Zhaofeng et al. EURASIP Journal on Image and Video Processing (2018) 2018:91
https://doi.org/10.1186/s13640-018-0327-1

EURASIP Journal on Image and Video Processing

RESEARCH Open Access

A new blockchain-based trusted DRM scheme for built-in content protection

Ma Zhaofeng[1*], Huang Weihua[2] and Gao Hongmin[1]

Abstract

With the development of Internet technology, transmitting, editing and misusing the digital multimedia bring great challenges in misusing detection for multimedia content protection. In this paper we proposed an artwork image digital rights management scheme for Internet misusing detection based on watermark and blockchain with robustness and high-level security. We embed artwork right information such as author, RightHolder, Date and Location information into the artwork image data. In the scheme, we use image Arnold transform to enhance the security and use image DCT coefficients of middle frequency to embed watermark for robustness. In the transparence of watermark, HVS and Watson models are used to control the watermark strength, which can enhance the invisibility. Once the suspicious image data from Internet are misused and spreading the image data on Internet without authorization, especially the high value artwork image data, we can trace the misuse responsibility by extracting the watermark. And according to the above algorithm, we implemented the scheme as DRMChain based on the consortium blockchain which stored the artwork and DRM information in an un-tampered ledger for decentralized rights confirmation. Large amount of experiments indicate the proposed watermark-based trusted blockchain DRM scheme is secure, robust, and for the protection and misuse detection of image data.

Keywords: Digital rights management (DRM), Watermark, Blockchain, Misusing detection

1 Introduction

The snaking of piracy has brought incalculable losses to the image creators, which is particularly prominent in areas such as news, design, photography, and e-commerce. However, due to the fact that the image itself is difficult to identify with embezzlement, and it takes a long time to legal proceedings, the actual cost of the infringement is often chosen by the victim, which also contributes to the proliferation of piracy.

In recent years, with the ever-increasing awareness of copyright protection at the national, social, and individual levels, the protection of copyrights such as videos, music, and literature has taken a big step forward. However, due to some characteristics of the picture itself, the copyright protection process has progressed slowly. Whether online or offline, the content of the picture is indispensable, the value of the picture is increasingly prominent, and the protection of the copyright of the picture becomes inevitable. The report of 2017 China Network Copyright Industry Development Report shows the industry scale of China's core network copyright industry exceeded 500 billion yuan, with a high growth rate of 31.3% year-on-year. Compared with the protection of copyrights such as videos and music, the protection of copyright of picture is currently less concerned, and people's awareness of copyright is also relatively weak. In order to solve the current market infringement of such image infringement, researchers hope to solve the current situation of difficulty in defending rights through the technical, so that the original author can be traced by labelling their own work and engraving imprinted. Blind watermark is a kind of image watermark technology, which can hide digital info in the picture. The processed image does not seem to change, but in fact, the image already has its unique identifier. No matter whether it is cropped, pasted, rotated, zoomed, or added with text or filters, the

* Correspondence: mzf@bupt.edu.cn
[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
Full list of author information is available at the end of the article

content of the watermark will be affected in some degree. This enables copyright protection and tracking without damaging the original work and being unnoticed.

Digital watermarking [1, 2] is a technique of using multimedia digital information such as images as a data carrier to embed copyright information, which can be visible or invisible. When a digital product copyright dispute occurs, the information in the data carrier can be extracted and verify the ownership of the copyright. Digital watermarking system generally includes two stages: watermark embedding and extracting. The indicators of evaluating the quality of the watermark system mainly include concealment, watermark capacity, robustness, and security [3].

From the perspective of the robustness of watermark resisting attacks, digital watermarking techniques can be divided into three types: robust, fragile, and semi-fragile [4–7]. Robust watermarks can be used against most image processing operations and be suitable for copyright and ownership verification, while fragile watermarks are sensitive to subtle modifications and are best suitable for authentication and integrity. According to the different fields of the hidden watermark, there are mainly two types: spatial domain watermarks and transform domain watermarks. Among them, the spatial domain-watermarking algorithm hides the watermark information by directly modifying the original signal. Although the watermark hiding and extraction process is simple, the robustness is not as good as the transform domain watermark. Therefore, in recent years, transform domain watermarking has attracted more attention. The watermarking algorithm based on discrete cosine transfer (DCT) has been widely used, and various watermarking algorithms based on discrete wavelet transfer (DWT) are the focus of current research, but these transform domain-watermarking algorithms are also facing the following challenges in research: (1) the watermarking algorithm based on DCT [8] has good compatibility with the commonly used image international compression standard. Therefore, this kind of algorithm can make full use of the characteristics of the compressed domain to hide the watermark information. However, such algorithms often choose the intermediate frequency coefficient to compromise the concealment and robustness of the watermark information, so it is difficult to resist the image processing attacks such as filtering and adding noise. (2) The watermarking algorithm based on DWT [9] can balance the characteristic of the watermark signal in the time domain and the frequency domain and can realize the fine analysis of different scales through the translation and zoom operations, so the characteristics of the signal can be extracted more effectively. The coefficients of the high-frequency sub-band obtained after wavelet analysis are mostly zero. If the watermark information is hidden in the high frequency, the high-frequency coefficient needs to be strictly selected. Compared with hidden low-frequency watermarks, hidden high-frequency watermarks have better resistance to geometric attacks, but they are not effective against low-pass filtering and JPEG lossy compression.

In [10], genetic algorithm optimization principles are employed and the strength of the watermark is controlled locally and according to the visual properties. The scheme is invisible to the human eyes and robust to a wide variety of common attacks. The disadvantage of this algorithm is that it is slow and not suited for real-time applications. A blind and highly robust watermarking scheme method for ownership verification and copyright protection has been presented in [11]. Watermarking is performed using principal component analysis (PCA) and Laplacian pyramid in contourlet transform. Wherever, it offers low payload. In [12], a novel blind watermarking algorithm is proposed. The algorithm is performed in DCT domain, using the correlation between two DCT coefficients of adjacent blocks in the same position. The watermarking algorithm is tested for some attacks, including JPEG compression, cropping, rotation, contrast enhancement, brightening, and sharpening. The disadvantage of this algorithm is that it is unable to embed a watermark bit in all the blocks, resulting in low capacity. In order to improve the payload capacity, all the blocks are used for the embedding purpose in [13]. The robustness of the proposed scheme has been examined for various singular and hybrid attacks, and a watermark of good quality is extracted even after various simultaneous attacks on the system.

Considering for copyright protection, DRM misusing detection, data authentication, and digital content tracking for illegal distribution, the watermarks should be secure. And then numerous encryption methods have been used to improve security and confidentiality of watermarks.

