

Robust color image watermarking technique in the spatial domain

Qingtang Su¹ · Beijing Chen²

Published online: 21 January 2017
© Springer-Verlag Berlin Heidelberg 2017

Abstract This paper proposes a new blind watermarking algorithm, which embedding the binary watermark into the blue component of a RGB image in the spatial domain, to resolve the problem of protecting copyright. For embedding watermark, the generation principle and distribution features of direct current (DC) coefficient are used to directly modify the pixel values in the spatial domain, and then four different sub-watermarks are embedded into the different areas of the host image for four times, respectively. When watermark extraction, the sub-watermark is extracted with blind manner according to DC coefficients of watermarked image and the key-based quantization step, and then the statistical rule and the method of “first to select, second to combine” are proposed to form the final watermark. Hence, the proposed algorithm is executed in the spatial domain rather than in discrete cosine transform (DCT) domain, which not only has simple and quick performance of the spatial domain but also has high robustness feature of DCT domain. The experimental results show that the proposed watermarking algorithm can obtain better invisibility of watermark and stronger robustness for common attacks, e.g., JPEG compression, cropping, and adding noise. Comparison results also show the advantages of the proposed method.

Keywords Blind watermarking · Color image · Spatial domain · DC coefficient

Communicated by V. Loia.

✉ Qingtang Su
sdytsqt@163.com

¹ School of Information Science and Engineering, Ludong University, Yantai 264025, Shandong, China

² School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

1 Introduction

With the rapid development of Internet and networked multimedia, illegal copying, tampering, and modifying of digital copyright have been becoming one more and more urgent problem and many techniques about information safety have been proposed to process these issues (Li et al. 2015; Zheng et al. 2015; Su et al. 2014; Ma et al. 2015; Xia et al. 2014; Fu et al. 2016; Guo et al. 2014). Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. The feature of digital watermarking is to allow for imperceptibly embedding watermark information in the original multimedia data (Seitz 2005; Cox et al. 2007). For a digital watermark to be effective, it should at least exhibit the following characteristics:

- (1) Imperceptibility. The watermark should be invisible in a watermarked image/video or inaudible in watermarked digital music. Embedding this extra data must not degrade human perception about the object. Evaluation of imperceptibility is usually based on an objective measure of quality, called peak signal-to-noise ratio (PSNR) or a subjective test with specified procedures.
- (2) Robustness. The embedded watermarks should not be removed or eliminated by unauthorized distributors using common processing techniques, including compression, filtering, cropping, and quantization.
- (3) Security. The watermarking procedure should rely on secret keys to ensure security, so that pirates cannot detect or remove watermarks by statistical analysis from a set of images or multimedia files. An unauthorized user, who may even know the exact watermarking algorithm, cannot detect the presence of hidden data, unless he/she has access to the secret keys that control this data embedding procedure.

- (4) Real-time processing. Watermarks should be rapidly embedded into the host signals without much delay.

Along with the rapid development of computer technique, digital watermarking has recently received an increasing attention in many application fields such as image, video, audio, text, and software. By embedding information into digital signals, digital watermarking can attain higher imperceptibility and robustness. Since the inception of digital watermarking around the early 1990s, there have been a variety of methods proposed in the literature, and there are many ways to classify them. For example, they can be classified according to the application, source type (image watermarks, video watermarks, audio watermarks, text watermarks), human perception, and technique used. As watermarks can be applied in the spatial or frequency domain, different concepts, such as discrete Fourier (DFT), discrete cosine (DCT), and wavelet transformation, or additionally, manipulations in the color domain and noise adding can be mentioned. Furthermore, digital watermarks can be subdivided on the basis of human perception. Digital watermarks can be invisible or visible. We see visible watermarks every day watching television, that is, TV station logos. They can be subdivided into blind and non-blind detection techniques, which are strongly related to the decoding process. At least, digital watermarks can be robust against operations or even fragile for use in copy control or authenticity applications (Seitz 2005). In which, robust watermarking techniques are developed to resist any kind of attack, modification or tampering of the cover data by an adversary. Robust watermarking algorithms are designed to achieve the maximum possible robustness against any intentional or unintentional modification of the watermarked data. On the contrary, fragile watermarking is mainly used for content authentication of multimedia data. In fragile watermarking algorithms, the watermark is generally a secure keyed hash of the entire cover signal. Even a minimal modification of the cover multimedia data (e.g., a single bit in the extreme case) by an adversary destroys a fragile watermark, and consequently causes authentication failure at the receiver side. In other words, a fragile watermark is desirably destroyed and is rendered undetectable, even in the case of minimal modification of the watermarked cover data (Cox et al. 2007).

According to the processing domain of the host image, these existing techniques of image watermarking may be divided into two categories: spatial domain watermarking (Nasir et al. 2010; Arcangelo et al. 2015; Coltuc and Chassery 2007; Pizzolante et al. 2014; Rigoni et al. 2016) and frequency domain watermarking (Zheng and Feng 2008; de Queiroz and Braun 2006; Su et al. 2013; Das et al. 2014; Zeng and Qiu 2008; Kalra et al. 2015).

The main feature of the spatial domain watermarking is to embed the watermark into the host image by directly

modifying a selected set of pixel values in the host image. Usually, the watermark is embedded into the least significant bit planes of the original image to obtain the resultant watermarked image. Any change in watermarked image will change bits of least significant bit (LSB) of watermarked image. In Nasir et al. (2010), a novel digital watermarking technique for the copyright protection of digital color images was proposed, in which four similar watermarks were directly combined after extracting the sub-watermarks, then the final watermark was selected from four similar watermarks according to correlation coefficient (CC), that is, the original watermark was required. Thus, method of Nasir et al. (2010) was a non-blind watermarking scheme. Seriously, the true state of extracted sub-watermark was not reflected by its final watermark since using the method that “first to combine sub-watermark to 4 whole watermarks, then select the optimum final watermark from the whole watermarks.” One of the contributions of Arcangelo et al. (2015) is an engine for lossless dynamic and adaptive compression of 3D medical images, which also allows the embedding of security watermarks within them was proposed, and the compression engine is based on a predictive technique for what concerns the 3D image compression part and on the LSB technique for that relating the digital watermarking. A spatial domain reversible watermarking scheme that achieves high-capacity data embedding without any additional data compression stage was proposed in Coltuc and Chassery (2007). Pizzolante et al. (2014) proposed a novel scheme which is able to embed two watermarks into a confocal 3-D microscopy image. Rigoni et al. (2016) presented a framework for detecting tampered information in digital audiovisual content, in which the proposed framework uses a combination of temporal and spatial watermarks that do not decrease the quality of host videos, and a modified version of the quantization index modulation (QIM) algorithm is used to embed watermarks. The fragility of the QIM watermarking algorithm makes it possible to detect local, global, and temporal tampering attacks with pixel granularity (Rigoni et al. 2016; Chen and Wornell 2001).

For increasing the robustness of spatial domain-based watermarking techniques, various methods have been proposed in recent years (Zheng and Feng 2008; de Queiroz and Braun 2006; Su et al. 2013; Das et al. 2014; Zeng and Qiu 2008; Kalra et al. 2015). Frequency domain watermarking is nonlinear and confidently deals with the frequency components of the image. At present, some watermarking based on discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) are well-known transform domain watermarking. The frequency domain watermarking has strong robustness and can resist many geometric attacks such as rotation, scaling, and cropping attack. For example, in Zheng and Feng (2008), a multi-channel DWT domain image watermarking was pro-

posed to against geometric attacks and experimental results show that the proposed method is fairly resistant against the lossy compression attack and has a good trade-off between robustness and computational complexity. In [de Queiroz and Braun \(2006\)](#), a reversible method to convert color graphics and pictures to gray images based on watermarking that using one level of the DWT, which provides a high-capacity embedding watermarking scheme and better invisibility.

