

Fast and robust image watermarking method in the spatial domain

ISSN 1751-9659

Received on 10th January 2020

Revised 15th June 2020

Accepted on 19th October 2020

E-First on 18th February 2021

doi: 10.1049/iet-ipr.2019.1740

www.ietdl.org

Zihan Yuan¹, Qingtang Su¹ ✉, Decheng Liu¹, Xueting Zhang¹, Tao Yao¹

¹School of Information and Electrical Engineering, Ludong University, Yantai 264025, People's Republic of China

✉ E-mail: sdytsqt@163.com

Abstract: To solve the copyright protection problem of a colour image, a new blind colour image watermarking method combining a discrete cosine transform (DCT) in the spatial domain is presented in this study. The advantages of the spatial-domain watermarking algorithm and frequency-domain one are made full use in this scheme. Based on the different quantisation steps in red, green, and blue three-layer images, the processes of watermark embedding and blind extraction are completed in the spatial domain without a real DCT domain. The scheme is realised by using the unique features of the direct current (DC) coefficient and the relativity of DC coefficients between adjacent pixel blocks. This scheme can effectively solve the problems of the large-capacity colour image watermarking algorithm, such as long-running time and weak robustness. Comparing with other advanced watermarking algorithms, the presented scheme has better invisibility, stronger robustness, and higher real-time performance.

1 Introduction

1.1 Previous work

Nowadays, internet technology is increasingly popular, and it has become an important channel for the transmission of multimedia information. The internet provides customers with open access, so we can easily get the information we need. However, piracy, infringement, tampering, and other problems occur commonly because of the openness of internet information. Copyright protection [1, 2] has become the focus of scholars' research. As an effective method of copyright protection, digital watermarking technology [3, 4] has arisen in the digital world. A watermarking scheme can embed identification information such as a digital watermark into the digital carrier through specific rules, which is not easy to be detected visually and has a certain anti-attack ability. The information hidden in the carrier can be used to confirm the content owner, transmit secret information, or judge whether the carrier has been tampered. The successful embedding and extraction of the digital watermark can solve the copyright protection problem effectively.

The embedding process of the watermarking scheme can be carried out in the spatial domain or frequency one. Therefore, the digital watermarking schemes are divided into spatial-domain watermarking schemes [4–6] and frequency-domain ones [7–17]. Currently, many watermarking schemes are carried out in the frequency domain, which are called the frequency-domain watermarking schemes, for instance, the schemes used DCT [7–10], discrete wavelet transform [11, 12], discrete Fourier transform (DFT) [13, 14], and matrix decomposition [15–17]. Comparing with spatial-domain watermarking schemes, the frequency-domain watermarking ones are more robust since it can resist malicious attacks and signal processing. However, the calculation of the frequency-domain watermarking scheme is relatively complex, so its running time is long. For example, Loan *et al.* [8] proposed a digital image watermarking method using coefficient differencing. In the scheme proposed in [8], the similarity of DCT coefficients of adjacent image blocks is used to embed the watermark, which makes this watermarking method more robust. However, the watermark images used in the scheme proposed in [8] are binary images, so that it cannot meet the need for copyright protection for the large-capacity digital colour image. Su *et al.* [9] presented a watermarking algorithm using two times operations of DCT, which embedded the colour digital watermark to the carrier image for

protecting copyright. However, the scheme performed DCT operation two times, so the computation complexity of the scheme proposed in [9] was high. Zhang *et al.* [18] presented a robust watermarking scheme, in which the used watermarks and carrier images were all colour images, and the scheme was accomplished with red–green–blue (RGB) channel correlations, which can effectively resist various attacks. Golea *et al.* [19] presented a digital watermarking scheme, a colour image was used as a watermark in this scheme, and watermark information was embedded through singular value decomposition. In addition, Hamidi *et al.* [14] presented a hybrid robust blind watermarking algorithm using DFT and DCT and used Arnold transform to scramble watermark image, which greatly improved the security of the watermarking scheme.

On the contrary, the spatial-domain watermarking algorithm can embed a watermark by modifying the pixel value directly in the spatial domain. These schemes are simple to calculate, so they have a short running time and weak robustness. For instance, Abraham and Paul [5] presented a kind of imperceptible watermarking scheme in the spatial domain; the scheme completed the watermark embedding in the spatial domain to obtain the watermarked image with high quality and used a variety of quality indicators to analyse the algorithm performance. Experimental analyses proved that the invisibility of this watermarking algorithm was good. Su *et al.* [20] presented a blind spatial-domain watermarking algorithm for colour images using DC coefficient which shortened the running time of this algorithm. However, the watermark image used in the method [20] is a binary image, which is difficult to meet the need for copyright protection for the large-capacity digital colour image.