A chaotic encryption-based blind digital image watermarking technique applicable to both grayscale and color images has been presented in [14]. The watermark bit is embedded by modifying the difference between DCT coefficients of adjacent blocks. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. A new digital image watermarking model based on scrambling algorithm logistic and RSA asymmetric encryption algorithm has been presented in [15]. The scheme performed the hybrid decomposition of DWT and SVD on the host image, and the watermark is

embedded into the low-frequency sub-band of the host. In [16], a novel chaos-based image encryption scheme using nonlinear inter-pixel computing and swapping-based permutation approach is presented. Simulation results demonstrate the high level of security for practical secret applications, but payload and imperceptivity have not been discussed in the paper. In [17], the watermarking image is encrypted by logistic map to enhance its confidentiality. The authors choose the region of interest of host image, and the experimental results show that the scheme does well against common attacks and geometric attacks. Although the scheme is secure to some degree, the imperceptivity and payload are not very good. In [18], the authors provide a promising solution to the security of watermarking. The watermark algorithm is performed in the encrypted domain, which means that the algorithm protects the original images from the third party embedders. The hybrid DCT and DWT methods are used to improve the robust performance of the scheme. Experiments demonstrate that the entire performance is satisfactory.

Recently, the improvement of DRM based on watermarking basically focused on algorithms. A new design scheme of DRM based on watermarking and blockchain is proposed in [19]. Blockchain is used to store watermark securely and provides timestamp authentication for multiple watermarks. Multiple watermarks and combine blockchain can prove the scheme which could improve copyright protection of multiple creations.

To address the abovementioned issues, we attempted to improve the security of watermarks based on ensuring high robustness. So we proposed a new image watermarking and blockchain scheme for DRM based on Arnold, human vision system (HVS), and DCT. The rest of this paper is organized as follows. In Section 2, we discuss the principle of Arnold, HVS, and DCT. In Section 3, the components of this DRM scheme based on digital watermarking are introduced, including watermark embedding and extracting processes. In Section 4, the simulation of this scheme is presented. In Section 5, we implemented the artwork DRM scheme and gave the blockchain data instance.

2 Preliminaries

In order to solve the problem of digital rights management misusing detection for multimedia content protection, we proposed a new watermarking scheme based on DCT transform domain. In the DCT watermarking algorithm, we embed watermark information into the low- and intermediate-frequency coefficients of the original digital image DCT transform domain. Firstly, after quantization process, watermark algorithm can enhance the ability of watermark information to resist compression attacks. Secondly, the coefficients in the DCT transform domain have the characteristics of the statistical distribution mathematical model. In theory, we can estimate the amount of the embedded watermark information. Thirdly, digital image watermarking through DCT transform will be dispersed into the whole image when doing the inverse DCT, so the embedded watermark information will not affect the compression, cutting, modification, and other attacks of the image. Therefore, the watermark based on DCT domain has high robustness and invisibility.

2.1 Security encryption

In order to enhance the robustness and security of the watermark, before embedding the watermark into the digital image, we first use the Arnold scrambling encryption algorithm to preprocess the watermark. Arnold transform is an encryption technique based on the combination of pixel displacement and matrix transformation, which can be encrypted by changing the position or gray value of pixels, so that even if the attacker extracts the watermark, the original watermark image cannot be obtained if the encryption method or encryption key is not known.

2.1.1 Two-dimensional Arnold transform

Two-dimensional Arnold transform is a commonly used transformation method. The Arnold transform formula of two-dimensional signal $N \times N$ is defined as follows:

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \bmod(N) \tag{1}$$

where $y \in (0, 1, 2, \ldots, N-1)$, (x_1, y_1) indicates the coordinates of a pixel point in the original matrix. (x_2, y_2) indicates the coordinates of the pixel after transforming. Inverse Arnold transform is used to decrypt the Arnold encryption message by using Eq. (2).

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \bmod(N) \tag{2}$$

2.1.2 Arnold transform effect

The original two-value watermark image is shown in Fig. 1a. The image is carried out using Arnold transform scrambling. Scrambling times is the encryption key of the watermark. The scrambling period corresponding to the order of the image subtracted from the scrambling times before is the decryption key. The graph is the result of watermark after 1, 2, 20 scrambling times.

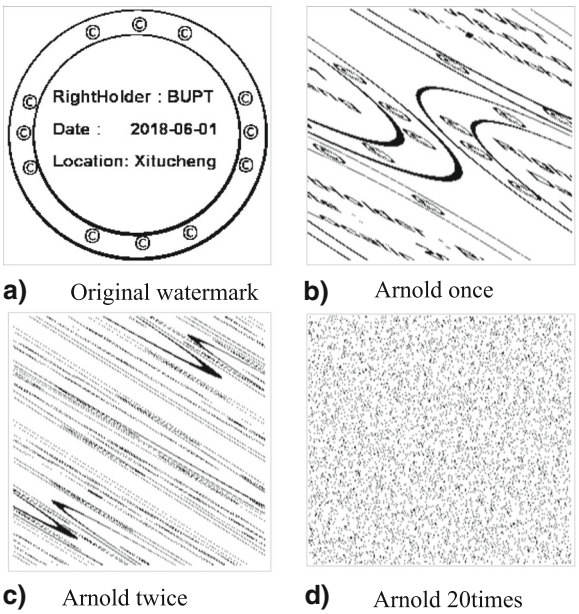

Fig. 1 a–d Arnold transform

2.2 Logistic map

Logistic map is a chaotic mapping method for one-dimensional, which is digital content security and other fields. The formula of logistic map is featured with a simple form, which is defined as follows:

$$\begin{aligned} &X(k+1) = u \times X(k) \times [1-X(k)], k = 0, 1, ..., n, \\ &X(k) \in (-1, 1), u \in (0, 4) \\ &0 < X(0) < 1 \\ &3.5699456 < u < 4 \end{aligned} \tag{3}$$

where $X(k)$ is the mapping variable and u is the system mapping parameter. The function of logistic works in a disorder and unpredictable way, and the function is sensitive to the system mapping parameter u. $[X(0), u]$ is used as the encrypted secret key.

2.3 Human visual system and Watson model

2.3.1 Human visual system

Background brightness masking, texture masking, and frequency masking effects of human vision system (HVS) are often applied to digital watermarking technology, which has a great relationship with the embedding strength and the value of the visible threshold value. In the visual system, brightness and frequency are much more important to image or video than color or direction. The higher the background brightness is, the less sensitive to the human eye. That is, background brightness can very well mask the change of image. In the transform domain algorithm, the human eye changes the image by the high-frequency coefficient or the diagonal coefficient, which does not reflect the change of the image, that is to say, the frequency coefficient can mask the change of the image. The more complex the image background texture is, the more difficult the human eye can judge the change of the image, the image texture can be changed by masking, so the embedding strength of the watermark can be increase moderately in the relatively complex background image.

