Wu *et al. J Wireless Com Network* (2022) 2022:20
https://doi.org/10.1186/s13638-022-02090-x

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A novel zero-watermarking scheme based on NSCT-SVD and blockchain for video copyright

Xiangqi Wu[1], Peng Ma[1], Zihan Jin[2], Yuxuan Wu[3], Wenbao Han[1] and Wei Ou[1*]

*Correspondence: ouwei@hainanu.edu.cn
[1] School of Cyber Security (School of Cryptology), Hainan University, 58 Renmin Avenue, Meilan District, Haikou 570228, China
Full list of author information is available at the end of the article

Abstract

With the advent of information era, the issues on video copyright continue to emerge. In the grey industrial chain of piracy, the film industry is suffering a major disaster area. The current protection schemes for video copyright are inefficient and costly so that video industry still has to face the infringement. To address poor robustness, weak imperceptibility and difficulty in traceability of the current protection schemes for video copyright, this paper proposes a novel zero-watermarking scheme based on NSCT-SVD and blockchain for video copyright. In addition, we research the feasibility and reason of combining zero-watermarking with blockchain. The designed zero-watermarking algorithm is based on NSCT-SVD, Arnold Transform and key-frames extraction algorithm which is based on distance threshold clustering. The results show the extracted features from video are stable and secure than DWT-SVD based and the past non-blocking. The performance of the blockchain scheme designed for video copyright practices well. Comparatively, the discussion and results showed that the proposed scheme has been verified more credible and efficient in authoritative traceability compared to trusted third party based. The registration information cannot be tampered and be more suitable for copyright protection.

Keywords: Video copyright, Blockchain, Zero-watermarking, Secure, Key-frames extraction

1 Introduction

With video springing up as the mainstream way of information dissemination all over the world, the demand for video copyright protection schemes is growing. TikTok, YouTube and Hollywood represent the three mainstreams of the digital video industry today (short video, we-media and digital cinema). However, Hollywood loses 64.6 billion dollars caused by pirated videos every year. TikTok and YouTube are even more so. Streaming videos on TikTok and YouTube are casually reproduced without the approval of the owner, which infringes the copyrights of owner. Supposing user publishes a video on the video site which is sourced from another video site. In general, it will bring serious economic losses to both video sites. Overall, some tortious video applications damage the owners' copyrights and destruct the economic stability

Springer Open

© The Author(s) 2022. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

of its markets. Against this background, reliable protection technology for video copyright requires reorganization and innovation.

Digital watermarking technology in information hiding technology has been applied in the field of copyright protection for many years. Since digital watermarking technology has been well applied to images, it has inspired many researchers to research digital watermarking to videos. Currently, there are three types of schemes of video watermarking. The first way is the watermarking scheme based on original video, which is about embedding the information of watermark into the original video. The second way is based on the video encoding process. The compression standards of mainstream video include the MPEG series of ISO/IEC and the H.264 series of ITU-T [1, 2], and the key technology to achieve a high compression ratio is predictive coding and transform coding. The disadvantage of the second way is the presence of cumulative errors which can have an adverse effect on video quality [3]. The third way is based on the compressed domain. The advantage of this method is that the embedded watermarking does not need to be re-encoded and decoded, so it can reduce computational complexity through this way. The disadvantage is that the low redundancy of the compressed data limits the amount of data that can be watermarked, and the embedding strength is limited by the encoding of the video data. For extensive applications, this paper proposes a protection scheme for video copyright based on watermarking a video frame which follows the above first way.

Watermarking technology with various types has different applicable scenarios. Traditional watermarking technology can be briefly concluded as embedding watermark into host. Firstly, a large amount of research has focused on the traditional watermarking which includes preventing the embedded watermark from detection or attacks. Because there always be some ways to detect and attack the watermark through analysis on watermarked images. Therefore, it will be restricted in practical copyright protection scenarios. Secondly, it is worth noting that trust relationships [4] of watermark are also an important issue on copyright protection. The traditional blind watermarking lacks public notarization because it is generally ignored the relationship between watermark and identity. And traditional video zero-watermarking schemes need the trusted third-party to certify. However, in situations regarding cyberspace security, the centralized management of traditional zero-watermarking still has some problems. Thirdly, if zero-watermarking encrypted by keys, key management is a very important issue. At present, blockchain technology has been used to prevent DDOS and Key Generation Centre attacks [5]. Overall, zero-watermarking scheme with decentralized management may be one of the most potentially suitable solutions. In conclusion, this research mainly is proposed to address the main issues of existing digital watermarking schemes on video copyright protection. The issues are included as follows:

- Poor robustness: There is a high probability that the watermark in the video will be corrupted after multi-transform in the current network architecture or compression. The video watermarking scheme should ensure that it can still be verified under any form of transformation.

- Weak imperceptibility: The addition of watermark to some videos has a visually perceptible impact on the original quality of the video, making it less commercially viable. Besides, weak imperceptibility can also vulnerable lead to detection and attack.
- Difficulty in traceability of rights: Most current schemes have single function on copyright authentication. However, in an actual scenario of copyright protection, there will be some functions such as traceability of rights. The deficiency of existing schemes makes the actual process of rights maintenance quite complicated.

To address these three pressing issues of existing protection schemes mentioned in the previous paragraph, we study a video key-frames extraction algorithm based on distance threshold clustering and a colour zero-watermarking algorithm based on combination of Non-Subsampled Contourlet Transform (NSCT) with singular value decomposition (SVD). In addition, we innovatively combine video zero-watermarking algorithm with blockchain to address data management [6] and traceability of rights in current scheme for video copyright. The NSCT and SVD have studied in this field for several years and have owned widely recognized. We follow the previous research and recombined into proposed algorithm. The most prominent feature of NSCT is its strong anisotropy. Compared with wavelet transform, the high-frequency information has only horizontal, vertical and diagonal components. So, NSCT can decompose high-frequency information into multiple directional components. Besides, the singular value is a matrix concept, which usually be obtained by SVD decomposition and corresponds to the key information in this matrix. The importance of information is positively correlated with the magnitude of the singular value.

The remaining part of this paper is organized as follows. The related works are in Sect. 2. This section introduces the digital watermarking algorithmes in related researches, and also lists the copyright protection schemes that introduce new technologies. The proposed scheme is elaborated in Sect. 3. Firstly, we introduce the overall architecture of system for video copyright protection and illustrate how zero-watermarking interacts with blockchain to achieve copyright protection. Secondly, we introduce the extraction algorithm of the key-frames from video. Thirdly, we detail a zero-watermarking algorithm on key-frames based on NSCT and SVD. Section 4 shows the experimental results of proposed scheme. The security and privacy of proposed scheme are discussed in Sect. 5. Lastly, works of this paper are summarized in Sect. 6.

