21075 and KYQD(ZR)20021), and the National Natural Science Foundation of China (62162020).

References

[1] S. Xuan, *Research on Copyright Protection of Short Videos*, East China Jiaotong University, Nanchang, China, 2020.

[2] M. Ning, *Research on Digital Intellectual Property Protection Scheme Based on Blockchain Technology*, Xi'an University of Electronic Science and Technology, Xian, China, 2020.

[3] Q. Liu, *Design and Implementation of Video Copyright Protection System Based on Blockchain*, Dalian University of Technology, Dalian, China, 2020.

[4] F. Zhang, *Research on Copyright Protection Method of Stereo Image Video*, Ningbo University, Nigbo, China, 2019.

[5] Y. Huang, H. Xu, H. Gao, and X. Ma, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.

[6] M. Yang, *Research on Watermark Algorithm for Video Copyright Protection and Content Authentication*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2014.

[7] J. Hu, *Research on the Legal Protection of the Copyright of Network Film and Television Works*, Yunnan University of Finance and Economics, Kunming, China, 2020.

[8] H. Hu, *Research on the Legal Issues in Cross-Border M&A of Intellectual Property*, Jilin University, Jilin, China, 2020.

[9] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Robust video watermarking of H.264/AVC," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 54, no. 2, pp. 205–209, 2007.

[10] H. Gao, X. Qin, J. D. B. Ramon, W. Hussain, and Y. Xu, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence(TETCI)*, 2020.

[11] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2131–2153, 2018.

[12] J. Xiao, H. Xu, H. Gao, M. Bian, and L. Yang, "A weakly supervised semantic segmentation network by aggregating seed cues: the multi-object proposal generation perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1, pp. 1–19, 2021.

[13] X. Yang, S. Zhou, and M. Cao, "An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *Mobile Networks and Applications*, vol. 25, no. 2, pp. 376–390, 2020.

[14] L. Li, *Research on Digital Copyright Protection Based on Blockchain Technology*, East China Jiaotong University, Jiatong, China, 2020.

[15] H. Gao, K. Xu, M. Cao, J. Xiao, Q. Xu, and Y. Yin, "The deep features and attention mechanism based method to dish healthcare under social IoT systems: an empirical study with a hand-deep local-global net," *IEEE Transactions on Computational Social Systems(TCSS)*, 2021.

[16] T. Wu, *The Design and Implementation of Copyright Registration System Based on Blockchain*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2019.

[17] J. Shi, *Research and Implementation of Image Digital Copyright Protection Based on Blockchain and SIFT*, Beijing University of Posts and Telecommunications, Beijing, China, 2020.

[18] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "QoS prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.

[19] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the 1st International Conference on Image Processing*, vol. 2, pp. 86–90, Austin, TX, USA, November 1994.

[20] X. Liu, "An overview of digital video watermarking," *Video Engineering*, vol. 44, no. 5, pp. 11–15, 2020.

[21] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, 2005.

[22] X. Chen, G. Bu, and H. Li, "A video zero-watermark algorithm based on the contourlet transform," in *Proceedings of the 3rd International Conference on Multimedia(ICMT 2013)*, pp. 216–223, Dallas, Texas, USA, April 2013.

[23] Q. Zhang, Y. Sun, and Y. Yan, "A reversible watermark algorithm based on block Adaptive compressed sensing," *Journal of Electronics and Information Technology*, vol. 35, no. 4, pp. 797–804, 2016.

[24] X. Miao, T. Zhu, Y. Liu, Y. Lai, and W. Liu, "Double watermark algorithm for color images based on contourlet transform," *Journal of Xi'an University of Posts and Telecommunications*, vol. 23, no. 5, pp. 77–84, 2018.

[25] R. Naskar and R. S. Chakraborty, "A technique to evaluate upper bounds on performance of pixel-prediction based reversible watermarking algorithms," *Journal of Signal Processing Systems*, vol. 82, no. 3, pp. 373–389, 2016.

[26] T. Li, R. Sun, and C. Xu, "Video watermarking based on pseudo-3D-DCT in Contourlet domain," *Journal of Electronic Measurement and Instrument*, vol. 25, no. 8, pp. 734–740, 2011.

[27] D. Shukla and M. Sharma, "Robust scene-based digital video watermarking scheme using level-3 DWT: approach, evaluation, and experimentation," *Radioelectronics and Communications Systems*, vol. 61, no. 1, pp. 1–12, 2018.

[28] S. Bao and S. Yang, "Total-blind digital video watermarking algorithm based on DWT-schur," *Journal of Chongqing University of Technology (Natural Science)*, vol. 33, no. 10, pp. 136–141, 2019.

[29] Y. L. Wang, "Video watermarking algorithm based on extreme learning machine and discrete wavelet transform," *Chinese Journal of Liquid Crystals and Displays*, vol. 35, no. 2, pp. 180–188, 2020.

[30] L. Baiying, Z. Xin, H. Lei et al., "Multipurpose watermarking scheme via intelligent method and chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 19, Article ID 27107, 2019.

[31] X. Liu, C. Lin, and S. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1047–1055, 2018.

[32] S. Chen, R. Qi, and Y. Tang, "Multi-purpose watermark algorithm for color image based on multiple transform domains," *Journal of Computer Applications*, vol. 38, no. 8, pp. 2274–2279+2286, 2018.

[33] X. Lv, *Design and Implementation of Content-Publishing Platform Based on Blockchain*, Beijing University of Posts and Telecommunications, Beijing, China, 2020.

[34] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing," *Transaction Emerging Telecommunition Technology*, vol. 32, no. 5, 2021.

[35] H. Xiong, "On the design of blockchain-based ECDSA with fault-tolerant batch verication protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.

[36] C. Li, B. Dai, H. Wang, and X. Wang, "Digital copyright protection and trading system based on blockchain technology," *Modern Computer*, vol. 29, pp. 80–84, 2018.

[37] L. Li, S. Zhou, Q. Liu, and D. He, "Blockchain-based digital copyright trading system," *Chinese Journal of Network and Information Security*, vol. 4, no. 7, pp. 22–29, 2018.

[38] G. Zhao, Y. He, and J. Zhou, "Digital copyright registration technology based on blockchain," *Information Technology and Network Security*, vol. 38, no. 4, pp. 79–83, 2019.

[39] Z. Chen, Q. Li, J. Gan, C. Zhang, and Z. Li, "VC chain: an alliance audio-video copyright blockchain system," *Computer Engineering & Science*, vol. 41, no. 11, pp. 1939–1948, 2019.

[40] R. Zhou and L. Qian, "Blockchain based digital right management for distributed content delivery network," *Application Research of Computers*, vol. 37, no. 6, pp. 1794–1798, 2020.

[41] W. Wang and Z. Ye, "Application of blockchain technology in the financing of digital publishing supply chain," *Publishing Research*, vol. 8, pp. 31–34, 2018.

[42] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pp. 128–133, Bangkok, Thailand, March 2017.