2.3.2 Illuminance masking model

The illuminance model proposed in [20] is one of the human visual models (Fig. 2), the background brightness masking effect and the pattern. The masking effect and the frequency masking effect are also applicable to the Watson model. In this paper, we use the formula in this model to calculate the embedding strength.

From the background brightness masking properties, according to the Weber-Fechner law, the visual brightness masking properties can be expressed as follows:
where L shows the background brightness and $L + \Delta L$ shows the brightness of the object that the human eye can observe. ΔL is the threshold that human visual organs can detect when brightness changes. Recent studies have shown that the mapping equation between ΔL and L is as follows:

$$\Delta L = 0.0594 \times \left(1.219 + L^{0.4}\right)^{2.5} \tag{4}$$

About frequency concealment characteristics, divide the image into 8×8 sub-blocks; the study of the frequency of 8×8 sub-blocks indicates that the sensitivity of the human eye decreases with the increase of frequency.

2.3.3 Texture masking model

Texture masking characteristics are also called contrast-masking characteristics. For the identification of contrast, there is no specific model at present. Usually, edge detection is used. Even in the case of high texture complexity,

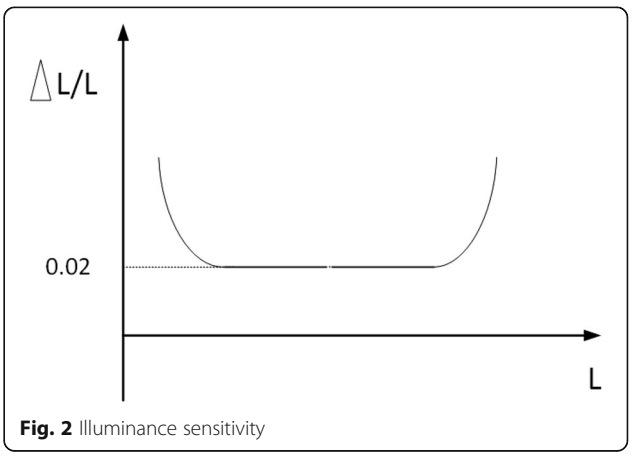

Fig. 2 Illuminance sensitivity

the human eye is still insensitive to image modification traces even if the watermark intensity is increased. Supposing two-dimensional image is $f(x_1, x_2) \in L^2\ (R^2)$, the two-dimensional wavelet decomposition image is:

$$\begin{aligned} A_2 f(x_1,x_2) &= < f(x_1,x_2), \varnothing_{2k_1}(x_1)\varnothing_{2k_2}(x_2) > \\ D_2^{(1)} f(x_1,x_2) &= < f(x_1,x_2), \varnothing_{2k_1}(x_1)\psi_{2k_2}(x_2) > \\ D_2^{(2)} f(x_1,x_2) &= < f(x_1,x_2), \psi_{2k_1}(x_1)\varnothing_{2k_2}(x_2) > \\ D_2^{(3)} f(x_1,x_2) &= < f(x_1,x_2), \psi_{2k_1}(x_1)\psi_{2k_2}(x_2) > \end{aligned} \tag{5}$$

$$Q(x_1,x_2) = \sum_{i=1}^{3} \sigma\left(D_2^{(i)} f(x_1,x_2)\right) + \Delta L(x_1,x_2) \tag{6}$$

where $\varnothing(\cdot)$ and $\psi(\cdot)$ are the horizontal filter function and vertical filter function respectively. $\sigma(\cdot)$ indicates the standard deviation function.

2.4 JPEG image compression and Watson DCT model

2.4.1 JPEG compression and DCT transform

Considering the image storage, the image data is commonly stored in a compressed way. JPEG is widely used in picture compression form, so we choose JPEG as an example of image data in our proposed multimedia content protection solution. In this scheme, robust watermark for DRM misusing detection is a binary image, which indicates some owner identification. We choose to embed watermarks based on the DCT coefficients in this scheme.

JPEG compression usually divides the complete digital image into 8×8 blocks, DCT, and quantifies the luma samples of each block. The DCT of the two-dimensional signal $f(x, y)$, $x = 0, 1, \ldots M-1$; $y = 0, 1, \ldots N-1$) is defined as follows:

$$F(u,v) = c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\frac{(2x+1)u\pi}{2M} \cos\frac{(2y+1)v\pi}{2N}$$
$$u = 0,1,\ldots,M-1; v = 0,1,\ldots,N-1. \tag{7}$$

The inverse IDCT is defined as follows:

$$f(x,y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} c(u)c(v)F(u,v) \cos\frac{(2x+1)u\pi}{2M} \cos\frac{(2y+1)v\pi}{2N}$$
$$x = 0,1,\ldots,M-1; y = 0,1,\ldots,N-1.$$
$$c(u) = \begin{cases} \frac{1}{\sqrt{M}} & u = 0 \\ \frac{2}{\sqrt{M}} & u \neq 0 \end{cases} \quad c(v) = \begin{cases} \frac{1}{\sqrt{N}} & v = 0 \\ \frac{2}{\sqrt{N}} & v \neq 0 \end{cases} \tag{8}$$

2.4.2 Watson DCT domain model

For the JPEG compression standard, we can use the visual model to calculate the quantization step size. The quantization error of the quantized DCT coefficient is within JND. Watson have presented optimal JPEG quantization step size.

For brightness-adaptive phenomenon, $T_{u,v,k}^L$ is defined as follows:

$$T_{u,v,k}^L = T_{u,v}\left(\frac{c_{0,0,k}}{c_{0,0}}\right)^a \tag{9}$$

where $c_{0,\,0,\,k}$ represents the DC coefficients of block k, which means the brightness value of block image. $c_{0,\,0}$ reflects the mean brightness of the whole image, which can be assigned $c_{0,\,0} = 1024$ when calculating. $T_{u,\,v}$ is the quantization step size matrix, independent on concrete images. Taking into account the contrast-masking effect, quantization step size can be obtained from the following formula, $w_{u,\,v} = 0.7$:

$$T_{u,v,b}^C = \mathrm{Max}\left\lfloor T_{u,v,b}^L, \left|X_{u,v,b}\right|^{w_{u,v}} \left(T_{u,v,b}^L\right)^{1-w_{u,v}} \right\rfloor \tag{10}$$