In addition, based on the detection process of the watermark, digital watermarking algorithms are divided into blind watermarking schemes [6, 9, 21] and non-blind ones [17, 22, 23]. The detection of a blind watermarking scheme does not need any primary data or reserved information while non-blind watermarking algorithms need them. For example, Su *et al.* [21] presented a blind watermarking scheme of a digital colour image using quadrature rectangle (QR) decomposition. This scheme embedded watermark information to a specific position of the colour carrier image by QR decomposition. However, at present, many watermarking schemes belong to the non-blind watermarking scheme, which requires the participation of the primary data in the watermark extraction process. Pandey *et al.* [22] presented a non-

blind watermarking scheme that used Arnold transform to scramble watermark. The scheme proposed in [22] embedded the singular value of the watermark to the Y channel of carrier image in YCbCr space. Ariatmanto and Ernawan [23] presented a robust image watermarking method, which uses different embedding strengths. The scheme proposed in [23] selects the middle DCT coefficients with a psycho-visual threshold to obtain the different embedding strength for embedding and extracting the watermark image, but, it must remember the coordinates of selected blocks, so it belongs to non-blind watermarking. In general, although the robustness of the non-blind watermarking scheme is stronger than the blind watermarking scheme, primary data is needed in the extraction process, so the blind watermarking scheme is more practical and has a wider application range.

The limitations of the existing watermarking methods are summarised as follows:

- (i) A binary image or a grey-scale image is often used as a watermark in the existing watermarking methods, which has a small embedding capacity and cannot meet the need for copyright protection for the large-capacity digital colour image.
- (ii) Many existing watermarking methods use the same quantisation step in R, G, and B three layers to embed watermark information without considering the different sensitivity of human eyes to the three colours, which cannot reduce the modification range of the pixel value to improve the invisibility of the watermark and results in the invisibility of the watermark is low.
- (iii) Many existing spatial-domain watermarking methods embed watermark by modifying the pixel value directly in the spatial domain, which makes their robustness weak, and the watermark information is easy to be destroyed by filtering, image compression, geometric deformation, and other attacks.
- (iv) Many of the existing frequency-domain watermarking methods have stronger robustness than spatial-domain ones and can resist malicious attacks, but their calculations are relatively complex, and real-time performances are poor.

1.2 Motivation and contributions

The basic requirements of a good digital watermarking technology include good invisibility, strong robustness, and high real-time performance. Therefore, on the premise of good invisibility of digital watermarking, how to design a digital watermarking algorithm with good robustness and short running time has become an urgent problem.

In this paper, a new blind colour image watermarking scheme combining a discrete cosine transform (DCT) in the spatial domain is presented. According to the correlation of the DC coefficients between adjacent pixel blocks, the presented scheme completed the watermark embedding and blind extraction by calculating and modifying the DC coefficients of pixel blocks in the spatial domain. Under the premise of good invisibility of the watermarking scheme, this scheme has strong robustness and short running time, which can be used in the fast and efficient copyright protection of digital media. The detailed contributions are introduced as follows:

- (i) Without the real DCT, the presented scheme directly calculates and modifies the DC coefficients of pixel blocks in the spatial domain, which belongs to the fusion domain watermarking scheme. This scheme combines the advantages of the fast operation speed of the spatial-domain watermarking and the high robustness of frequency-domain watermarking, which can effectively protect the copyright.
- (ii) For keeping the strong correlations between R, G, and B layers of the colour image, the different quantisation steps for the different layers are used to embed and extract watermark, which can reduce the modification range of the pixel value to improve the invisibility of the watermark.
- (iii) The meaningful similarity between the DC coefficients of adjacent pixel blocks is founded and used in the presented scheme, which not only ensures the good invisibility of the watermark but also guarantees the robustness of the watermarking scheme.

(iv) A binary image or a grey-scale image is often viewed as the watermark image in the traditional DCT-based watermarking scheme, which has a small embedding capacity. Compared with the traditional watermarking schemes, the colour watermark image is used in this scheme, which contains more information. The presented scheme meets the need for copyright protection for the large-capacity digital colour image.

The remaining part of this paper is structured as follows: the theoretical bases are shown in Section 2, which includes Arnold scrambling, two-dimensional DCT, obtaining and modification of the DC coefficient in the spatial domain, and variable quantisation steps selection. Section 3 shows the watermarking scheme proposed in this paper that is the watermark embedding and watermark extraction process. Section 4 presents the results and analysis of simulation attacks of this scheme, and the conclusion is presented in Section 5.

2 Preliminaries

2.1 Arnold transform

Arnold transform is a chaotic mapping from the torus to itself, which is also referred to as Cat mapping. Arnold transform is usually used in image encryption, information hiding, and other studies.