[Das et al. \(2014\)](#) presented a novel blind watermarking algorithm in DCT domain using the correlation between two DCT coefficients of adjacent blocks in the same position. [Zeng and Qiu \(2008\)](#) considered direct current (DC) coefficient to trade-off the robustness and the invisibility and proposed a blind watermarking scheme with quantization index modulation (QIM) technology, in which the DC coefficient was obtained after the 2-DCT was performed independently for every block of the image. [Kalra et al. \(2015\)](#) proposed an adaptive digital image watermarking for color images in frequency domain which utilizes the advantages of DCT, DWT, Arnold transform, Chaos and Hamming as ECC. In the methods of [Das et al. \(2014\)](#), [Zeng and Qiu \(2008\)](#), [Kalra et al. \(2015\)](#), 2-DCT was performed independently for every block of the image and inverse 2-DCT was applied to the modified DCT coefficients of each embedding block to rebuild the watermarked image when embedding the watermark. Moreover, 2-DCT was also performed independently for every block of the watermarked image when extracting the watermark. Although more information for embedding and better robustness against the common attacks can be achieved through frequency domain method, the computational cost is higher than that of spatial domain. Embedding the watermark into the component of the original image in spatial domain is a straightforward method which has the advantages of low computational complexity ([Su et al. 2013](#)).

Motivated by the above-mentioned discussions, combining these advantages of the frequency domain and spatial domain, a blind watermarking algorithm is proposed in this paper, which using the DC coefficient that directly obtained in spatial domain instead of DCT transform to extract the embedded watermark in the spatial domain based on the statistical rule and the method that “first to select the optimum sub-watermark from 4 sub-watermarks, then combine the optimum sub-watermarks to the final watermark,” i.e., “first to select, second to combine,” which is different from the method of [Nasir et al. \(2010\)](#). Experimental results prove that the proposed method not only can resolve the non-blind extraction problem, but also can embed and extract watermark in the spatial domain instead of the DCT domain.

The rest of this paper is organized as follows. Section 2 introduces the technique of modifying DC coefficients in spatial domain. Section 3 gives the procedures of the watermark embedding and extraction. The experimental results prove

the performance of the proposed method in Sect. 4. Finally, Sect. 5 concludes this paper.

2 The technique of modifying DC coefficients in spatial domain

2.1 The important feature of DC coefficient

DCT is a kind of transform domain methods in the field of real number, whose transform kernel is the cosine function. An image can be transformed from the spatial domain to DCT domain by 2-D DCT, and the image can also be restored from DCT domain to the spatial domain via 2-D inverse DCT.

For a $M \times N$ image $f(x, y)$ ($x = 0, 1, 2, \dots, M - 1, y = 0, 1, 2, \dots, N - 1$), 2-D DCT is given as follows:

$$C(u, v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{\pi(2x+1)u}{2M} \times \cos \frac{\pi(2y+1)v}{2N} \quad (1)$$

where M and N are the row and the column size of $f(x, y)$, u and v are the horizontal and the vertical frequency ($u = 0, 1, 2, \dots, M - 1, v = 0, 1, 2, \dots, N - 1$), and $C(u, v)$ is DCT coefficient of image $f(x, y)$.

$$\alpha_u = \begin{cases} \sqrt{1/M}, & u = 0 \\ \sqrt{2/M}, & 1 \leq u < M - 1 \end{cases}, \quad \alpha_v = \begin{cases} \sqrt{1/N}, & v = 0 \\ \sqrt{2/N}, & 1 \leq v < N - 1 \end{cases} \quad (2)$$

DCT coefficients of an image include one DC coefficient and some alternating current (AC) coefficients with different frequencies. From Eq. (1), DC coefficient can be obtained by

$$DC = C(0, 0) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \quad (3)$$

As can be seen from Eq. (3), DC coefficient can be directly obtained in spatial domain without DCT transform.

2.2 Modifying DC coefficients in the spatial domain rather than in DCT domain

As is mentioned above, DC coefficient can be directly obtained in the spatial domain. When DC coefficient of the image block has been changed in the DCT domain, the value of each pixel in the spatial domain will be changed after inverse DCT, that is, the modified quantity of each pixel of the image block is decided by the changed quantity of DC coefficient. Now, the key problem is how to determine the

modified quantity of each pixel in the spatial domain according to the changed quantity of DC coefficient in DCT domain.

According to DCT principle, the inverse DCT of the image $f(x, y)$ is described as following.

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v C(u, v) \cos \frac{\pi(2x+1)u}{2M} \times \cos \frac{\pi(2y+1)v}{2N} \quad (4)$$

The inverse DCT in Eq. (4) can be rewritten by

$$f(x, y) = \frac{1}{\sqrt{MN}} \text{DC} + \text{AC}(x, y) \quad (5)$$

where $\text{AC}(x, y)$ is the reconstructed image from the set of AC coefficients.

Suppose the host image is represented by

$$f(x, y) = \left\{ \begin{array}{l} f_{i,j}(m, n), 0 \leq i < \frac{M}{b}, 0 \leq j < \frac{N}{b}, \\ 0 \leq m, n < b \end{array} \right\} \quad (6)$$

where M, N are the row and the column size of the host image, the host image is divided into $i \times j$ non-overlapped blocks with $b \times b$ pixels. The indexes of each block are represented by (i, j) , and (m, n) is the pixel position in each block.

When embedding watermark W into DC coefficient of the (i, j) -th block, the modified quantity of DC coefficient is denoted as $\Delta M_{i,j}$. According to Eq. (3), the traditional process of embedding the watermark into DC coefficient of the (i, j) -th non-overlapped $b \times b$ block is given by

$$\text{DC}'_{i,j} = \text{DC}_{i,j} + \Delta M_{i,j} \quad (7)$$

where $\text{DC}_{i,j}$ is DC coefficient of the (i, j) -th block, $\text{DC}'_{i,j}$ is the modified DC coefficient with increment $\Delta M_{i,j}$.

According to Eq. (5), the recovered image block $f'_{i,j}(m, n)$ can be described as follows.

$$f'_{i,j}(m, n) = \frac{1}{b} \text{DC}'_{i,j} + \text{AC}_{i,j}(m, n) \quad (8)$$

Using Eqs. (6) and (7), (8) can be rewritten as

$$\begin{aligned} f'_{i,j}(m, n) &= \frac{1}{b} \text{DC}'_{i,j} + \text{AC}_{i,j}(m, n) \\ &= \frac{1}{b} (\text{DC}_{i,j} + \Delta M_{i,j}) + \text{AC}_{i,j}(m, n) \\ &= \frac{1}{b} \Delta M_{i,j} + \frac{1}{b} \text{DC}_{i,j} + \text{AC}_{i,j}(m, n) \end{aligned}$$

$$\begin{aligned} &= \frac{1}{b} \Delta M_{i,j} + f_{i,j}(m, n) \\ &= \text{PM}_{i,j} + f_{i,j}(m, n) \end{aligned} \quad (9)$$

where $\text{PM}_{i,j}$ denotes the modified quantity of each pixel in the spatial domain, and it is defined by

$$\text{PM}_{i,j} = \frac{1}{b} \Delta M_{i,j} \quad (10)$$

In Eq. (9), it is shown that for the host image $f(x, y)$, the procedure of embedding watermark into DC coefficients in DCT domain can also be performed directly in the spatial domain rather than in DCT domain.