2 Related works

In the previous works, scholars have made a great progress in the study of digital watermarking on images. He studied on wavelet-based high-frequency and low-frequency methods for inserting watermark and tested their anti-compressibility for watermark extraction [7]. The experiments show that the insertion of watermark in the high-frequency domain keeps the original quality better, and the insertion of watermark in the low-frequency domain makes the robustness better. Li and Wei proposed a watermarking algorithm with double encryption based on cosine transform and fractional Fourier transform in the invariant wavelet domain [8]. Their work innovatively utilized image magnification technique to pre-process the host image to enhance embedding capacity of the watermarking algorithm. They used

the redistribution-invariant wavelet transform and the discrete cosine transform to obtain the hybrid domain. In conclusion, the present researches on blind watermark tend to enhance effectivity, but carry the computational burden.

Zero-watermarking has become a special way to address some issues about copyright protection in recent years since it was proposed by Wen, as it has the advantage of not making any modification to the original digital file [9]. Wang et al. proposed multiple zero-watermarking scheme based on local quaternion polar harmonic Fourier moments (QPHFMs) for colour medical images, and the construction of multiple zero-watermarking effectively improved reliability and resists complex out-of-step attacks, such as clipping [10]. Similar like present blind watermarking way, the cost of multiple zero-watermarks in exchange for robustness is actually expensive. Xue et al. proposed a more robust zero-watermarking algorithm based on NSST, DCT and Hessenberg decomposition. They innovatively generated a zero-watermark by performing XOR between the QR code and the characteristic matrix of a colour image [11]. Amiri and Mirzakuchaki proposed an intelligent watermarking model based on NSCT-SVD. They innovatively used PSO-GA-AI algorithm, and the obtained PSO and PSO-GA algorithms with larger SF have higher stability; then, low-frequency coefficient is fed back to the SVD through NSCT and SWT so that the values of model visual transparency and PSNR will increase [12]. Xue and Amiri support novel ideas in improved NSCT-SVD blind watermark.

Researches on recent key-frames extraction methods have achieved a lot. Nagaska et al.'s key-frames extraction based on shot boundaries, which combined key-frames by extracting the first, last and middle frames of the images [13]. But, this method is weak in abstracting the features in the images. Hannane et al. proposed a key-frames extraction method based on typical features, which selected key-frames by the change in information entropy, and the accuracy of the threshold setting will directly determine the quality of key-frames extraction [14]. Barbieri et al. select the candidate frames and the distance of the feature vector to extract key-frames based on CNN (convolutional neural network). However, this method needs to give the size of the candidate frame and has some limitations in the extraction of dynamic picture feature values [15].

Except using digital watermarking for copyright protection, blockchain technology is applied to digital copyright protection. *PetaPixel* develops *Blockkai* which uses the Bitcoin blockchain to protect copyright, and *Baidu* develops *Totem* based on blockchain technology for copyright protection. *Tencent Cloud* uses blockchain technology to launch the *Zhixin Chain* to protect original content protection. *Byte Dance*'s *Tuchong* cooperates with *Ant Blockchain* which is affiliated with *Ant Financial*. Currently, *Tuchong* becomes the leading platform based on blockchain for the identification and ownership of photographers and the copyright of original works can be checked on the chain. Significantly, it is also extremely important to ensure that the recorded user on the blockchain is matched with the actual identity. Song et al. proposed a new method of secure alignment with continued matrix identity information which can also be used for the protection of blockchain user identity [16]. Song et al. provided a solution based on identity authentication and also provided new ideas for research blockchain for copyright protection.

3 The proposed methods

3.1 Structure of zero-watermarking scheme

In the video copyright protection system, the blockchain network replaces the third-party notary of the traditional zero-watermarking algorithm and avoids the security issues existed in third-party notaries. Furthermore, excellent security control mechanisms exist in the blockchain. A brief description of the above steps and the scheme architecture is shown in Fig. 1. The video zero-watermarking is located in "off-chain" of the architecture. In this part, we will introduce the video zero-watermarking algorithm that works with blockchain for protecting copyright. To explaining the content of scheme, we suppose three figures called User A and User B to comprehend. Besides, it is worth noting that our blockchain is alliance chain in the field of copyright protection. In addition, if blockchain network can install on cloud platform, various application requests from User A and User B, which are regarded as a group of VM lists in the data centre, are submitted to the cloud platform [17, 18].

Registration is to obtain copyright certification. User A uploads a video and a colour image which is used for identification, then pre-process the video data and extract the key-frames by distance threshold clustering. Construct zero-watermarks on extracted key-frames. Zero-watermarks, information of key-frames and Key K_2, then package these data to Blockchain network through Blockchain SDK. In Blockchain network, the terminal constructs and signs the data package into a transaction, then the transaction is sent to the access peer in the blockchain network, and the access peer broadcasts the transaction after verification. After receiving the transaction, the peer verifies the transaction and composes the transaction into a block to be verified, then sends it to other peers for processing. Through the Smart Contract, the peers perform the transaction to generate an entity which contains the information need to be notarized and stored in the

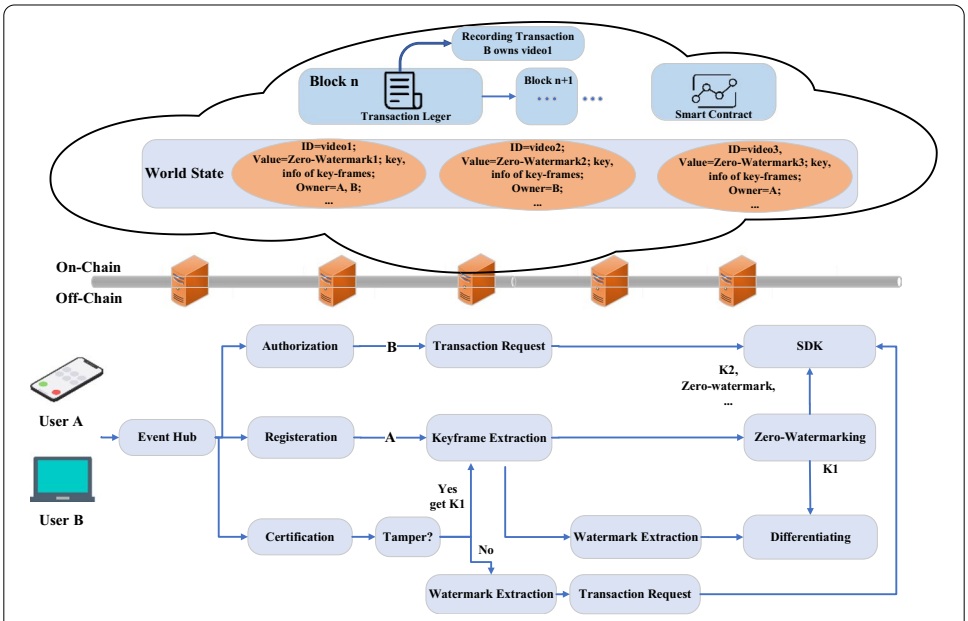

Fig. 1 Architecture of the protection system with blockchain, including two layers named "on-chain" and "off-chain"

Blockchain network. When more than two thirds of the peers reach a consensus on the result, the peer starts to generate blocks, then sends them to other peers in Blockchain network. After above steps, each peer will check the block height or block hash mapping and store a complete block. In other words, the registration content (zero-watermarks, information of key-frames and Key K_2) will store into World State in Blockchain network. Finally, the terminal returns the Key K_1 to User A.