3 Method: The proposed DRM misusing detection scheme based on watermark

3.1 Watermark scheme architecture for DRM misusing detection

The whole scheme includes two import parts. The first part is the watermarking embedding process. In the pre-processing of the input JPEG image, we convert the RGB image into YCbCr image, in which Y is the luminance signal, Cb is chrominance blue signal, and Cr is chrominance red signal of the image. The redundancy of luminance signal is more than that of the Cb signal and Cr signal, and the luminance Y signal is insensitive to watermark, so we select the luminance to embed the watermarks. After pre-processing the input image, the Y matrix could be divided into 8×8 blocks. And with each 8×8 DCT block, the watermark could be embedded in the DCT domain with HVS characteristics. The brightness equation is as follows:

$$\begin{aligned} Y &= 0.299 \times R + 0.587 \times G + 0.114 \times B \\ \mathrm{Cb} &= -0.299 \times R - 0.587 \times G + 0.886 \times B \\ \mathrm{Cr} &= 0.701 \times R - 0.587 \times G - 0.114 \times B \end{aligned} \tag{11}$$

In the watermark security aspect, we utilize logistic mapping sequence and Arnold transform to encrypt watermark image to make it impossible for attacker to extract the watermark exactly especially when some knowledge of the watermark embedding algorithm has been gotten.

3.2 Watermark embedding algorithm for DRM misusing detection

In the watermark embedding algorithm, we select one $M \times N$ binary image as watermark W. $W = \{W(i,j) | 0 \le i < M, 0 \le j < N\}$, and $W(i,j) \in \{0,1\}$. We scramble the binary image using Arnold transform for security and then convert the encrypted image into one-dimensional image sequence and then use logistic mapping to encrypt the one-dimensional sequence to encrypted watermark sequence, namely $W = \{w_i\}$, $i = 1, 2, \ldots, C$; $C = M \times N$, $w_i = 0$ or 1. The RGB of the host JPEG image is converted into YUV signals. And the Y luminance is divided into 8×8 blocks. The sequence of DCT coefficients of one block is recorded as $D_i(k)$, $(k = 0, 1, 2, \ldots 63)$ in a zigzag scan form. i is the number of blocks. We choose a continuum of mid-frequency coefficients to embed watermark, such as $D_i(L)$, $L = 3,4,\ldots 18$.

The processing of coefficient $D_i(k)$ balances the robustness and transparency of watermark. The specific methods are as follows:

$$D_i(k)' = \begin{cases} Q(D_i(k)) \times T^L_{u,v,k} + \\ \left(\left\lceil \frac{T^L_{u,v,k}}{2} \right\rceil + \mathrm{mod}(Q(D_i(k)), 2) \times T^L_{u,v,k} \right) \times S(D_i(k)) \\ if(w_i = 0) \\ Q(D_i(k)) \times T^L_{u,v,k} + \\ \left(\left\lceil \frac{T^L_{u,v,k}}{2} \right\rceil + \mathrm{mod}(Q(D_i(k)) + 1, 2) \times T^L_{u,v,k} \right) \times S(D_i(k)) \\ if(w_i = 1) \end{cases} \tag{12}$$

$$Q(D_i(k)) = \begin{cases} \left\lceil \frac{D_i(k) - Q_i \times S(D_i(k))}{T^L_{u,v,k}} \right\rceil & D_i(k) > 0 \\ \left\lceil \frac{D_i(k) - Q_i \times S(D_i(k))}{T^L_{u,v,k}} \right\rceil & D_i(k) < 0 \end{cases}$$
$$S(D_i(k)) = \mathrm{sign}(D_i(k))$$
$$D_i(k) \epsilon \{D_i(L), D_i(L+1), D_i(L+2), D_i(L+3), D_i(L+4)\} \tag{13}$$

where mod(.) indicates modular operation, sig(.) returns the symbol variable of the parameter, $D_i(k)$ is the DCT coefficient, i is the 8×8 block image number, and k is the coefficient number. In order to control the excessive increase of bit rate of the image data after watermark embedding, the watermark embedding algorithm only considers non-zero coefficients.

Mid-frequency coefficients are selected to embed watermarks. The choice of the mid-frequency coefficients directly affects the robustness and transparency of watermarks. Different modifications of DCT coefficients may bring different visual perception and different robustness of watermark. Figure 3 describes the relationship of, namely, different $D_i(k)$ and transparency and robustness. Peak signal to noise ratio (PSNR) is used to measure the transparency, and bit error is used to measure the robustness. The image Green bamboo is used as the host image, and watermark is random sequence.

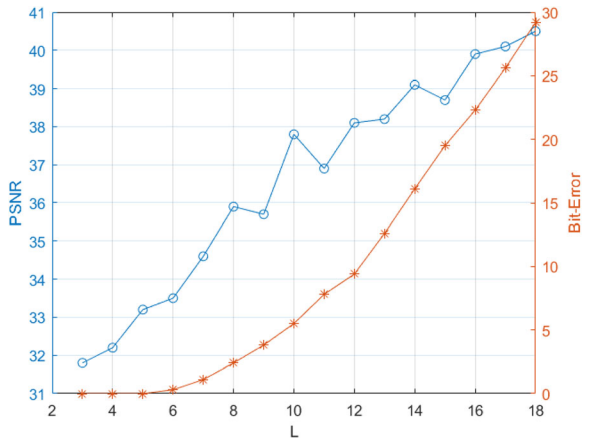

Fig. 3 a–d Host image and watermark

In Fig. 4, the horizontal ordinate indicates the choice of $D_i(L) \sim D_i(L+4)$ to be embedded watermark. The left vertical ordinate is the PSNR between the host image and the watermarked JPEG image. For different L, the watermark is embedded in different coefficients; when L is small, the watermark is embedded in low-frequency coefficients, which may bring low PSNR but low bit

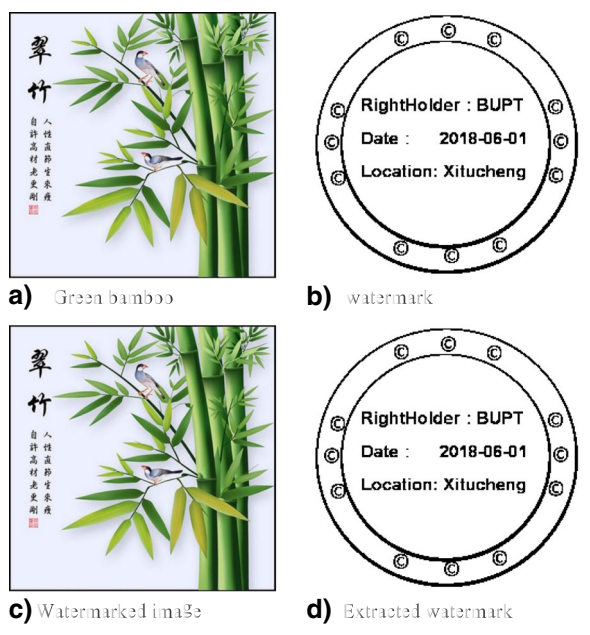

Fig. 4 PSNR and bit error for different k

error robustness, and when L is big, the watermark is embedded in mid-frequency coefficients, which may bring high PSNR but also high bit error.