3 The proposed watermarking scheme

In this paper, a new blind digital image watermarking algorithm is proposed by combining spatial domain with frequency domain. Firstly, the original binary watermark is divided into four sub-watermarks, and the blue component of the color host image is also divided into 16 sub-images. When embedding the watermark, the distribution features and quantization table of DC coefficients are used and the pixel values are directly modified in the spatial domain, which means DC coefficients in DCT domain are modified indirectly. All of the four sub-watermarks can be repeatedly embedded into the 16 sub-images for 4 times based on the security key Key_1 , which can effectively improve the security and robustness of watermark. Moreover, the key-based quantization step will be utilized to extract the watermark with blind manner.

3.1 Watermark preprocessing

The preprocessing of watermark is one of the key steps in the watermarking algorithm, and it will directly influence the robustness and security of watermark, which includes the following two steps.

Firstly, the 32×32 original watermark is divided into four sub-watermarks W_i with size 32×8 ($1 \leq i \leq 4$), which will decrease the probability of whole watermark be attacked and enhance the robustness of watermark.

Secondly, the key-based Hash pseudo-random permutation algorithm based on MD5 is utilized to permute the sub-watermarks with different keys K_i ($1 \leq i \leq 4$).

It should be pointed out that, in the proposed method, MD5 is applied to the specific Hash function (Rivest April 1992), which makes it difficult for the third party to extract the watermark integrally without the keys. Hence, this proposed algorithm is of higher security. The permuting process of the original binary watermark W is shown in Fig. 1.

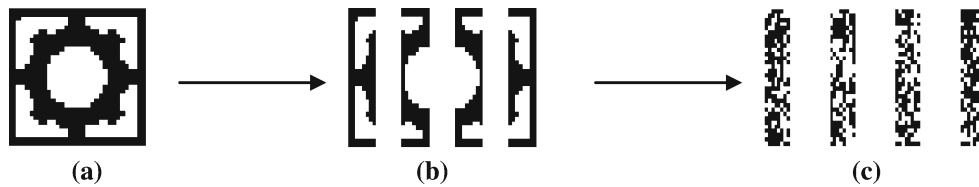


Fig. 1 The permuting process of original watermark: (a) original watermark, (b) sub-watermark blocks and (c) permuted sub-watermark blocks

3.2 Watermark embedding scheme

Because, the sensors in the human eye are called as cones which are responsible for color vision. The cones could be separated into three major sensing categories as red, green and blue. Nearly 65% of the cones are sensitive to red color, 33% are sensitive to green color and just 2% are sensitive to blue color (Vaishnavi and Subashini 2015). That is, the human visual system is much less sensitive to blue colors than to others (Kutter and Winkler 2002). Hence, the permuted watermark is embedded into the blue component of the host image in this paper. Firstly, the blue component of the host image is firstly divided into many sub-images and each host sub-image is further divided into sub-blocks with 8×8 pixels, and DC coefficient of each sub-block is calculated. Then, the modified quantity of DC coefficient is decided according to the watermark information and DC coefficient of the present sub-block. Finally, one watermark bit is embedded into one pixel block by modifying the pixel value via Eq. (9). The proposed embedding watermark process is shown in Fig. 2, and the detail steps of embedding watermark are given as follows.

Step 1 Obtain sub-image of the blue component.

In order to improve the robustness of watermarking, the 512×512 blue component of the original host image I is divided into 16 sub-images $I_s (1 \leq s \leq 16)$ with size 128×128 pixels based on the security key Key1

Step 2 Obtain embedding block.

Each sub-image is divided into 256 non-overlapped embedding blocks with 8×8 pixels. Thus, the whole host image can be divided into 4096 non-overlapped embedding blocks.

Step 3 Obtain DC coefficients in the spatial domain.

The DC coefficient of embedding block is further calculated according to Eq. (3).

Step 4 Create the quantization table QA(k) and QB(k), which are created by the quantification step Δ based on the secret key Key2.

$$QA(k) = \min(DC_{i,j}) + (2k - 4) \times \Delta \tag{11}$$

$$QB(k) = \min(DC_{i,j}) + (2k - 5) \times \Delta \tag{12}$$

where $1 \leq k \leq \text{round}((\max(C_{i,j}(0,0)) + 2\Delta)/(2\Delta)) - \text{round}((\min(C_{i,j}(0,0)) - 2\Delta)/(2\Delta))$, $\min(\cdot)$ and $\max(\cdot)$

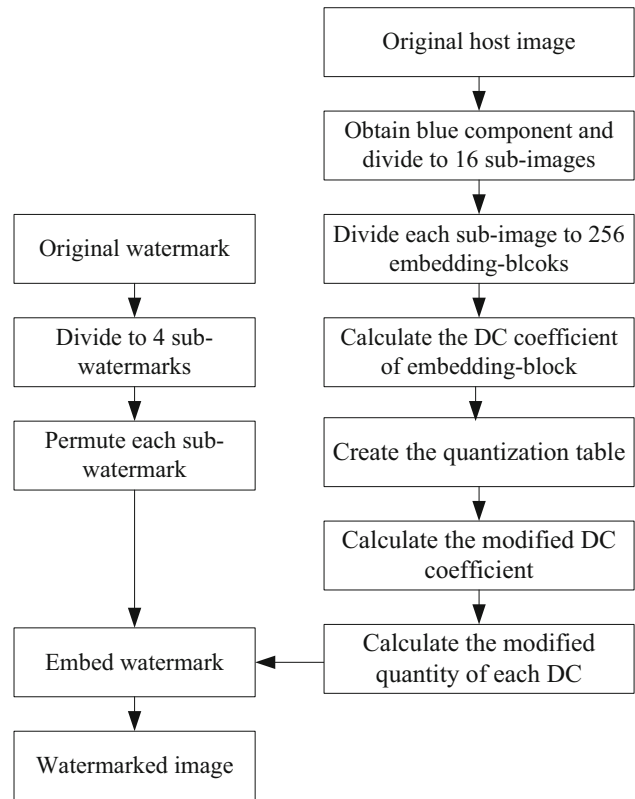


Fig. 2 The diagram of embedding watermark process

denote the minimum and the maximum of the DC coefficient of all embedding non-overlapped blocks with 8×8 pixels in the host image, respectively, $i (1 \leq i \leq 64)$ is the horizontal position of non-overlapped embedding block in the host image, $j (1 \leq j \leq 64)$ is the vertical position of non-overlapped embedding block in the host image, and $\text{round}(\cdot)$ is the integral function.

Step 5 Calculate the modified DC coefficient $DC'_{i,j}$.

The modified value $DC'_{i,j}$ of the DC coefficient is calculated by

$$DC'_{i,j} = \begin{cases} QA(k), & \text{if } W(i,j) = 1 \text{ and } \min(\text{abs}(DC_{i,j} - QA(k))) \\ QB(k), & \text{if } W(i,j) = 0 \text{ and } \min(\text{abs}(DC_{i,j} - QB(k))) \end{cases} \tag{13}$$

where $\text{abs}(\cdot)$ is the absolute function.

Fig. 3 The embedded positions of sub-watermarks

W_2	W_1	W_2	W_1
W_4	W_3	W_4	W_3
W_1	W_2	W_1	W_2
W_3	W_4	W_3	W_4

Step 6 Calculate the modified quantity of each DC coefficient.

The modified quantity $\Delta M_{i,j}$ of each DC coefficient can be calculated by Eq. (14).

$$\Delta M_{i,j} = DC'_{i,j} - DC_{i,j} \quad (14)$$

Step 7 Embedding watermark.

By using Eqs. (9) and (10), the pixel value can be modified by $\Delta M_{i,j}$ in the spatial domain rather than in DCT domain, that is, one binary watermark bit is embedded into one embedding block. In this procedure, the modified quantity is between 0 and 2.5, which will enhance the invisibility of watermark.