Proposed scheme realizes the authorization of copyright through Blockchain. Compared with complicated operations through other solutions, the blockchain is specifically developed to solve the trading problems. The main processes of copyright transaction are as follows. User B sends a transaction for acquiring copyright to access peer, which is constructed and signed by terminal. The consensus peer receives and takes out a number of proposals from pool in order. After that, it will assemble them as consensus blocks and then send them to each peer for processing. After the peer receives the block, the transaction is taken out of the block and executed in order. Supposing User B would like to acquire video1's copyright, User B are added into the video1's owner by performing Smart Contract. After that, the peers exchange their execution results. When more than 2/3 of the peers get the same execution result, the peer will start to generate blocks and permanently storage the transaction and execution results to hard disk. In conclusion, the result of every copyright transaction is realized by the trusted blockchain.

The main processes for certification on video copyright are as follows. In order to verify copyright, User A needs to provide Key K_1 and the block hash to match other information on the blockchain to get the information of key-frames, zero-watermarks and Key K_2 on the chain. Perform the watermark extraction algorithm to return a colour watermark which can authenticate the identity. Moreover, User B can simply check copyright transaction on the Blockchain ledger when he completes the transaction to prove his successive copyright of the video1. If User B want to certify his copyright under video1 has been tampered, the proposed scheme will ask the User A to provide Key K_1 to decrypt and the rest processes are the same as above.

3.2 Key-frames extraction

Firstly, the main processes of key-frames extraction algorithm are inputting video samples and processing the video library. Secondly, unstructured dynamic video is converted into a static sequence of video frames. Thirdly, the processes are preliminary process of samples and extraction of feature vectors. Fourthly, the clustering is completed by calculating the inter-frame similarity and distance threshold according to the extracted feature vectors. Finally, the processes are judging key-frames according to the clustering results and outputting the extracted key-frames.

3.2.1 Feature extraction

Feature selection is very important to the expression of key-frames and the completion of effective clustering. Colour and texture features are common image features. At present, most of the key-frames extraction algorithms are based on clustering use colour histogram, but the feature of colour histogram cannot describe colour space distribution between adjacent pixels. As a local feature of an image, texture feature does not depend on colour and brightness. It not only reflects the grey level statistics

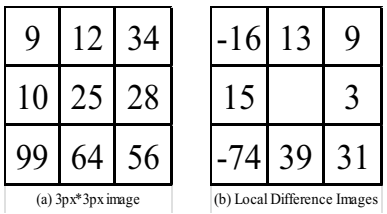

Fig. 2 Description of CLBP algorithm 1. The matrix of sampling block and its local difference are **a** and **b**

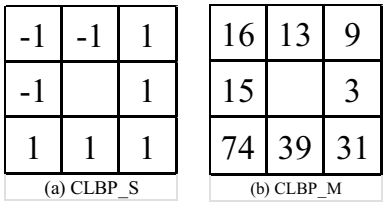

Fig. 3 Description of CLBP algorithm 2. Sign components and gradient components are **a** and **b**

of the image, but also reflects the spatial distribution information and structure information of the image. Its grey level invariability and rotation invariant can cleverly avoid experimental errors caused by significant changes in light. Therefore, in this paper, the completed LBP (CLBP) descriptor of the improved local binary patterns (LBP) is chosen to handle the texture features [19]. CLBP texture descriptor is an extended texture descriptor based on LBP descriptor, which can effectively describe the missing information of LBP type in order to obtain better performance of texture classification [20, 21].

Usually, given a central pixel and other P neighbourhood values, the local difference vector is expressed as $[d_0 \ldots\ldots d_{P-1}]$, $d_p = g_p - g_c$. s_p and m_p are the sign (positive or negative) and magnitude values of d_p using the local difference sign-separation-magnitude transform (LDSMT), respectively. The above content is shown as follows:

$$d_P = s_{p^*} m_p \quad \text{and} \quad \begin{cases} s_p = \text{sign}(d_P) \\ m_p = |d_p| \end{cases} \tag{1}$$

and

$$s_p = \begin{cases} 1, & d_p \geq 0 \\ -1, & d_p < 0 \end{cases} \tag{2}$$

The above formulas cannot be used directly as a descriptor because it is sensitive to light, rotation, noise, etc. The difference between the neighbouring pixels and the central pixel is divided into a sign component and a gradient component and is obtained by multiplying the two together, denoted as CLBP_S and CLBP_M.

For example, Fig. 2a is a sampling block which is size of 3×3, which can be divided into Fig. 3a, b, and its difference can be represented by Fig. 2b. Figure 3a is sign components, and Fig. 3b is gradient components. Actually, CLBP_S is the traditional LBP, and the two coding methods are the same. -1 in Fig. 3a is equal to 0 in

the traditional LBP. Furthermore, the CLBP_*S* is more capable of describing texture than the CLBP_*M*. Formula of CLBP_*S* is shown as follows:

$$\mathrm{CLBP\_}S_{P,R} = \sum_{P=0}^{P-1} s(s_p)2^p \tag{3}$$

and

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \tag{4}$$

It can be seen from Fig. 3b that CLBP_*M* is a continuous value. In order to harmonize the encoding with CLBP_*S*, it needs to be converted to binary encoding as well. Inspired by CLBP_*S*, this paper follows the following encoding for them, c is an adaptive threshold, and the value of c is taken as the mean value of m_p in the whole image. m_p is the absolute value accumulation of gradient differences between neighbourhood pixels and centre pixels (or the average of them, the final results of comparison are equal). Formula of CLBP_*M* is shown as follows:

$$\mathrm{CLBP\_}M_{P,R} = \sum_{p=0}^{p-1} t(m_p, c)2^p \tag{5}$$

and

$$t(x, c) = \begin{cases} 1, & x \geq c \\ 0, & x < c \end{cases} \tag{6}$$

The central pixel represents the local grey level and also contains the local grey level discriminant information. In order to effectively combine it with CLBP_*M* and CLBP_*S*, we carry out the following encoding:

$$\mathrm{CLBP\_}C_{P,R} = t(g_c, c_I) \tag{7}$$

and

$$t(x, c) = \begin{cases} 1, & x \geq c \\ 0, & x < c \end{cases} \tag{8}$$

In Eq. (7), g_c represents the centre pixel grey value, c_I represents the average grey value of the whole image. Binary encoding is performed by comparing the centre pixel and the average pixel value of the entire image.

The process of CLBP algorithm is shown in Fig. 4. After the above calculation, the three descriptors CLBP_*S*, CLBP_*M*, CLBP_*C* are all generated, which can be fused in the form of series, parallel or series–parallel histogram, and can achieve more effective rotation invariant classification ability than the traditional LBP.