In Fig. 4, we find when L=10, the PSNR is near 39 dB, one maximum value in around the curve, and also the bit error is less than 2%. The main reasons may be as follows:

(1) We can find when L=10, the coefficients to be embedded is $D_i(10)$~$D_i(14)$, which are in the same layer in the zigzag scanning line and impact the 8×8 block image evenly.

(2) In JPEG compression table, the quantization step is not very big in the layer responding to L=10, which bring small quantization errors and some good balance between PSNR and bit error of the block image.

From the above analysis, we select $D_i(10)$~$D_i(14)$ (L=10) as the watermark embedding coefficients.

From Formula 5, we can get Q_i is related to the texture of the image. The much bigger Q_i means the higher texture in the blocks of the image and the easier to embed watermarks.

For the host image is JPEG image, when the watermark is embedded, the watermarked image is often saved in JPEG format. The lossy compression of JPEG may attack the watermark in the saved JPEG image and bring some bit error in the extracted watermark process, so the choice of JPEG compression quality is very important. Meantime, the high quality may cause the storage volume to be very big, which is not very suitable for practical application. So in order to determine the bit error of the watermark and the storage volume of the watermarked image, some treatment measures will be used before the watermark embedding process is quite over.

Store watermarked JPEG image with compression quality factor $Q = 100$. And then extract the watermark from the stored image; if there is no bit error in the extracted watermark, store the watermarked JPEG image with the new compression quality factor $Q = Q - 1$, and so on. Until bit error happens, save the watermarked JPEG image with the final compression quality factor $Q = Q + 1$, then the watermark embedding process is complete.

3.3 Watermark extracting algorithm for DRM misusing detection

In the watermark extracting algorithm, we get one suspicious JPEG image for digital rights management. Convert the RGB signals of JPEG image into YUV signals and divide the Y luminance into 8×8 blocks, and then perform DCT transform on each block image. The sequence of DCT coefficients of one block is also recorded as $D_i(k)$, $(k = 0, 1, 2, \ldots 63)$ in a zigzag scan form the same as the watermark embedding process, where i is the number of blocks. We choose a continuum of mid-frequency coefficients to extract watermark, such as $D_i(L)$, L = 10,11,...14. The watermark to be extracted is recorded as W_n, where n is the number of watermark bit extracted. The watermark extracting methods are on the basis of the characteristics of DCT coefficients, and the specific methods are as follows:

$$w_i = \begin{cases} -1, & \mathrm{mod}\left(Q\left(D_i(k)'\right), 2\right) = 0 \\ +1, & \text{otherwise} \end{cases} \tag{14}$$

$$Q\left(D_i(k)'\right) = \begin{cases} \left[\dfrac{D_i(k)' - Q_i \times S\left(D_i(k)'\right)}{T^L_{u,v,k}}\right] & D_i(k)' > 0 \\ \left[\dfrac{D_i(k)' - Q_i \times S\left(D_i(k)'\right)}{T^L_{u,v,k}}\right] & D_i(k)' < 0 \end{cases}$$

$$S\left(D_i(k)'\right) = \mathrm{sign}\left(D_i(k)'\right) \tag{15}$$

And then

$$W_n = \begin{cases} 0, & \sum_i w_i < 0 \\ 1, & \text{otherwise} \end{cases} \tag{16}$$

where i the number of block coefficient is $D_i(k)$ and n is the number of watermark bit.

After all watermark bits are extracted, the watermark bits should be changed into a two-dimensional image signal, and then retrieve watermark image by reverse Arnold transform and reverse logistic mapping transform.

4 Results and discussions

4.1 Experiments and evaluations of the watermark algorithm for DRM misusing detection

In this scheme, we designed a watermark-based effective DRM algorithm for misusing detection by embedding watermarks based on DCT, in which the robust watermark is for misusing detection process. In our scheme, we constructed the watermark in an image format with some copyright text information; thus, even if the image data is being attacked, the copyright text information can still be recognized in the image watermark and can parse the user-related information and then can be taken as an evidence by the image watermark.

In order to evaluate the transparency and robustness, we carry out various experiments about this scheme. In terms of watermark transparency, PSNR is used for evaluating the image quality objectively, which is defined as:

$$PSNR = 10\ \log_{10}\left(\frac{(O-1)^2}{\mathrm{MSE}}\right)\mathrm{dB} \tag{17}$$

where $O-1$ reflects the maximum value of the original image pixels. MSE is the mean squared errors, given by

$$\mathrm{MSE} = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[W(i,j)-\hat{W}(i,j)\right]^2 \tag{18}$$

Structural similarity index (SSIM) values can also be used to evaluate the quality of the watermarked image. The maximum value is 1 when both images are structurally similar.

$$L(X,Y) = \frac{2u_X u_Y + C_1}{{u_X}^2 + {u_Y}^2 + C_1} \tag{19}$$

$$C(X,Y) = \frac{2\sigma_X\sigma_Y + C_2}{{\sigma_X}^2 + {\sigma_Y}^2 + C_2} \tag{20}$$

$$S(X,Y) = \frac{\sigma_{XY} + C_3}{\sigma_X\sigma_Y + C_3} \tag{21}$$

$$C_3 = C_2/2 \tag{22}$$

$$\mathrm{SSIM}(X,Y) = \frac{(2u_X u_Y + C_1)(2\sigma_{XY} + C_2)}{({u_X}^2 + {u_Y}^2 + C_1)({\sigma_X}^2 + {\sigma_Y}^2 + C_2)} \tag{23}$$

where u_X and u_Y reflect the mean value of image X and image Y. σ_X and σ_Y reflect the standard deviation of image X and image Y. σ_{XY} reflects the covariance of image X and image Y.

Normalized cross correlation (NC) is a standard method for evaluating the degree of similarity between the original watermark image and the extracted watermark image, which is defined as:

$$\mathrm{NC} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W(i,j)\times\hat{W}(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W(i,j)^2} \tag{24}$$

Bit error rate (BER) is defined as the ratio of watermark bit errors. BER is defined as follows:

$$BER(\%) = \frac{1}{n}\left[\sum_{j=1}^{n} W(i,j)\oplus\hat{W}(i,j)\right]\times 100 \tag{25}$$

where n is total number of watermark bits, which are embedded.