By repeating the procedures of Steps 3–7, each sub-watermark W_i ($1 \leq i \leq 4$) can be embedded into four different positions according to the order number in Fig. 3. Thus, each sub-watermark is embedded into the host image for four times and the watermarked image I' .

3.3 Watermark extraction scheme

When extracting the watermark, the quantization step is used to directly extract watermark from DC coefficients without the original host image and original watermark. Firstly, the four sub-watermarks of each sub-image are extracted. Then, the optimum sub-watermark is obtained by the statistics-based optimum. Finally, these optimum sub-watermarks are combined to attain the whole watermark. The proposed embedding watermark process is shown in Fig. 4, the detailed steps are listed as follows.

Step 1 Obtaining DC coefficients in the spatial domain.

The watermarked image is processed by using the similar operation of Steps 1–2 in Sect. 3.2, and DC coefficient $DC'_{i,j}$ of each embedded block is obtained by Eq. (3).

Step 2 Extracting the sub-watermarks.

According to Eq. (15), the quantization step Δ based on key Key2 is used to extract the watermark $W'_{i,j}$ in $DC'_{i,j}$, until all sub-watermarks are extracted.

$$W'_{i,j} = \text{mod} \left(\text{ceil} \left(DC'_{i,j} / \Delta \right), 2 \right) \quad (15)$$

where $W'_{i,j}$ presents the extracted watermark from the (i, j) -th embedding block, and $\text{mod}(\cdot)$ is modulo operation.

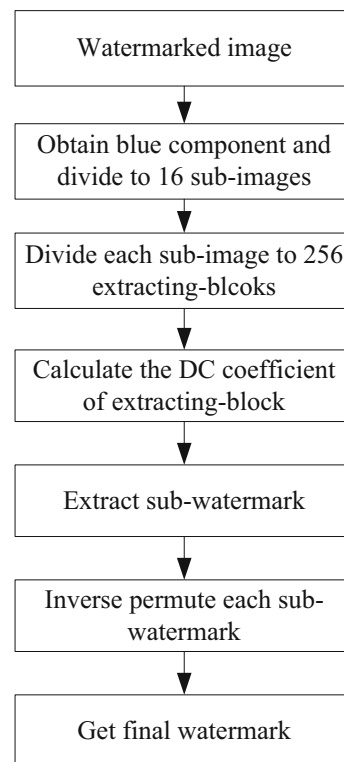


Fig. 4 The diagram of extracting watermark process

Step 3 Getting the optimum sub-watermark.

Because each sub-watermark is repeatedly embedded for 4 times, 4 similar or identical watermarks of the same sub-watermark can be extraction. Hence, the optimum sub-watermark $W^*(m, n)$ ($1 \leq m \leq 32$, $1 \leq n \leq 8$) of each sub-watermark can be statistically computed by Eq. (16).

$$W^*(m, n) = \begin{cases} 1, & \text{if } \text{sum}(W(m, n)) \geq 2 \\ 0, & \text{if } \text{sum}(W(m, n)) < 2 \end{cases} \quad (16)$$

where $W(m, n)$ is the watermark bit in the coordinate (m, n) of four sub-watermarks, and $\text{sum}(\cdot)$ is the sum function.

Step 4 Obtaining the final watermark.

By using the secret key K_i ($1 \leq i \leq 4$), Hash inverse permutation is performed on the 4 optimum sub-watermarks, respectively. Then, these permuted sub-watermarks are combined to obtain the whole extracted watermark image W' .

In summary, the proposed method firstly selects the optimum sub-watermark of each part via the statistic feature of the extracted 4 sub-watermarks, and then combines the selected optimum sub-watermarks to form the final watermark. Hence, this proposed method, i.e., “first to select the optimum sub-watermark from 4 sub-watermarks, then combine the optimum sub-watermarks to the final watermark,” not only extract the optimum watermark to improve the watermark robustness, but also can achieve the purpose of blind extraction.

4 Experimental results and discussion

In this paper, the binary image of size 32×32 is used as original watermark, as shown in Fig. 1a, and all 24-bit 512×512 color images in the CVG-UGR image database are used as the host images (University of Granada 2012). For limitation space of the paper, only four 24-bits color images, as shown in Fig. 5, are taken for example. By considering the trade-off between the robustness and the invisibility of the watermark, let quantization step $\Delta = 20$.

For evaluating the performance of the proposed method, the original color image I is re-arranged to two-dimensional host image H by the order of R, G and B component, and the watermarked image I' is also re-arranged to two-dimensional watermarked image H' by the order of R, G and B component. The peak signal-to-noise ratio (PSNR) in Eq. (17) is utilized to measure the similarity degree between the two-dimensional image H and the watermarked two-dimensional image H'

$$PSNR = 10 \lg \frac{M \times N \times \max\{[H(x, y)]^2\}}{\sum_{x=1}^M \sum_{y=1}^N [H(x, y) - H'(x, y)]^2} \quad (17)$$

where $H(x, y)$, $H'(x, y)$ present the value of pixel (x, y) in the two-dimensional host image and the watermarked one, and M, N denote its width and height, respectively.

Moreover, structural similarity (SSIM) index measurement developed by Wang et al. (2004) was considered to be correlated with the quality perception of the human visual system (HVS). The SSIM is designed by modeling image distortion that combines three factors: loss of correlation, luminance distortion and contrast distortion, and it is defined as:

$$SSIM(H, H') = l(H, H')c(H, H')s(H, H') \quad (18)$$

where

$$\begin{cases} l(H, H') = (2\mu_H\mu_{H'} + C_1) / (\mu_H^2 + \mu_{H'}^2 + C_1) \\ c(H, H') = (2\sigma_H\sigma_{H'} + C_2) / (\sigma_H^2 + \sigma_{H'}^2 + C_2) \\ s(H, H') = (\sigma_{HH'} + C_3) / (\sigma_H\sigma_{H'} + C_3) \end{cases} \quad (19)$$

The first term in Eq. (19) measures the closeness of the two images' mean luminance (μ_H and $\mu_{H'}$). The second term

measures the closeness of the contrast of the two images, and the contrast is measured by the standard deviation σ_H and $\sigma_{H'}$. The third term is the structure comparison function which measures the correlation coefficient between the two images H and H' . Note that $\sigma_{HH'}$ is the covariance between H and H' . The positive constants C_1, C_2 and C_3 are used to avoid a null denominator. The positive values of the SSIM index are in $[0, 1]$.

In addition, in order to measure the robustness of the watermark, we use the normalized correlation (NC) between the original watermark W and the extracted watermark W' , which is shown as follows.

$$NC = \frac{\sum_{x=1}^P \sum_{y=1}^Q (W(x, y) \times W'(x, y))}{\sqrt{\sum_{x=1}^P \sum_{y=1}^Q [W(x, y)]^2} \sqrt{\sum_{x=1}^P \sum_{y=1}^Q [W'(x, y)]^2}} \quad (20)$$

where P and Q denote the row and the column size of the original watermark image, and (x, y) is the pixel position of watermark image.

4.1 Testing the watermark invisibility

Generally, a larger PSNR or SSIM indicates that the watermarked image resembles the original host image more closely, which means that the watermarking method makes the watermark more imperceptible. A higher NC reveals that the extracted watermark resembles the original watermark more closely. If a method has a higher NC value, it is more robust.