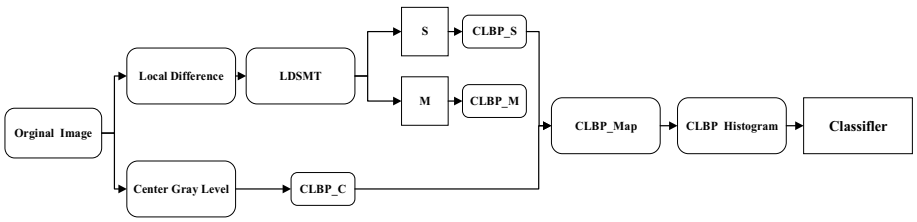

Fig. 4 CLBP algorithm. Original image is classed by CLBP

3.2.2 Inter-frame similarity and the distance threshold

Distance measurement is used to measure the distance between individuals in space. The greater the distance is, the greater the difference between individuals, and the lower the similarity between them. Chi-square distance is the most common measure to measure the difference between two individuals, and its calculation is simple. Therefore, in this paper, we use chi-square distance to represent the similarity between frames. The smaller the chi-square distance is, the higher the similarity between frames is. The chi-square distance between any two frames is defined as follows:

$$\mathrm{dist}(F_a, F_b) = \sum_{i=1}^{n} \frac{(F_a[i] - F_b[i])^2}{F_a[i] + F_b[i]} \tag{9}$$

In Eq. (9), $F_a[i]$ and $F_b[i]$ represent the values of image a and image b on the binary bit i. Respectively, n is the total number of video frame histogram bins, and $\mathrm{dist}(F_a, F_b)$ represents the inter-frame similarity.

The distance threshold directly affects the number of clusters, thereby affecting the extraction efficiency of key-frames. If the threshold is too small, it is easy to extract too many key-frames, resulting in information redundancy. If the threshold is too large, the extracted key-frames cannot represent the main content of the lens. According to the idea of data density sampling, the distance threshold is defined as follows:

$$d = \frac{2c}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \mathrm{dist}(F_i, F_j) \tag{10}$$

In Eq. (10), N is the total number of video frames, and $\frac{N(N-1)}{2}$ is the number of chi-square distances between two N frames. c is a constant. A large number of experiments show that the value of 0.25 in this algorithm is better. d is the distance threshold of clustering algorithm obtained by density sampling. By this method, different thresholds can be selected for different videos, which reflects the adaptability of the threshold. The threshold selected by this method will be small but not too small, and an appropriately small threshold can obtain more initial clustering, which is conducive to cluster centre merging and secondary clustering.

3.2.3 Description of clustering

All the steps of algorithm description are shown as follows in Algorithm 1. The first step is sampling the data set to determine the distance threshold d. The second steps are initialling clustering of data sets based on threshold and similarity, and determining the

initial number of clusters k and cluster centre set C. The third step is using K-means algorithm to optimize the initial clustering centre; then, we get new sets of clustering centre G. The fourth step is using the sequential clustering idea [22] to merge the closer classes in G; then, it can determine the final k and clustering centre set, so the clustering centre self-determination will complete.

The clustering algorithm process is shown in Algorithm 1. After clustering, we select all the nearest frames from the clustering centre to be the key-frames of the video.

Algorithm 1 Process of clustering algorithm

```
Input: Video
Output: The Final Cluster
  Extract the feature
  Select a feature vector
  d = Avg distance in N vectors
  for each feature vector do
     Calculate the distance
     repeat
        Remove the feature vector
     until Min (dist) ≥ 2 * d
     Features number = features number + 1
     Add feature vector to the cluster center set
  end for
  Initiate cluster center sets C and k
  for each G do
     repeat
        G = Clustering()
     until Min (dist) ≥ 2 * d
     Merge two clusters by sequential clustering
     Recalculate the cluster center
  end for
  Complete
```

3.3 Zero-watermarking for key-frames

After the digital image has been SVD [23–25], the corresponding orthogonal matrix represents the geometric structure of the image while the corresponding singular matrix represents the image luminance information. The real number field we define is R. Assuming the digital image matrix is A and $A \in R_{N\times N}$, then orthogonal matrix $U \in R_{N\times N}$, orthogonal matrix $V \in R_{N\times N}$ and diagonal matrix $S \in R_{N\times N}$. Therefore, A can be expressed as:

$$A = S \times U \times V^T \tag{11}$$

U is defined as the left orthogonal matrix and V is defined as the right orthogonal matrix. They satisfy the conditions respectively, which are $U \times U^T = 1, V = V^{-1}$. In that S:

$$S = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_r \end{pmatrix} \tag{12}$$

A special singular value in the S matrix is usually much larger than other singular values, which can represent the overall energy of A [26].

The Arnold Transform [27–29] can change the position of pixels and eliminate correlations between pixels or content in a host image, thus improving image security. The special Arnold Transform is the Simplest kind of Arnold Transform. The formula for operation of matrix is given as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mathrm{mod}(N) \tag{13}$$

The special Arnold Inverse Transform makes it easy to recover the transformed image. The formula for operation of matrix is given as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \mathrm{mod}(N) \tag{14}$$

(x', y') denotes the position of (x, y) at the pixel point after the transformation and N denotes the size of the image involved in the transformation.

3.3.1 Watermark generation

After using the key-frames extraction algorithm based on distance threshold clustering, a series of key-frames are selected from the video which represent the feature information of the whole video. The zero-watermarking algorithm is extracting the feature information of these key-frames and embedding the feature information into the watermark later. The detailed steps are as following Algorithm 2.

Algorithm 2 Process of watermark generation

Require: key frame I size of $M \times N \times 3$; watermark image I' size of $m \times n \times 3$; disordering key is Key key_1; disordering key is Key key_2;

Ensure: zero watermark;

I_k = RGB decomposition(I)

for each $k \in \{R, G, B\}$ **do**

$B_{i,j} = \frac{I_k{}^{M \times N}}{A \times B}, k \in \{R, G, B\}$;

$B_{i,j}$ = Arnold Transform$(B_{i,j}, key_1)$;

$cA_{i,j} = NSCT(B_{i,j})$;

$cB_{m,n} = \frac{cA_{i,j}}{8 \times 8}$;

$[U_{i,j}, S_{i,j}, V_{i,j}] = SVD(cA_{i,j})$;

Get characteristic matrixes X_k

I'_k = RGB decomposition(I');

for each $k \in \{R, G, B\}$ **do**

W'_k = Arnold Transform(I'_k, key_2);

$L'_k, H'_k = NSCT(W'_k)$;

$Z_{KH} = \mathbf{XOR}\ (X_k, H'_K)$;

$Z_{KL} = \mathbf{XOR}\ (X_k, L'_K)$;

$Z_{KH} + Z_{KL} = Z_K$;

$Z_{R,G,B} = Z_R + Z_G + Z_B$;

Complete

3.3.2 Watermark extraction

The extraction method is organized as following Algorithm 3.