In the experiment, some pictures taken on the Internet with the size of 2560×2560 are used. A binary logo of size 250×250 is used as watermark, which describes some info for misusing detection, such as right holder, date, and location information. Figure 5 shows the original image, binary watermark, and the corresponding watermarked image. The PSNR of watermarked image is 39.32 dB while quality factor is 100. The bit- error of the watermark extracted is 0.

After the host JPEG image is embedding the watermark for misusing, storage capacity of the watermarked JPEG file may be increased. To constraint the storage capacity, the watermarked JPEG image should be compressed with low quality factor and storage in a limit capacity. The index CIR (capacity increase ratio) will be used in this paper, which can be used as the percentage

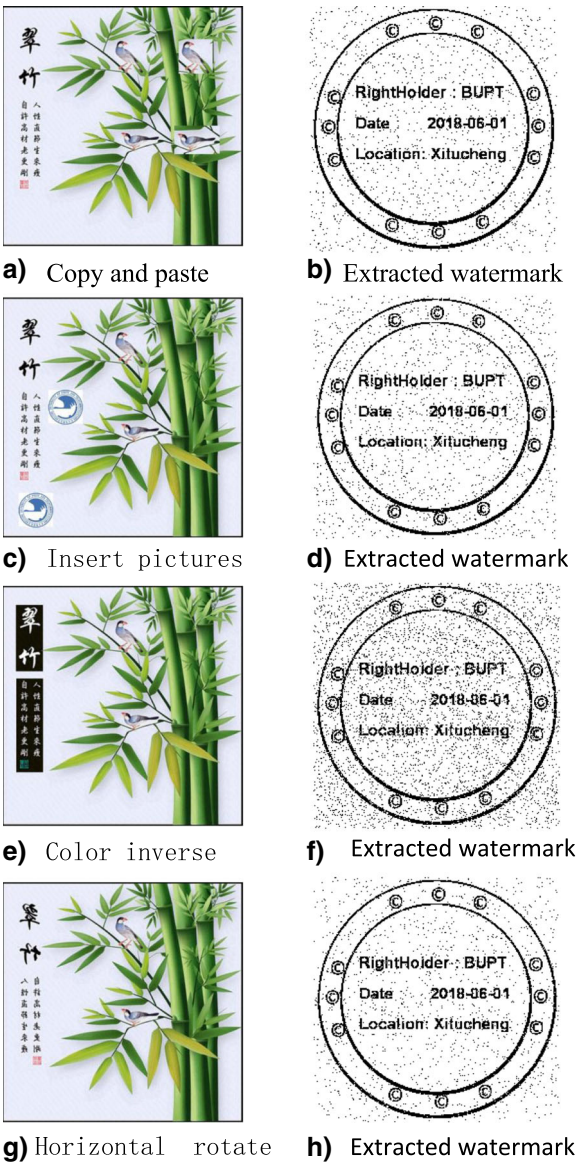

Fig. 5 a–h Watermark attacking and extracting

Table 1 Different quality factors for the Green bamboo image

Quality factor	CIR (%)	PSNR (dB)	SSIM	Bit error
100	163.24	39.32	0.9750	0
95	32.89	39.34	0.9762	0
90	2.91	39.03	0.9723	0
85	− 18.23	39.23	0.9736	0.001
80	− 26.33	38.82	0.9715	0.004
75	− 31.88	38.33	0.9687	0.016
70	− 36.65	37.99	0.9660	0.037
65	− 47.67	38.00	0.9657	0.075

of image capacity increase ratio between the host image and the watermarked image.

$$\mathrm{CIR} = \frac{\text{Capacity (Watermarked)} - \text{Capacity (Original)}}{\text{Capacity(Original)}} \times 100\% \tag{26}$$

where Capacity (Original) and Capacity (Watermarked) are the file capacity of the original image and the watermarked image capacity.

We can analyze the following conclusions from Table 1. When the quality factor decreases, the CIR of JPEG image decreases. CIR is lower than 0 when quality factor is below 90. When compression factor is reduced to 90, bit error may be happened.