Table 1 shows the comparison results of watermark invisibility between the proposed method, methods of Das et al. (2014) and Kalra et al. (2015). It can be seen from Table 1, all embedded watermarks can be completely extracted from the watermarked images without any attacks (all NC values are 1), and the proposed algorithm has better invisibility (its PSNR values are more than 45 db and SSIM values are bigger than other methods). This is because the modified quantity of each pixel ranges from 0 to 2.5 according to the watermark bit and DC coefficient. Less modified amplitude will get a better invisibility and obtain bigger PSNR or SSIM values. Hence, the proposed method can obtain higher watermark invisibility than other methods.

Fig. 5 Original host images: **a** Lena, **b** Baboon, **c** Avion, and **d** Peppers

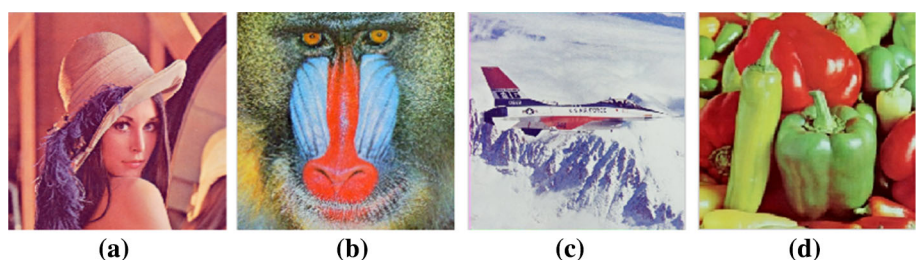


Table 1 The invisibility comparison results between the different methods without any attacks

Image	PSNR (db)			SSIM			NC		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
Lena	49.9898	41.7801	42.0109	0.9872	0.9704	0.9787	1.0000	1.0000	1.0000
Baboon	49.8901	40.2446	36.1103	0.9957	0.9893	0.9754	1.0000	1.0000	1.0000
Avion	49.8664	40.7932	39.7644	0.9854	0.9872	0.9851	1.0000	1.0000	1.0000
Peppers	50.0839	41.0122	42.6843	0.9859	0.9733	0.9816	1.0000	1.0000	1.0000

4.2 Testing the watermark robustness

In practice, the watermarked image will be subjected to a variety of distortions before reaching the detector. Watermarks designed to survive legitimate and everyday usage of image, e.g., JPEG compression, adding noise and filtering, are referred to as robust watermark. To verify the watermark robustness of the proposed method, all watermarked images are attacked by common image processing operations (such as JPEG compression, adding Salt-and-Pepper noise, adding Gaussian noise, median filtering, and mosaic piecing attack) and geometrical distortions (such as scaling, rotation, affine transform, and cropping). At the same time, the proposed method is compared with methods of Das et al. (2014) and Kalra et al. (2015) in term of NC.

Lossy compression techniques are commonly used to encode color image for efficient storage and communication. The watermark robustness against the attack of lossy compression is an important performance to be evaluated. In this simulation, JPEG compression is employed to attack the watermarked image. It is shown in Table 2 that the original watermark can be extracted from all attacked images when compression factor is 70 by all compared method, which because the NC value is more than 0.75. Relatively, the method of Kalra et al. (2015) is the best method to resist the compression attack. The proposed method has better robust than method of Das et al. (2014) in most cases.

The watermarked image is easily and inevitably attacked by adding noise in the image transmission. Hence, adding noise is a classical attack and can affect the embedded watermark. Table 3 shows the results of the extracted watermark from the image attacked by adding Salt-and-Pepper noise with different noise intensities. It can be seen from it that the watermark still can be extracted normally when the noise intensity is 0.012 in the proposed method and method of Kalra et al. (2015), but the watermark can hardly be extracted when noise intensity is below 0.006 with method of Das et al. (2014). Relatively, the proposed algorithm has stronger robustness (NC value is bigger than 0.75) to resist noise adding attack than other methods of Das et al. (2014) and

Kalra et al. (2015). Moreover, adding Gaussian noise is performed on the watermarked image. The watermarked images were tested against Gaussian noise with mean = 0 and different variance values from 0 to 0.15. Table 4 shows the comparison results of extracted watermark by different methods. Relatively, the proposed method and method of Kalra et al. (2015) have better robust than the method of Das et al. (2014).

Filtering attack is one of the classical attacks. Since the embedded watermark can be removed by the filter with different sizes, the median filtering and Butterworth low-pass filtering are used to attack the watermarked image. Table 5 gives the comparison results of extracted watermark from the watermarked image attacked by median filtering with different sizes. It is obvious that when the filter template size is odd, the watermark robustness is superior to that with the even size. In addition, Table 6 shows the comparison results of the extracted watermark from the watermarked image attacked by Butterworth low-pass filtering with cut-off frequency 50Hz and different fuzzy radii N , which illustrates that the watermark can be extracted in the whole test range. However, it is difficult for method of Das et al. (2014) to extract the watermark information in the Baboon image (because NC value is smaller than 0.75). Hence, the algorithm in this paper has stronger robustness to resist median-filtering attack and Butterworth low-pass filtering attack than other methods of Das et al. (2014) and Kalra et al. (2015).

In the image processing, the image rotation is one of the geometric operation, which will lead to the change of image size and image pixel values. Hence, the embedded watermark will be affected by rotation operation. The watermarked image is rotated by 30°, 60°, 90°, 120°, 180° and 270° in clockwise direction, respectively, and the watermark is extracted by re-rotating the image in counter-clockwise direction. In the rotation process, the size of the watermarked image will be changed. For extracting watermark, the cropping and the scaling operations are also needed to make the size of the watermarked image be 512 × 512, that is, the combined attacks, e.g., rotation+cropping+scaling, are performed on the watermarked image. Table 7 gives the

Table 2 The comparison of extracted watermark by different methods after JPEG compression attacks

JPEG compression factor	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
	10	0.7673	0.6221	0.6359	0.5760	0.5010	0.7991	0.2097	0.2777	0.6345	0.8594	0.5671
20	0.7304	0.7166	0.7222	0.5991	0.4901	0.8023	0.3917	0.4188	0.7009	0.8041	0.6102	0.7818
30	0.6728	0.6730	0.8543	0.6567	0.5116	0.8601	0.6774	0.5693	0.8447	0.6544	0.6539	0.8656
40	0.6659	0.6207	0.9782	0.7211	0.6842	0.9644	0.7212	0.6309	0.9605	0.7097	0.6637	0.9631
50	0.7166	0.6792	0.9993	0.6959	0.6733	0.9902	0.6959	0.6675	0.9708	0.6659	0.7021	0.9807
60	0.7350	0.6809	0.9996	0.7512	0.7312	0.9973	0.7419	0.7123	0.9991	0.7857	0.7322	0.9932
70	0.7650	0.7962	1.0000	0.7719	0.7868	1.0000	0.8111	0.7863	1.0000	0.8341	0.7718	1.0000
80	0.9124	0.8747	1.0000	0.9355	0.8419	1.0000	0.9286	0.8712	1.0000	0.9539	0.8613	1.0000
90	0.9931	0.9999	1.0000	0.9793	0.9809	1.0000	0.9839	0.9788	1.0000	0.9954	0.9435	1.0000
100	1.0000	1.0000	1.0000	1.0000	0.9990	1.0000	1.0000	0.9861	1.0000	1.0000	0.9718	1.0000

Table 3 The comparison of extracted watermark by different methods after Salt-and-Pepper noise attacks