Algorithm 3 Process of watermark generation

Require: key frame I size of $M \times N \times 3$; zero-watermark image I'' size of $m \times n \times 3$; disordering key is Key key_1; disordering key is Key key_2;
Ensure: watermark image;
I_k = RGB decomposition(I)
for each $k \in \{R, G, B\}$ **do**
$B_{i,j} = \frac{I_k{}^{M \times N}}{A \times B}, k \in \{R, G, B\}$;
$B_{i,j}$ = Arnold Transform$(B_{i,j}$, $key_1)$;
$cA_{i,j} = NSCT(B_{i,j})$;
$cB_{m,n} = \frac{cA_{i,j}}{8 \times 8}$;
$[U_{i,j}, S_{i,j}, V_{i,j}] = SVD(cA_{i,j})$;
Get characteristic matrixes X'_k
I''_k = RGB decomposition(I');
for each $k \in \{R, G, B\}$ **do**
$L''_k, H''_k = NSCT(W'_k)$;
$V'_{KH} =$ **XOR** (X'_k, H''_K);
$V'_{KL} =$ **XOR** (X'_k, L''_K);
$V'_{KH} + V'_{KL} = V'_K$;
Z'_k = Arnold Inverse Transform(V'_k);
$Z'_{R,G,B} = Z'_R + Z'_G + Z'_B$;
Complete

4 Results

In this section, we conduct tests on the three parts of the proposed scheme, which are blockchain system, key-frames extraction algorithm based on distance threshold clustering and zero-watermarking algorithm for key-frames based on NSCT-SVD.

The purpose of testing blockchain system is to actually explore whether the performance poor blockchain can be applied to the protection for video copyright. Furthermore, it is worth emphasizing that video zero-watermarking consists of key-frames extraction algorithm and zero-watermarking algorithm. Therefore, the purpose of testing efficiency key-frames extraction algorithm and zero-watermarking algorithm is to verify the process of extracting the features on key-frames in the video and obtained zero-watermark which was recorded on blockchain is robust and secure. It is worth noting that we choose FISCO BCOS for testing because the structural design of FISCO BCOS focuses on layering business into on-chain and off-chain. It is in line with our proposed scheme.

4.1 Experiment deployment

The hardware configuration of the whole experiments is shown in Table 1, and the software configuration of the whole experiments is shown in Table 2.

In process of simulating the key-frames extraction algorithm, we choose videos with unequal length to test the actual effect of the key-frames extraction algorithm, which are *Landscapes*, *Advertisement*, *Animation clips* and *News*, respectively. The experimental protocols were approved by the Animal Care and Protection Committee of Hainan University.

Table 1 Hardware configuration

Environmental parameters	Config
CPU	Intel i7, 2.4 GHz
GPU	GTX1080 Ti 11 GB
RAM	16 GB
Mainboard	Z270-AR
Hard disk	500 GB SSD + 2T HDD

Table 2 Software configuration

Environmental parameters	Config
OS	Windows 10
Host environment	Ubuntu 18.04, 64bit
Database	MySQL 8.0.18
Blockchain platforms	FISCO BCOS
Python	3.7.4
MATLAB	R2019b

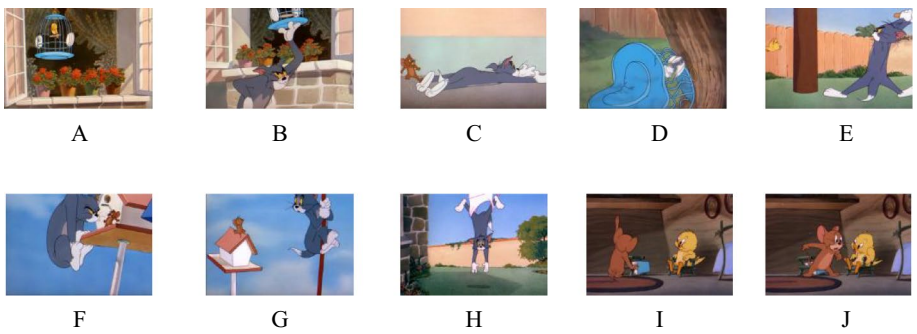

Fig. 5 Key-frames. **A**–**J** Results of extraction by proposed Key-frames extraction methods

4.2 Video zero-watermarking

4.2.1 Key-frames extraction

First of all, the key-frame proposed in this paper is defined as a computer animation term, which refers to the frame where the action of the character or object changes, which is equivalent to the film of an old-fashioned movie. Clustering algorithm is a very effective technique which is widely used in pattern recognition, speech analysis and information retrieval. Shot clustering is to study the relationship between shots, that is, how to combine shots with similar content. The frame sequence in the shot is divided into each cluster by shot clustering, and then the video key-frames are selected. The key-frames extracted by this technology can well reflect the main content of the video. The extracted frames are shown in Fig. 5.

To ensure the feasibility of extracting key-frames, we set 0.9 as the threshold of NC for initial screening. If the threshold value is less than 0.9, the image is reserved, and the

Table 3 Video key-frames NC to show similarity between frames

NC	A	B	C	D	E	F	G	H	I	J
A	1.00	0.8855	0.8513	0.8307	0.8416	0.8152	0.8510	0.7213	0.7988	0.7955
B	0.8855	1.00	0.8657	0.8456	0.8539	0.8113	0.8916	0.7721	0.7956	0.8326
C	0.8513	0.8657	1.00	0.8478	0.7568	0.8234	0.8123	0.7885	0.8012	0.8156
D	0.8307	0.8456	0.8478	1.00	0.8741	0.8601	0.869	0.8494	0.8405	0.837
E	0.8416	0.8539	0.7568	0.8741	1.00	0.8332	0.8356	0.8098	0.8185	0.8529
F	0.8512	0.8113	0.8234	0.8601	0.8332	1.00	0.8466	0.8272	0.8195	0.8089
G	0.8512	0.8916	0.8123	0.869	0.8356	0.8466	1.00	0.8375	0.8485	0.8351
H	0.7213	0.7221	0.7885	0.8494	0.8098	0.8272	0.8375	1.00	0.8123	0.8376
I	0.7988	0.7956	0.8012	0.8405	0.8185	0.8195	0.8485	0.8351	1.00	**0.9321**
J	0.7955	0.8326	0.8156	0.837	0.8529	0.8089	0.8351	0.8376	**0.9321**	1.00

Table 4 Experimental results of video key-frames extraction algorithm

	Cartoon	Advertisement	Animation clips	News
Total frames	100	1254	15,324	26,987
CF	15	135	735	1452
DF	3	7	52	182
P/%	83.33	95.07	93.39	88.86

image greater than 0.9 is deleted. The calculation results are shown in Table 3. The NC between Fig. 5I and J reaches greater than 0.9 so that one of the two frames should be deleted. The NC has been highlightened and bolded in Table 3.