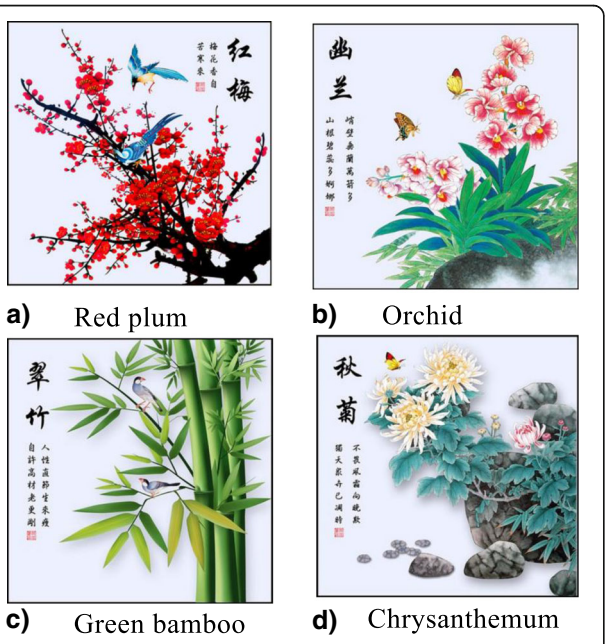

Fig. 6 a–d Experiment images

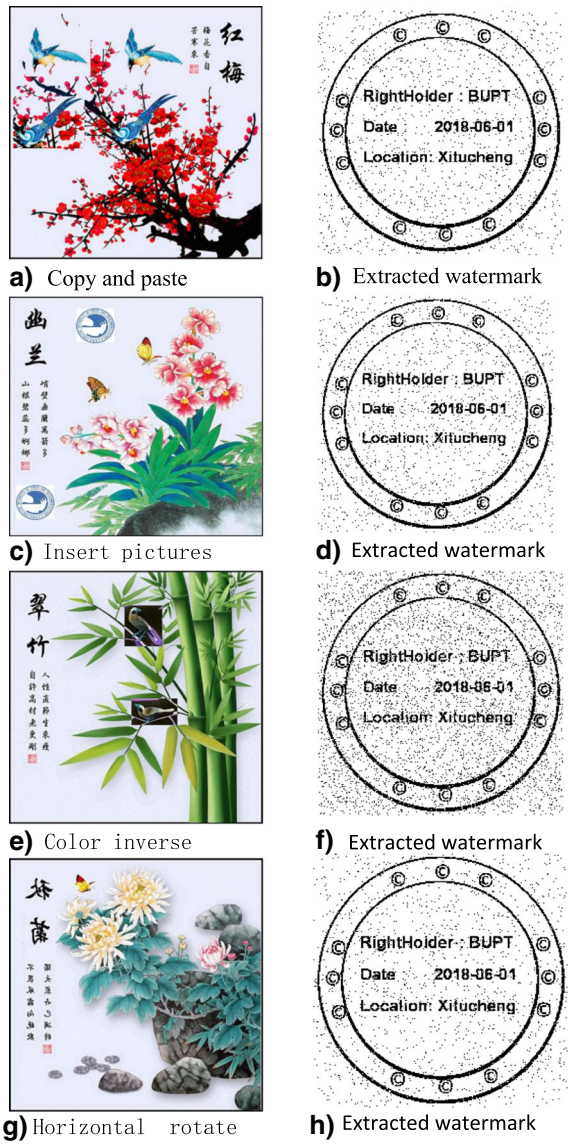

Fig. 7 a–h Experiment images attacking and extracting

4.2 Attacks and analysis of DRM watermark algorithm

In this experiment (see Fig. 5), we attack the watermarked image firstly and then verify whether we can extract the watermark from the attacked images. In the experiment, we gave the detailed experiments according to the six kinds of attacks: (1) copy and paste attack, (2) insert picture attack, (3) color inverse attack, and (4) horizontal rotate.

From the results in Fig. 6, in which the watermark can be easily recognized, it describes the information, such as right holder, date, and location information after the attacks.

For further experimental verification, we use different benchmark images as experimental object images (see Figs. 6 and 7). The watermark describes info for misusing detection, such as right holder, date, and location information. Table 2 shows the experiment results, and the

Table 2 Experiments for Green bamboo

Image number	Attack type	Tampering ratio (%)	Bit error	NC
1	Copy and paste	7.3	0.048	0.9771
2	Insert pictures	5.5	0.051	0.9722
3	Color inverse	7.8	0.072	0.9310
6	Horizontal rotate	8	0.044	0.9763

experiments show the validation and performance of the proposed algorithm.

According to the experimental results from Table 2, we draw the conclusion as follows: The CIR for different images are generally less than 0 when compression quality is 90, which means the file storage size of watermarked images cannot be increased very much after watermark embedding, even decreased for JPEG compression. Especially, CIR for image of high texture are commonly below zero, such as red plum and chrysanthemum. CIR for image of low texture are commonly above zero, such as orchid and green bamboo. The PSNR of the images are general above 38 dB, and the bit error of the identification watermarks is near 0.

The related methods are compared with the proposed schemes in terms of functionalities and performance.

Comparing with the current related schemes, our proposed scheme has the following three advantages and innovations:

Obviously, in addition to the abovementioned analysis, the present schemes have another three advantages.

(1) *Automatic watermark generation*: Compared with some other watermark schemes, the watermark scheme is efficient. The security of watermark is very well for Arnold transform and logistic mapping transform.
(2) *Parameter control for watermark performance*: Different quality of JPEG compression can control the quality of watermarked images, so as to balance the capacity of the image storage file and watermark performance, the watermark scheme can use quality of JPEG to compact the algorithm.
(3) *Scheme proposed misuse detection method based on robust watermark in post-usage stage*: The proposed watermark scheme supports robust watermark, which can certificate the Internet image source authentication and misusing detection, even if the watermarked image was attacked by variant tamping.

Table 3 Experiments for different images when quality is 90

Image number	Image	CIR (%)	PSNR (dB)	SSIM	Bit error
1	Red plum	− 9.38	39.17	0.9729	0.003
2	Orchid	1.0	38.98	0.9721	0
3	Green bamboo	3.53	39.03	0.9723	0
4	Chrysanthemum	− 2.96	38.85	0.9713	0

Table 4 Experiments for tampering

Image number	Image	Attack type	Tampering ratio (%)	Bit error	NC
1	Red plum	Copy and paste	11.6	0.066	0.9771
2	Orchid	Insert pictures	5.9	0.036	0.9722
3	Green bamboo	Color inverse	6.3	0.057	0.9310
4	Chrysanthemum	Horizontal rotate	8.1	0.042	0.9763

Through experiments, we can see that the proposed watermark scheme is practical and effective, which can recognize the device-related information to trace and find the one who misuse or violate the confidential Internet pictures.

In Table 3, we can get that the watermark algorithm is embedded randomly and securely in the host images. So the robustness of watermark is very good against the attack of parts of (Table 4). The bit error is 0 even when the tampering ratio is up to 1%. The algorithm is effective especially when parts of image rotate and color inverse attack happen, and the bit error is also very slow in the experiments.

5 Artwork DRM blockchain platform implementation and its blockchain data management

5.1 Artwork DRM blockchain platform implementation

Based on the above availability and security analysis of the digital rights management and its misusing detection technology, we implemented the artwork DRM platform (named DRMChain) based on Hyperledger Fabric 1.0 [21–24] consortium blockchain for authorized membership user service (see Figs. 8 and 9),

Fig. 8 DRMChain platform service function

Fig. 9 DRMChain block data instance

upon which authorized consortium users can find and confirm their interested artwork and can track the artwork's copyright information such as artwork's author, right holder, and date.

5.2 Artwork DRM blockchain data management

5.2.1 Artwork raw data management

When the user is using the DRMChain platform, he/she firstly needs to register as user-level account, then he/she can commit his/her artwork, and the DRMChain will create the raw artwork and its corresponding blockchain data, which includes block data (block header) and the block transaction (block body).

5.2.2 Artwork DRM blockchain data creation

Upon the implementation of the consortium blockchain, the DRMChain first creates the blockchain channel and chain code and builds up the blockchain in the Docker system. When the raw artwork data is committed as a proposal in the DRMChain blockchain platform, the DRMChain creates the block-related discrete data and then commit the unconfirmed discrete data to the order peer; the order peer then confirmed and ordered the data in Kafka or Solo mode; once the data is confirmed in the blockchain system, the artwork data is formally stored in all the related peers and created its corresponding blockchain data structure. Table 5 shows an instance of a raw artwork data and its corresponding blockchain data (block header and body):

5.3 Artwork DRM blockchain data management

As for the blockchain, data is created and confirmed by cryptography-based digital signature with unique timestamp, and each block (except for the genesis block) is linked with the previous block which is ensured by un-tampered hash algorithm, and the consortium-based DRMChain platform can provide authorization access, isolation of different level user data, privacy protection, and high-level TPS (transaction per second). Thus, the DRMChain can provide a technique-based, fair, and trusted artwork content protection solution, in which the artwork is protected by the content provider with watermark (the unauthorized fake artwork can NOT provide the authorized watermark); the DRMChain is useful for artwork content exhibition and exchange.