Salt-and-Pepper noise	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
	0.002	1.0000	0.8120	1.0000	0.9908	0.8201	0.9901	0.9977	0.8109	0.9963	1.0000	0.8009
0.004	0.9724	0.7809	0.9632	0.9816	0.7741	0.9803	0.9839	0.7907	0.9755	0.9908	0.7756	0.9805
0.006	0.9378	0.7632	0.9209	0.9700	0.7655	0.9633	0.9770	0.7742	0.9666	0.9654	0.7613	0.9573
0.008	0.9032	0.7212	0.8978	0.9608	0.7258	0.9504	0.9309	0.7193	0.9281	0.9447	0.7116	0.9461
0.010	0.9009	0.6731	0.8899	0.9032	0.7004	0.8915	0.8917	0.7074	0.8909	0.9378	0.7866	0.9244
0.012	0.8687	0.6517	0.8417	0.9055	0.6667	0.8885	0.8594	0.6762	0.8406	0.9124	0.7113	0.8588

Table 4 The comparison of extracted watermark by different methods after Gaussian noise attacks

Gaussian attack (%)	Lena		Baboon		Avion		Peppers				
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)			
(0, 5)	1.0000	0.9739	1.0000	0.9977	0.9862	1.0000	1.0000	0.9885	1.0000	0.9671	0.9972
(0, 10)	0.9816	0.8816	0.9663	0.9816	0.8699	1.0000	0.9862	0.8478	0.9855	0.8922	0.9464
(0, 15)	0.9654	0.8231	0.9259	0.9378	0.8108	1.0000	0.9562	0.8301	0.9321	0.8525	0.8709

Table 5 The comparison of extracted watermark by different methods after median-filter attacks

Median filtering	Lena		Baboon		Avion		Peppers				
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)			
2 × 2	0.9493	0.8316	0.9339	0.7442	0.6988	0.7476	0.9516	0.8548	0.9488	0.8133	0.9322
3 × 3	0.9977	0.9118	0.9451	0.8848	0.8771	0.7543	0.9977	0.9401	0.9891	0.9233	0.9394
4 × 4	0.9147	0.7607	0.9129	0.7327	0.6461	0.7003	0.9585	0.7491	0.9311	0.7906	0.9349
5 × 5	0.9839	0.8909	0.9882	0.7650	0.8709	0.7436	0.9724	0.8899	0.9615	0.9011	0.9817
6 × 6	0.8802	0.7444	0.8755	0.7304	0.6503	0.7223	0.9401	0.8405	0.9249	0.7589	0.8909
7 × 7	0.9263	0.7908	0.9135	0.7535	0.6944	0.7516	0.9562	0.8213	0.9418	0.8094	0.9144

Table 6 The comparison of extracted watermark by different methods after Butterworth low-pass filtering attacks

Butterworth low-pass filtering	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
(1, 50)	0.9654	0.8715	0.9501	0.7857	0.6771	0.7666	0.9700	0.8699	0.9599	0.9816	0.8713	0.9801
(2, 50)	0.9954	0.8905	0.9700	0.8203	0.7382	0.8044	0.9677	0.8312	0.9503	0.9862	0.8809	0.9714
(3, 50)	0.9908	0.8832	0.9699	0.8272	0.7199	0.8144	0.9585	0.8612	0.9499	0.9908	0.8756	0.9888
(4, 50)	0.9839	0.8799	0.9633	0.8341	0.7291	0.8031	0.9514	0.8372	0.9435	0.9888	0.8733	0.9756
(5, 50)	0.9724	0.8666	0.9600	0.8203	0.7751	0.7991	0.9447	0.8453	0.9317	0.9885	0.8692	0.9619
(6, 50)	0.9747	0.8591	0.9519	0.8041	0.7813	0.7803	0.9424	0.8480	0.9233	0.9862	0.8625	0.9776

Table 7 The comparison of extracted watermark by different methods after rotation attacks

Rotation	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
30	0.7612	0.6902	0.7448	0.7125	0.6301	0.7028	0.7408	0.6977	0.7309	0.7851	0.6902	0.7719
60	0.7709	0.6991	0.7522	0.7705	0.5997	0.7309	0.7799	0.7208	0.7641	0.7903	0.6994	0.7801
90	0.8917	0.8650	0.8443	0.8581	0.6533	0.8344	0.9009	0.6789	0.8999	0.8909	0.8617	0.8788
120	0.9670	0.9545	0.9221	0.9571	0.7984	0.9109	0.9862	0.9312	0.9559	0.9677	0.9003	0.9673
180	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
270	0.8899	0.8561	0.8444	0.8548	0.6728	0.8401	0.8895	0.6807	0.8817	0.8877	0.8701	0.8787

Table 8 The comparison of extracted watermark by different methods after mosaic attacks

Mosaic piecing	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
2 × 2	1.0000	1.0000	1.0000	1.0000	0.8433	0.9978	1.0000	1.0000	0.9988	1.0000	1.0000	1.0000
3 × 3	0.9954	0.9716	0.9818	0.9341	0.6322	0.9312	0.9908	0.9877	0.9772	0.9908	0.9613	0.9807
4 × 4	1.0000	0.9833	0.9912	1.0000	1.0000	0.9871	1.0000	1.0000	0.9899	1.0000	1.0000	0.9977
5 × 5	0.8963	0.8709	0.8189	0.7327	0.6412	0.7341	0.9378	0.8907	0.9178	0.9055	0.8533	0.8908
6 × 6	0.9055	0.8644	0.8667	0.7327	0.6503	0.7483	0.9009	0.8619	0.8909	0.8502	0.8401	0.8469
7 × 7	0.8318	0.8008	0.7901	0.6866	0.5907	0.6688	0.8664	0.8431	0.8433	0.8134	0.7983	0.8364

Table 9 The comparison of extracted watermark by different methods after scaling attacks

Scaling	Lena			Baboon			Avion			Peppers		
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)
0.25	0.9954	0.9439	0.9745	0.8111	0.7731	0.7988	0.9816	0.9642	0.9788	0.9978	0.9807	0.9803
0.33	0.9677	0.9103	0.9346	0.7765	0.6874	0.7008	0.9724	0.9631	0.9334	0.9124	0.9005	0.8988
0.5	1.0000	0.9602	0.9809	0.9885	0.9242	0.9415	0.9931	0.9708	0.9617	1.0000	0.9863	0.9736
1	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
2	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