Figure 5G, J were removed, and the remaining images were retained as key-frames through the initial extraction. The zero-watermarking algorithm we proposed is to construct a zero-watermark based on the extracted key-frames. So, this part tests the effectiveness of video key-frames extraction algorithm which is based on *K*-means clustering algorithm.

This part of experiment has the following definitions: Precision ratio is denoted as *P*. Correctly detection is CF. False detection is DF. *P* is calculated as follows:

$$P = \frac{\mathrm{CF}}{\mathrm{CF} + \mathrm{DF}} \tag{15}$$

The experimental results are shown in Table 4.

4.2.2 Analysis on zero-watermarking algorithm

To prove the false alarm and robustness of proposed zero-watermarking algorithm, five images are selected to replace key-frames in experiments, which are Fig. 6A–E. Figure 6F is defined as copyright watermark in experiment. In Fig. 7, there is an example of generated zero-watermark.

(1) False alarm

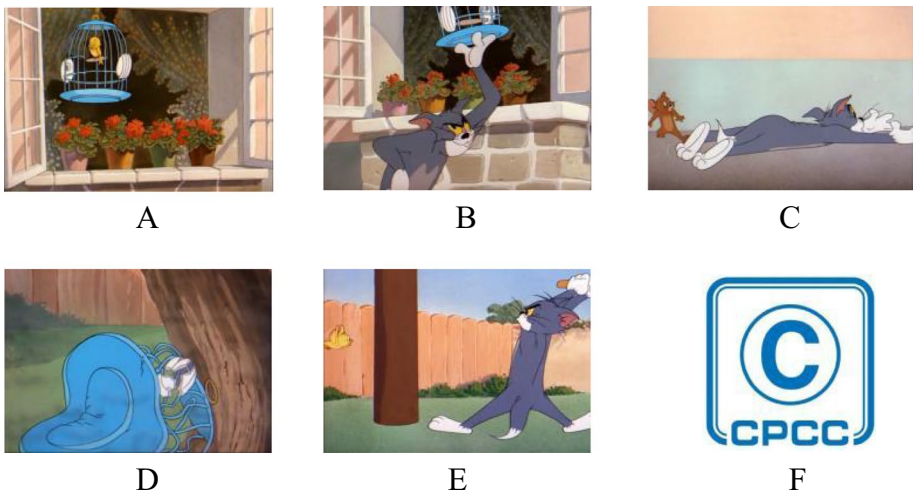

Fig. 6 Images and copyright watermark. Five images (**A**–**F**) are selected to replace key-frames in experiment

Fig. 7 Zero-watermark after extraction. An example to show the result of zero-watermarking

Table 5 NC of zero-watermark between different images

Host image	A	B	C	D	E
A	1.00	0.8855	0.8513	0.8307	0.8416
B	0.8855	1.00	0.8657	0.8456	0.8539
C	0.8513	0.8657	1.00	0.8478	0.7568
D	0.8307	0.8456	0.8478	1.00	0.8741
E	0.8416	0.8539	0.7568	0.8741	1.00

The experiment content is as follows. In this experiment, we use the five images which are Fig. 6A–E to generate the corresponding zero-watermark with the copyright watermark, and then calculate normalized correlation (NC) between the five zero-watermarks. NC value reflects false alarm rate. The experimental results are shown in Table 5.

(2) Robustness

In this part, we discuss robustness on the proposed zero-watermarking algorithm in this paper from six parts which are affine, rescale, median filtering, noise attack, rotation, Gaussian filtering.

Before attacking test on the proposed zero-watermarking, we select Fig. 6A as a subject to compare traditional DWT-SVD and NSCT-SVD in resisting conventional attacks, and the similarity of copyright watermark extracted after attacks is cal-

Table 6 Comparation between DWT-SVD and NSCT-SVD

Attack types	DWT-SVD [30]	NSCT-SVD
Affine (Y-shearing 0.01)	0.9669	0.9879
Rescale (200%)	0.9643	0.9785
Median filtering (5 * 5)	0.9712	0.9987
Noise attack (10%)	0.9209	0.9557
Rotation (0.75)	0.9481	0.9676
Gaussian filtering (0.01)	0.9321	0.9757

Table 7 Robustness test

Attack		NC		NC		NC
Zero-watermark						
Gaussian Filtering (0.01)		0.9757		0.976		0.9722
Gaussian Filtering (0.03)		0.9671		0.9671		0.9624
Rotation (1°)		0.9191		0.9195		0.9206
Noise attack (5%)		0.9781		0.9876		0.9866
Noise attack (10%)		0.9557		0.9514		0.9502
Median filtering (3*3)		0.9987		0.9986		0.9974
Median filtering (5*5)		0.9983		0.9981		0.9968
Rescale (200%)		0.9987		0.9985		0.9975
Rescale (50%)		0.987		0.991		0.985
Affine (X-shearing 0.01)		0.9745		0.9742		0.9737

culated. According to Table 6, NSCT-SVD has greater superiorities under noise attacks, filtering attacks than DWT-SVD [30].

Afterwards, we test the robustness of the zero-watermarking algorithm for key-frames under affine, rescale, median filtering, noise attack, rotation, Gaussian filtering. The results are shown in Table 7.

(3) Security

In this subsection, we carry out three comparative experiments to verify the security by Arnold transform. In Table 8, the zero-watermark (A) is obtained by adding Fig. 6E, F, and watermark is correctly extracted by right secret Keys. (B) in Table 8

Table 8 Security test of zero-watermarking, A, B, C and D are experimental results.

	A	B	C	D
Images				

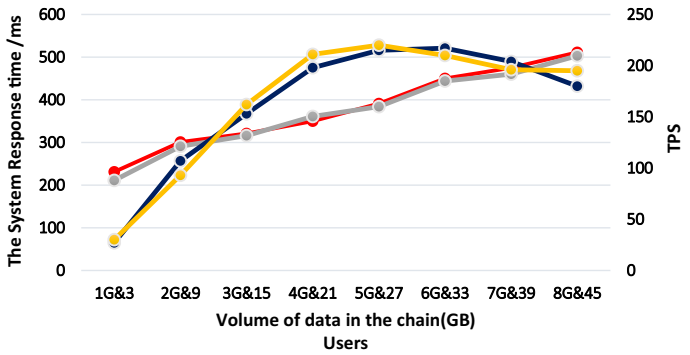

Fig. 8 Response time and throughput. The red and grey curves show the relationship between the data volume of on-chain traceability information and the response time of the system for FISCO BCOS and Hyperledger Fabric, respectively. The blue curve depicts the TPS variation curve for FISCO BCOS as the number of users increases, and the yellow curve is the TPS variation curve for fabric

is extracted by wrong Keys. (C) in Table 8 is extracted by wrong scrambling rounds. (D) in Table 8 is extracted by wrong Keys and scrambling rounds.

4.3 Blockchain system

To verify the usability of combining blockchain applications with zero-watermark storage, this section tests the response time and TPS of the FISCO BCOS and fabric blockchain systems to represent their actual efficiency and to illustrate the feasibility and reasonableness of combining the systems with blockchain.