6 Conclusions

A new watermarked-based image data security scheme for digital rights management misusing detection was proposed in this paper. We embedded the information,

Table 5 Artwork DRM blockchain data instance

Name	Data
Creation name	Chinese bamboo painting
Creation author	Mr. Li Qing
Copyright owner	BUPT Library
Creation time	2008-08-08
BlockNumber	36
CurrentHash	2c8c4881b34e13bce7d4ed4869f890fbbd5754ab7f02b4c229cfc0495419ca77
PreviousHash	3dc7555ead146a41302865873e941767e7126064da73e343e282654ace5103ff
Datahash	469f57098a297611c450f2d138fe7a4851cd383825c10fef9e0b3bbd9ae23587
Number of tx	1
tx_id	1c50bc264ee12588711e8a77c3ea8ebf81651079a260ebebc95d9c7de12984d7
ProposalHash	e5b66ffa37aaa8c8ea9ffd21cd042051b943a28d518b9cecf121a601cd9b380b
Payload	{"application":"","creation_time":"2008-08-08","datahash":"da98e1c5dfee073245b2d15afa22e96485fdd657e304486c06d86f4a713abab1","files":"upload/1533984942206.jpg","id":49,"creation_author":"Mr. Li Qing","copyright_owner":"BUPT Library","artwork_name":"Chinese Bamboo Painting","status":"0","storagetime":"2018-08-11 18:55:42"}
Timestamp	Sat Aug 11 2018 18:55:42 GMT+0800 (CST)

such as right holder, date, and location information into the confidential image data. In the scheme, we use image Arnold transform to enhance the security and use image DCT coefficients of middle frequency to embed watermark for robustness. In the transparence of watermark, HVS and Watson models are used to control the watermark strength, which can enhance the invisibility. Once the image data was spreading and misused in the Internet and for some commerce purposes without authorization, we can extract the watermark even after some attacks happen on the images. Finally, we evaluated the proposed watermark scheme for DRM misusing detection by groups of variant style image data for security and efficiency, and a large amount of groups of experiments indicate the proposed scheme was secure, robust, pervasive, and efficient for confidential image data protection and misusing detection.

Abbreviations

DCT: Discrete cosine transfer; DRM: Digital rights management; DWT: Discrete wavelet transfer

Funding

This work is supported by the National Natural Science Fundamental of China (Nos. 61272519, 61170297, 61572080, and 61472258).

Availability of data and materials

Please contact the author for data requests.

Authors' contributions

The work is mainly finished by the author MZ, who proposed the whole architecture and complemented main work of the paper. The other authors made part of the experiments and help in formatting the references. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China. [2]Shenzhen Datong Industrial Co. Ltd, Shenzhen 518000, China.

Received: 13 July 2018 Accepted: 28 August 2018
Published online: 19 September 2018

References

1. D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans. Inf. Technol. Biomed. **16**(5), 891–899 (2012)
2. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, 2nd edn. (Morgan Kaufmann, San Francisco, 2007)
3. C.I. Podilchuk, E.J. Delp, Digital watermarking: algorithms and applications. IEEE Signal Process. Mag. **18**(4), 33–46 (2001)
4. C.C. Chang, P.Y. Lin, J.S. Yeh, Preserving robustness and removability for digital watermarks using subsampling and difference correlation. Inf. Sci. **179**(13), 2283–2293 (2009)
5. S. Bravo-Solorio, A.K. Nandi, Secure fragile watermarking method for image authentication with improved tampering localisation and selfrecovery capabilities. Signal Process. **91**(4), 728–739 (2011)
6. X. Wu, Reversible semi-fragile watermarking based on histogram shifting of integer wavelet coefficients, in Proc. DEST, Cairns, 2007, pp. 501–505
7. Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun, X. Lin, Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans Circuits Syst Video Technol **18**(4), 497–509 (2008)
8. C.-C. Lai, C.-C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans. Instrum. Meas. **59**(11), 3060–3063 (2010)
9. A. Benoraira, K.B. Mahammed, N. Boucenna, Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP J Adv Signal Process, 55 (2015). https://doi.org/10.1186/s13634-015-0239-5
10. E. Vahedi, R.A. Zoroofi, M. Shiva, Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. Digit Signal Process **22**(1), 153–162 (2012)
11. I. Prathap, V. Natarajan, R. Anitha, Hybrid robust watermarking for color images. Comput. Electr. Eng. **40**(3), 920–930 (2014)
12. C. Das, S. Panigrahi, V.K. Sharma, K.K. Mahapatra, A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. Int. J. Electron. Commun. **68**(3), 244–253 (2014)
13. S.A. Parah, J.A. Sheikh, N.A. Loan, G.M. Bhat, Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digit. Signal Process. **53**, 11–24 (2016)
14. Loan N A, Hurrah N N, Parah S A, et al. Secure and robust digital image watermarking using coefficient differencing and chaotic encryption [J]. IEEE Access, vol.6, no.99, pp. 19876–19897, 2018
15. Y. Liu, S. Tang, R. Liu, et al., Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Syst. Appl. **97**, 95–105 (2018)
16. J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, Y. Zhang, An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. Commun. Nonlinear Sci. Numer Simul **23**(1–3), 294–310 (2015)
17. C. Dong, L. Jingbing, M. Haung, and Y. Bai, The medical image watermarking algorithm with encryption by DCT and logistic, in Proc. WISA, Haikou, 2012, pp. 119–124
18. J. Guo, P. Zheng, J. Huang, Secure watermarking scheme against watermark attacks in the encrypted domain. J. Vis. Commun. Image Represent. **30**, 125–135 (Jul. 2015)
19. MENG Zhaoxiong, Morizumi Tetsuya, Miyata Sumiko, Kinoshita Hirotsugu, Design scheme of copyright management system based on digital watermarking and blockchain, 42nd IEEE International Conference on Computer Software & Applications,2018, pp. 359–364
20. A.B. Watson, J. Hu, J.F. Mcgowan, DVQ, a digital video quality metric based on human vision. J. Electron. Imaging **10**, 20–29 (2001)
21. The Hyperledger Project. https://www.hyperledger.org
22. M. Vukolić, The quest for scalable blockchain fabric: proof-of-work vs. BFT replication, International Workshop on Open Problems in Network Security, pp. 112–125, 2015
23. A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, BlockChain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. **55**(12), 119–125 (2017)
24. R. M. Frey, P. Buhler, A. Gerdes, T. Hardjono, K. L. Fuchs, and A. Ilic, The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data, IEEE 16th International Symposium on Network Computing and Applications (NCA), pp.1–5, 2017