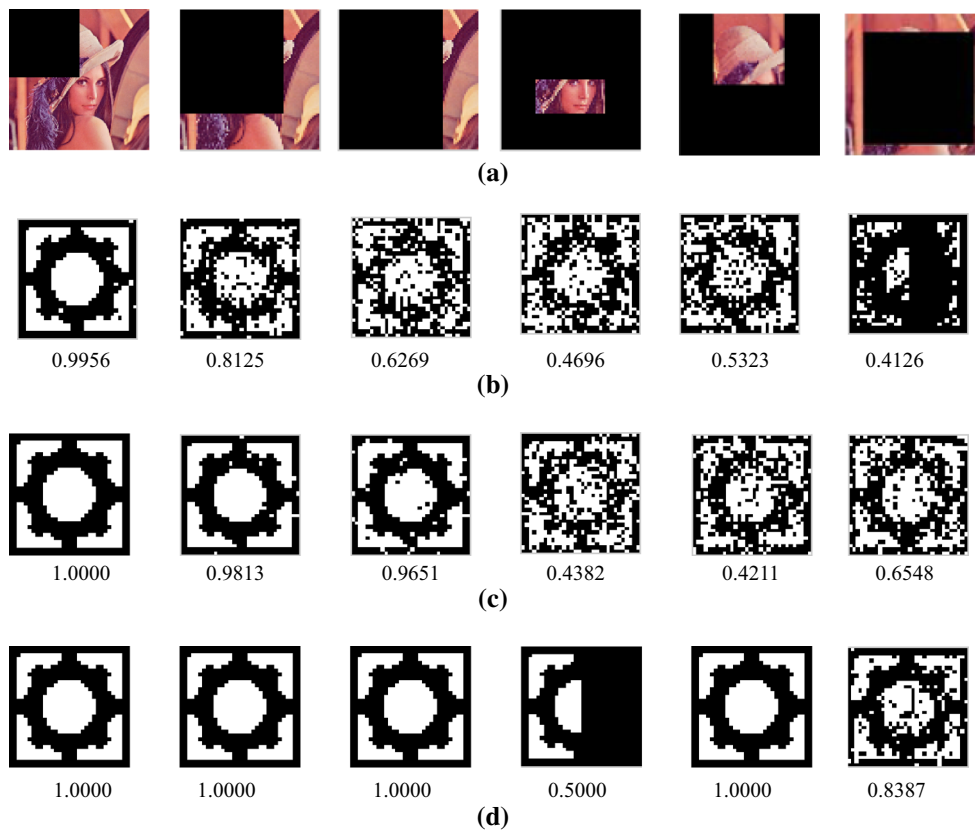


Fig. 6 The comparison of extracted watermark by different methods after cropping attacks: **a** cropped watermarked image, **b** extracted watermark from (a) by method of Das et al. (2014) (NC), **c** extracted watermark from (a) by method of Kalra et al. (2015) (NC), and **d** extracted watermark from (a) by the proposed method (NC)

comparison result of the extracted watermark from the watermarked image attacked by rotation, and shows the robustness of the proposed algorithm is superior to other methods of Das et al. (2014) and Kalra et al. (2015).

The mosaic processing has very simple principle and can directly change the pixel values in the pixel template by average operation. Table 8 lists the comparison results of the extracted watermark from the watermarked image attacked by mosaic processing with different sizes, which shows the robustness that measured by NC value is decreasing with increasing the size of mosaic and the robustness in the proposed method is superior to those of Das et al. (2014) and Kalra et al. (2015).

The scaling operation includes scaling up and scaling down, in which the pixel values are modified by interpolation computing. Table 9 shows the comparison results of the extracted watermark from the watermarked image attacked by scaling with different ratios, which shows the robustness that measured by NC value is weaker when scaling down the watermarked image. Relatively, the proposed method has higher robust than those of Das et al. (2014) and Kalra et al. (2015). The reason can be explained as follows: in the scaling test, the watermarked image of size 512×512 is scaled up or down by the scaling ratio, and then resize the scaled

image to the original size 512×512 for extracting watermark. When scaled up is performed, the interpolation is involved, and the watermarked image has little influence when resize to the original size. Hence, the robustness of scaling with ratio more than 1 is good, but it is bad when the scaling ratio is less than 1.

Obviously, the cropping attack can cut part of image pixel, which directly decides the quality of the extracted watermark. Figure 6 is the results of the extracted watermark from the watermarked Lena image attacked by cropping with different sizes in different positions, in which Fig. 6a is the cropped watermarked image, Fig. 6b–d shows the extracted watermarks and NC values by methods Das et al. (2014), Kalra et al. (2015) and the proposed one, respectively. By comparison, it is found the proposed method has strong robustness to resist cropping attack because of each sub-watermark is embedded for 4 times in different positions of the original host image.

In addition, various affine transform geometric attacks are performed on the watermarked image. Table 10 shows the results obtained by different methods, where Attack 1 denotes Resize 0.8 times at X direction, Attack 2 denotes Resize 1.2 times at X direction, Attack 3 denotes Resize 0.8 times at Y direction, Attack 4 denotes Resize 1.2 times at Y direc-

Table 10 The comparison of extracted watermark by different methods after affine transform attacks

Attack	Lena		Baboon		Avion		Peppers					
	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)	Method of Kalra et al. (2015)	Proposed method	Method of Das et al. (2014)				
Attack 1	0.9972	0.8977	0.9840	0.8249	0.7008	0.8099	0.9926	0.9077	0.9806	0.9999	0.9145	0.9963
Attack 2	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Attack 3	0.9968	0.8649	0.9831	0.8302	0.7132	0.8133	0.9875	0.9115	0.9764	0.9989	0.9206	0.9833
Attack 4	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Attack 5	1.0000	0.9088	0.9769	1.0000	0.8769	0.9433	1.0000	0.8809	0.9633	1.0000	0.9103	0.9636
Attack 6	1.0000	0.9109	0.9766	1.0000	0.8801	0.9507	1.0000	0.8881	0.9701	1.0000	0.9099	0.9688
Attack 7	1.0000	0.9099	0.9911	1.0000	0.9445	0.9466	1.0000	0.8991	0.9888	1.0000	0.9864	0.9709
Attack 8	1.0000	0.9113	0.9899	1.0000	0.9501	0.9511	1.0000	0.9002	0.9862	1.0000	0.9855	0.9721

tion, Attack 5 denotes Line transform [1.013, 0.008; 0.011, 1.008], Attack 6 denotes Line transform [1.007, 0.010; 0.010, 1.012], Attack 7 denotes Removing row 17 column 5, and Attack 8 denotes Removing row 5 column 17. Because the proposed method selects the optimum sub-watermark from 4 sub-watermarks and combine the sub-watermarks to the final watermark, the final watermark will better than other methods.

It can be seen from the above comparison results that the proposed method has better robustness than other methods in most cases. The main feature in the proposed method is based on the idea “first to select the optimum sub-watermark from 4 sub-watermarks, then combine the sub-watermarks to the final watermark”, which is different with Nasir et al. (2010), i.e., “first to combine sub-watermark to 4 whole watermarks, then select the optimum final watermark from the whole watermarks.”

4.3 The execution time comparison

In our experiments, a laptop computer with a duo Intel CPU at 2.007 GHZ, 4.00 GB RAM, Win 7, MATLAB 7.10.0 (R2010a) is used as the computing platform. As can be seen from the Table 11, the whole execution time of the proposed method is 5.9972 s with standard variation 0.0871 when the DC coefficient is directly obtained in the spatial domain, but the whole execution time is 6.9478 s with standard variation 0.0507 in Das et al. (2014), and 7.0928 s with standard variation 0.0661 in Kalra et al. (2015) which performed in DCT and DWT domain. Since 2-DCT and inverse 2-DCT were applied to the modified DCT coefficients of each embedding block to rebuild the watermarked image when embedding the watermark in Das et al. (2014), Kalra et al. (2015), and 2-DCT was also performed independently for every block of the watermarked image when extracting the watermark in Das et al. (2014), Kalra et al. (2015), which need more time than in the spatial domain. Moreover, 2-DWT is also used in Kalra et al. (2015). Hence, the proposed method has higher efficiency than (Das et al. 2014; Kalra et al. 2015).





4.4 The security analysis

In the proposed method, the security key Key1 is used to select the embedding position, the probability of locating all blocks is $1/(16 \times 4!)$; since the Hash pseudo-random algorithm based on MD5 with keys K_i ($1 \leq i \leq 4$) is used to permute the sub-watermarks, and the key space of MD5 is 128 bits, the probability of restoring right state is $1/2^{128} \times 1/2^{128} \times 1/2^{128} \times 1/2^{128}$; the key Key2 is used as the quantization step to determine the strength of embedding watermark and extracting watermark and its value is integer or float number between 0 and 255. When key Key2 is integer number, its probability of determining right number is

Table 11 The execution time comparison between different methods (s)

Method	Domain	Embedding time		Extracting time		Total time	
		Average value	Standard variation	Average value	Standard variation	Average value	Standard variation
Proposed method	Spatial domain	0.1948	0.0227	5.8023	0.0774	5.9972	0.0871
Method of Das et al. (2014)	DCT domain	3.7136	0.0411	3.2342	0.0201	6.9478	0.0507
Method of Kalra et al. (2015)	DCT domain	4.5712	0.0463	2.5216	0.0311	7.0928	0.0661

Fig. 7 The extracted watermark with different wrong keys

	Case 1	Case 2	Case 3	Case 4
key Key1	✓	✗	✓	✓
key K_i	✓	✓	✗	✓
key Key2	✓	✓	✓	✗
Extracted watermark				

$1/255 \approx 1/256$, the security of our algorithm only relies on the right private key Key1, Key2 and K_i ($1 \leq i \leq 4$). Thus there requires a tremendous number of colluding attackers (24×2^{524}), and this implies the probability of extracting right watermark is very lower. When key Key2 is float number, the value of Key2 cannot be determined, the probability of extracting right watermark is near to 0.