The response time of a blockchain system is one of the most important indicators of the system's performance. The main functions of the blockchain system in this proposal are on-chain data storage and on-chain data traceability. Therefore, the amount of data in the on-chain traceability information is key to the response time of the system. The red and grey curves in Fig. 8 show the relationship between the data volume of on-chain traceability information and the response time of the system for FISCO BCOS and fabric, respectively. As the data on the chain increases from 1G to 8G, the FISCO BCOS system response time increases from 231 to 511 ms and the fabric system response time increases from 211 to 503 ms. we also conducted performance tests using multiple threads, using each thread to simulate a user (client) with the blockchain for multiple sets of tests. Six users were added to each set of tests and experimental data such as response time and number of requests were recorded to calculate the system throughput under different loads. Server memory, CPU utilization, network, disk read/write and

other resource usage are also monitored. The tests are not stopped until the TPS (transactions per second, concurrency/average response time) reaches its peak. The results of the experiment are shown in Fig. 8. The blue curve depicts the TPS variation curve for FISCO BCOS as the number of users increases, and the yellow curve is the TPS variation curve for fabric. As can be seen, FISCO BCOS system does not peak until the number of users simulated is between 3 and 27, and stabilizes beyond 27, while performance starts to degrade when the number of users exceeds 36, while the fabric system performs in much the same way as FISCO BCOS in this test.

4.4 Analysis

From the experimental results in Table 4, it can be seen that key-frames extraction algorithm works well for various videos. Although a small number of missed detection and false detection exist, there is still a human factor to distinguish frames and we agree that the proposed algorithm has met expectations.

From the above experimental results on zero-watermarking algorithm, the proposed zero-watermarking algorithm in this paper can effectively avoid false alarm. Furthermore, our zero-watermark algorithm combined with NSCT-SVD is more robust than the traditional DWT-SVD method in zero-watermarking. Due to the combination of NSCT and SVD, the change in the low-frequency coefficients of each sub-block is small under noise attacks and filtering attacks. The results show that the algorithm is robust under noise attacks and filtering attacks. Due to the block processing when constructing the feature matrix and SVD of each sub-block, so that proposed zero-watermarking algorithm can effectively resist local cropping attack. From the above experimental results, it can be seen that as long as the Keys or scrambling rounds is incorrectly, the correct watermark cannot be obtained, which fully verifies the security of Arnold Transform in proposed zero-watermarking algorithm.

According to the experimental results on blockchain system, the delay of the blockchain system is within range of technical standards of the blockchain industry. Assuming the zero-watermark is 50 kB, the data volume of the 18 min short video on the chain is 71 MB. When the amount of data on the chain increases to 80 GB, the system can register 18 min videos about 1153, while the response time of the blockchain system is still a few seconds. In the process of testing TPS, the utilization rate of each hardware was below 100%. After comparison and inspection, it may be caused by the performance limitation of FISCO BCOS. The experimental results show that the TPS of the blockchain system is about 216, which not only meets the performance indicators of the blockchain network, but also meets the needs of the video copyright protection scheme.

5 Discussion

Before discussing the proposed video zero-watermarking algorithm, we compare the traditional blind watermarking algorithm with zero-watermarking algorithm. The traditional blind watermarking scheme is embedding the features of watermark into key-frames. The zero-watermarking algorithm is embedding the features of key-frames into the watermark to generate zero-watermark. Copyright protection is realized by registering zero-watermark with features of key-frames. From the perspective of visual quality,

the traditional blind watermarking is embedding the watermark into the key-frames, so key-frames in the video will inevitably produce noise. However, zero-watermarking will not take actions on key-frames so that it will not influence video quality. From the perspective of security, the traditional blind watermark is easy to be detected and destroyed, even erased. However, the zero-watermarking is encrypted and stored in a trusted third-party, which makes it difficult for attackers to know where to begin.

In the proposed zero-watermarking algorithm, a colour video will generate many zero-watermarks from extracted key-frames. The zero-watermarks generated by multiple key-frames can effectively resist malicious clipping of key-frames in the actual state of secondary creation and prevent key-frames being clipped to extract effective feature matrices, so as to get the copyright watermarks. By this way, even if the key-frames are clipped, watermarks which are extracted still recognize. Besides, there are twice blocking in the generation of feature matrices which belongs to the proposed zero-watermarking algorithm. The first processing is before NSCT. When the colour video is attacked by cropping attack, the coefficients after NSCT can be independent of each other. The second processing makes the subsequent SVD more stable. In addition, the decomposition of RGB in this algorithm enhances security of the system, because the three zero-watermarks are required to extract a colour watermark, and the decomposition of RGB achieves a triple encryption logically with Arnold Transform. Above all, the fundamental feature of the zero-watermarking algorithm is that copyright protection is realized without any modification of the video. This zero-watermarking algorithm generates Key K_1, which will be kept by the owner of video copyright. Key K_2 can be uploaded to the blockchain network. In process of copyright certification, the user provides the Key K_1 to match the key pairs (K_1, K_2) so as to extract copyright watermarks from zero-watermarks on the blockchain.

The system applied in the field of video copyright protection have high demand for data security, so access control of data on the alliance chain is required, whose strategy is mainly divided into the following two aspects:

- Access control of communication data on the chain is accomplished through peer certificates and SSL (Secure Socket Layer).
- In the access control of peer storage data, the blockchain uses disk encryption, which is performed within the institution. In the institution's intranet, each institution independently encrypts the peer's rigid disk data. When the rigid disk of the machine is away from the institution and the peer is allowed to start up on a network outside the institution's intranet. The rigid disk data will not be decrypted and the peer will not be able to start up and thus steal the data on the federated chain.

In addition, the data on the chain (the colour zero-watermark) have been scrambled. Even if being accessed, no valuable information can be obtained. Copyright rights transactions will only be done on the blockchain network without any further manipulation on the video. This way is more efficient than traditional methods. For example, all permission transactions and permission ownership information will be recorded on the blockchain network and be protected from malicious tampering.

Thus, the malicious user uses and reproduces a video illegally, a legally valid proof will be found through fast traceability in the video copyright protection system.

6 Conclusions

The proposed scheme is mainly used to solve poor robustness, weak imperceptibility and difficulty in traceability of the current watermarking scheme and others.

In this proposed scheme, apparently, the main innovation is combination of "zero" and blockchain. "Zero" means that there is no operation on the original video. The proposed scheme will not add information to key-frames so that there is no need to consider the detection and erasure of traditional watermarks. The process of authentication and copyright traceability relies on the blockchain, so that the blockchain combined with the zero-watermarking solves the problem of rights traceability and realizes non-tampering storage. In addition, compared with the existing blockchain scheme based on video fingerprinting, the zero-watermark directly links to the video frame. In other words, the proposed scheme can protect the copyright of video information than the video fingerprinting, and the video information can be seen as visual content.