As can be seen from Fig. 7, the right watermark cannot be extracted when either the secret Key1 is wrong, or the secret Key2 is wrong or the secret K_i is wrong. If and only if all the three secret keys are right, the right watermark can be extracted and combined. Hence, the attacker can hardly extract the legal watermark image without any right keys, which enhance the security of watermarking.

4.5 The capacity analysis

In this paper, the capacity of watermark is also analyzed by the embedding rate. The embedding rate represented in bit per pixel (bpp) is the pure payload (i.e., the total amount of embedded bits minus that of all overhead information) ([Wu and Huang 2012](#)). Since the embedded watermark is 32×32 binary image and the host image is 512×512 color image

in this paper, the capacity is $(32 \times 32)/(512 \times 512 \times 3) = 0.0013(\text{bpp})$. The capacity of method of [Das et al. \(2014\)](#) is $(64 \times 63)/(512 \times 512) = 0.0154(\text{bpp})$, and the capacity of method of [Kalra et al. \(2015\)](#) is $(64 \times 64)/(512 \times 512) = 0.0156(\text{bpp})$. It is obviously that the proposed method has the lowest capacity, which because the 8×8 image block is only embedded one watermark information and all watermark information is repeat embedded into the host image for four times. Hence, we will consider how to improve the capacity of watermark when keeping the robustness and the invisibility.

In summary, the proposed method not only has higher watermark invisibility, but also has stronger robustness against the common image processing attacks and part of the geometric attacks. Moreover, the experimental results have proved the proposed method has higher efficiency and better security.

5 Conclusion

In this paper, we have proposed a blind watermarking based on DC coefficients in the spatial domain. When embedding

watermark, the principle of DC coefficient modification in DCT domain is used to repeatedly embed watermark in the spatial domain for four times, which can improve the invisibility and the robustness of watermark. Moreover, in this method the sub-watermark is extracted by the extraction rules without the original host image or the original watermark. Moreover, the statistical rule and the idea of “first to select the optimum sub-watermark from four sub-watermarks, then combine the optimum sub-watermarks to the final watermark” are proposed to combine the sub-watermarks. Experimental results have shown that the proposed algorithm has strong robustness against common image processing and geometric attacks. In the further work, the color image will be viewed as original watermark.

Acknowledgements The research was partially supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAET), Natural Science Foundation of China (61202111, 61572258), Natural Science Foundation of Shandong Province (ZR2014FM005), Key Science and Technology Plan Projects of Yantai City (2016ZH057), Department of Science and Technology of Shandong Province (2013GGB01231) and Shandong Province Important Research Plan Projects (2015GSF116001). The authors would like to thank anonymous referees for their valuable comments and suggestions which lead to substantial improvements of this paper.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

- Arcangelo Castiglione, Pizzolante R, De Santis A, Carpentieri B, Aniello Castiglione, Francesco Palmieri (2015) Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Gener Comput Syst* 43:120–134
- Chen B, Wornell GW (2001) Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Trans Inf Theory* 47(4):1423–1443
- Coltuc D, Chassery JM (2007) Very fast watermarking by reversible contrast mapping. *IEEE Signal Process Lett* 14(4):255–258
- Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T (2007) *Digital watermarking and steganography*. Morgan Kaufmann, Los Altos
- Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU-Int J Electron Commun* 68(3):244–253
- de Queiroz RL, Braun KM (2006) Color to gray and back: color embedding into textured gray images. *IEEE Trans Image Process* 15(6):1464–1470
- Fu Z, Wu X, Guan C, Sun X, Ren K (2016) Towards efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. *IEEE Trans Inf Forensics Secur*. doi:10.1109/TIFS.2016.2596138
- Guo P, Wang J, Geng XH, Kim CS, Kim JU (2014) A variable threshold-value authentication architecture for wireless mesh networks. *J Internet Technol* 15(6):929–935
- Kalra GS, Talwar R, Sadawarti H (2015) Adaptive digital image watermarking for color images in frequency domain. *Multimed Tools Appl* 74(17):6849–6869
- Kutter M, Winkler S (2002) A vision-based masking model for spread-spectrum image watermarking. *IEEE Trans Image Process* 11(1):16–25
- Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. *IEEE Trans Inf Forensics Secur* 10(3):507–518
- Ma T, Zhou J, Tang M, Tian Y, Abdullah AD, Mznah AR, Sungyoung L (2015) Social network and tag sources based augmenting collaborative recommender system. *IEICE Trans Inf Syst* 98(4):902–910
- Nasir I, Weng Y, Jiang J, Ipson S (2010) Multiple spatial watermarking technique in color images. *Signal Image Video Process* 4(2):145–154
- Pizzolante R, Castiglione A, Carpentieri B, De Santis A, Castiglione A (2014) Protection of microscopy images through digital watermarking techniques[C]. In: *Intelligent Networking and Collaborative Systems (INCoS)*, 2014 International Conference on. IEEE, pp 65–72. doi:10.1109/INCoS.2014.116
- Rigoni R, Freitas PG, Farias MCQ (2016) Detecting tampering in audiovisual content using QIM watermarking. *Inf Sci* 328:127–143
- Rivest RL (1992) The MD5 message-digest algorithm. Request for comments (RFC) 1321, Internet activities board, Internet privacy task force. <https://www.ietf.org/rfc/rfc1321.txt>
- Seitz J (2005) *Digital watermarking for digital media*. IGI Global, Information Science Publishing, USA, pp 25–27
- Su Q, Niu Y, Zhao Y, Pang S, Liu X (2013) A dual color images watermarking scheme based on the optimized compensation of singular value decomposition. *AEU-Int J Electron Commun* 67(8):652–664
- Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color watermark image embedded in color host image via QR decomposition. *Signal Process* 94:219–235
- University of Granada (2012) Computer vision group. CVG-UGR Image Database. [2012-10-22]. <http://decsai.ugr.es/cvg/dbimagenes/c512.php>
- Vaishnavi D, Subashini TS (2015) Robust and invisible image watermarking in RGB color space using SVD. *Procedia Comput Sci* 46:1770–1777
- Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* 13(4):600–612
- Wu HT, Huang J (2012) Reversible image watermarking on prediction errors by efficient histogram modification. *Signal Process* 92(12):3000–3009
- Xia Z, Wang X, Sun X, Wang B (2014) Steganalysis of least significant bit matching using multi-order differences. *Secur Commun Netw* 7(8):1283–1291
- Zeng G, Qiu Z (2008) Image watermarking based on DC component in DCT. In: *Intelligent Information Technology Application Workshops, 2008. IITAW '08. International Symposium on*, pp 573–576
- Zheng JB, Feng S (2008) A color image multi-channel DWT domain watermarking algorithm for resisting geometric attacks. In: *2008 International Conference on Machine Learning and Cybernetics, vol 2*. IEEE pp 1046–1051
- Zheng Y, Jeon B, Xu D, Wu QMJ, Zhang H (2015) Image segmentation by generalized hierarchical fuzzy C-means algorithm. *J Intell Fuzzy Syst* 28(2):961–973