Abbreviations

NSCT: Non-Subsampled Contourlet Transform; CNN: Convolutional neural network; SDK: Software Development Kit; PSNR: Peak signal-to-noise ratio; SVD: Singular value decomposition; DCT: The discrete cosine transforms; QPHFMs: Quaternion polar harmonic Fourier moments; HEVC: High Efficiency Video Coding; NC: Normalized correlation; LDSMT: Local difference sign-separation-magnitude transform; LBP: Local binary patterns; CLBP: Completed LBP; TPS: Transaction Per Second, number of concurrent/average response time; NSP: Non-subsampled Pyramid; NSDFB: Non-subsampled Directional Filter Bank; SSL: Secure Socket Layer.

Acknowledgements

We sincerely thank the Reviewers and the Editor for their valuable suggestions.

Authors' contributions

XW designed the experimental algorithm and verified and tested it. PM helped design and edit the experimental algorithms. ZJ and YW were responsible for writing and collecting materials. WO and WH provided financial support and technical support. All authors read and approved the final manuscript.

Funding

This work was supported in part by the Hainan Provincial Natural Science Foundation of China (621RC508), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A16), the Science Project of Hainan University (KYQD(ZR)-21075).

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Cyber Security (School of Cryptology), Hainan University, 58 Renmin Avenue, Meilan District, Haikou 570228, China. [2]School of Information and Communication Engineering, Hainan University, 58 Renmin Avenue, Meilan District, Haikou 570228, China. [3]School of Computer Science and Technology, Hainan University, 58 Renmin Avenue, Meilan District, Haikou 570228, China.

Received: 17 June 2021 Accepted: 17 January 2022
Published online: 21 March 2022

References

1. M. Xuan, *H. 264/AVC Video Integrity Authentication Key Technology Research* (Hefei University of Technology, Hefei, 2011)

2. H. Meng, *Research on Video Encryption Technology Based on H. 264 Coding Standard* (North University of China, Taiyuan, 2020)
3. X. Liu, An overview of video digital watermarking technology. Televis. Technol. **44**, 11–15 (2020)
4. H. Gao, C. Liu, Y. Yin, Y. Xu, Y. Li, A hybrid approach to trust node assessment and management for VANETs cooperative data communication: historical interaction perspective. IEEE Trans. Intell. Transport. Syst. (2021). https://doi.org/10.1109/TITS.2021.3129458
5. W. Wang et al., Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Trans. Industr. Info. (2021). https://doi.org/10.1109/TII.2021.3084753
6. H. Gao, C. Liu, Y. Li, X. Yang, V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability. IEEE Trans. Intel. Trans Syst. **22**(6), 3533–3546 (2021)
7. F. He, Digital watermarking and its anti-compression robustness test based on wavelet domain. Autom. Inf. Eng. **44**, 42–44, 50 (2020)
8. Y. Li, D. Wei, L. Zhang, Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. Inf. Sci. **551**, 205–227 (2020)
9. Q. Wen et al., Concept and application of zero-watermarking. J. Electron. **2**, 214–216 (2003)
10. C. Wang et al., Stereo image zero-watermarking algorithm based on ternary polar harmonic Fourier moments and chaotic mapping. Inf. Sci. **48**, 78–99 (2018)
11. H. Xue et al., A zero-watermarking algorithm based on NSST and Hessenberg decomposition. Modern Comput. **89–93**, 103 (2020)
12. A. Amiri, S. Mirzakuchaki, A digital watermarking method based on NSCT transform and hybrid evolutionary algorithms with neural networks. SN Appl. Sci. **2**, 1–15 (2020)
13. A. Nagaska, Automatic video indexing and full-video search for object appearances, in *Proceedings of IFIP 2nd Working Conference Visual Database System* (1992)
14. R. Hannane et al., An efficient method for video shot boundary detection and keyframe extraction using SIFT-point distribution histogram. Int. J. Multimed. Inf. Retrieval **5**, 89–104 (2016)
15. T. Barbier, R. Goularte, KS-SIFT, a keyframe extraction method based on local features, in *2014 Proceedings of IEEE International Symposium on Multimedia Washing on DC, IEEE Computer Society* (IEEE, 2015), pp. 13–17
16. J. Song, Z. Han, W. Wang, J. Chen, Y. Liu, A new secure arrangement for privacy-preserving data collection. Comput. Standards Interfaces **80**, 103582 (2022)
17. Y. Huang, H. Xu, H. Gao, X. Ma, W. Hussain, SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center. IEEE Trans. Green Commun. Netw. **5**, 670–681 (2021). https://doi.org/10.1109/TGCN.2021.3067374
18. X. Ma, H. Xu, H. Gao, M. Bian, Real-time multiple-workflow scheduling in cloud environments. IEEE Trans. Netw. Serv. Manag. **18**, 4002–4018 (2021). https://doi.org/10.1109/TNSM.2021.3125395
19. Q. Kou, D. Cheng, W. Yu, H. Li, Texture target classification integrating CLBP and local geometric features. Opto-Electron. Eng. Photoelectr. Eng. **46**, 180604–1 (2019)
20. S. Xu, Texture descriptors for spatial statistical features based on LBP values. Pattern Recognit. Artif. Intell. **26**, 769–776 (2013)
21. J. Yang, Research on undersampling methods based on data density distribution. Comput. Appl. Res. **33**, 2997–3000 (2016)
22. J. Liu, W. Zhao, H. Zhu, *Pattern Recognition: Pattern Recognition* (Harbin Institute of Technology Press, Harbin, 2014)
23. S. Deng, Robust watermarking algorithm for wavelet transform and singular value decomposition. Laser J. **36**, 86–89 (2015)
24. L. Guo, F. Liu, S. Li, J. Pang, Fingerprint watermarking authentication algorithm based on SM2 and singular value decomposition (SVD). J. Beijing Inst. Print. **27**, 46–50 (2019)
25. X. Hao, G. Peng, Video summarization based on SVD and sparse subspace clustering. J. Comput. Aided Des. Graph. **29**, 485–492 (2017)
26. Z. Xiao, H. Zhang, H. Cheng, T. Gao, Enhanced singular value decomposition and cellular neural networks for zero-watermarking. Chin. J. Graph. Graph. **3**, 1144–1148 + 1153 (2017)
27. L. Wang, X. Zhang, C. He, Digital watermarking algorithm in wavelet domain based on Arnold scrambling and logistic chaotic encryption. Inf. Technol. **11**, 49–53 + 58 (2018)
28. Y. Chen, Research on colour image encryption algorithm based on chaotic random blocking and Arnold transform. Digit. Technol. Appl. **37**, 135–137 (2019)
29. L. Wu, J. Zhang et al., Arnold transform and its inverse transform. Microcomput. Inf. **26**, 206–208 (2010)
30. P. Kadian, N. Arora, S.M. Arora, Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD, in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)* (2019), pp. 987–991. https://doi.org/10.1109/SPIN.2019.8711681

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.