For providing more security to the presented watermarking scheme, the watermark image was preprocessed before watermark embedding. In other words, Arnold transform was used to scramble the watermark image. As a commonly used image scrambling and encryption technology, Arnold transform can rearrange all the pixels in the digital image to achieve the purpose of digital image encryption. For example, according to (1), Arnold transform is performed on a digital image sized $N \times N$, and the pixel point at position (u, v) is transformed to the position (u', v')

$$\begin{bmatrix} u' \\ v' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} \bmod N \quad (1)$$

where

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

is the transform matrix, $u, v, u', v' \in \{0, 1, 2, \dots, N-1\}$, $\bmod(\cdot)$ is the modulo operation, N is the size of the length of watermark image to be scrambled, (u', v') is the pixel position obtained after Arnold transform, and (u, v) is the pixel position of the watermark image before scrambling.

After the watermark extraction, it is necessary to reverse scramble the extracted watermark information to restore the original watermark image, which requires inverse Arnold transform. The process of inverse Arnold transform is given by

$$\begin{bmatrix} u \\ v \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} u' \\ v' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \right) \bmod N \quad (2)$$

where

$$\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$$

is the transform matrix of the inverse Arnold transform.

2.2 Two-dimensional discrete cosine transform (2D-DCT)

DCT is one of the mathematical transforms, which is frequently used in frequency-domain watermarking schemes. After DCT, multiple coefficients can be obtained, including one DC coefficient and multiple AC coefficients. These coefficients can be divided into three different frequency bands of coefficients, namely high frequency, medium frequency, and low frequency. DC coefficient is

located in the top-left corner of the pixel block and has the highest energy of the pixel block.

According to (3), one $M \times N$ matrix A in the spatial domain can be converted into the DCT domain using 2D-DCT. The corresponding 2D-DCT coefficients are defined as below

$$F(u, v) = \frac{2}{\sqrt{MN}} c(u) c(v) \times \left[\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \times \cos \frac{(2x+1)u\pi}{2M} \cos \frac{(2y+1)v\pi}{2N} \right] \quad (3)$$

among them, $u=0, \dots, M-1$, and $v=0, \dots, N-1$

$$c(u) = \begin{cases} 1/\sqrt{2}, & u=0 \\ 1, & \text{otherwise} \end{cases}$$

$$c(v) = \begin{cases} 1/\sqrt{2}, & v=0 \\ 1, & \text{otherwise} \end{cases}$$

$f(x, y)$ is the pixel value at the position (x, y) in the spatial domain. Similarly, $F(u, v)$ is the pixel value at the position (u, v) in the frequency domain obtained after 2D-DCT.

Through the inverse transform of 2D-DCT (2D-IDCT), a digital image can be converted to the spatial domain from the DCT domain and its formula is as follows: (see (4)).

2.3 Obtaining and modification of the DC coefficient in the spatial domain

As can be seen from (3), when $u=0$ and $v=0$, we can obtain $F(0, 0)$, i.e. DC coefficient. The DC coefficient value can be calculated using

$$F(0, 0) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \quad (5)$$

In other words, by dividing the sum of pixel values in the pixel block by arithmetic square root of the row and column size product, then the DC coefficient of the pixel block is calculated in the spatial domain.

Generally, watermark information can be embedded by modifying the DC coefficient obtained by 2D-DCT, and then the watermarked image can be obtained by 2D-IDCT. Since there is no loss of energy added to the DC coefficient after the 2D-IDCT, it indicates that the watermark embedding operation with corresponding modification on the DC coefficient can also be completed in the spatial domain. In other words, the pixel value can be directly modified in the spatial domain to accomplish the watermark embedding process [20].

Suppose that after embedding the watermark information into pixel block A at the position (i, j) of the carrier image, the watermarked pixel block A^* is obtained. The change of DC coefficient is $\Delta C_{i,j}$, then the DC coefficient of watermarked pixel block A^* can be expressed by

$$F'_{i,j}(0, 0) = F_{i,j}(0, 0) + \Delta C_{i,j} \quad (6)$$

In addition, according to (4) and (5), another representation of each pixel value after IDCT can be obtained

$$f(u, v) = \frac{1}{\sqrt{MN}} F(0, 0) + f^{AC}(u, v) \quad (7)$$

where $f^{AC}(u, v)$ is the pixel value of each AC coefficient at the position (u, v) after IDCT.

According to (7), each pixel value of watermarked pixel block A^* after IDCT can be obtained that

$$f'_{i,j}(m, n) = \frac{1}{N} F'_{i,j}(0, 0) + f^{AC}_{i,j}(m, n) \quad (8)$$

where $F'_{i,j}(0, 0)$ represents the DC coefficient value after modifying pixel block A at the position (i, j) of the carrier image, N is the size of the row or column of pixel block A , $f^{AC}_{i,j}(m, n)$ is the pixel value of each AC coefficient at the position (m, n) of pixel block A at the position (i, j) of the carrier image after IDCT.

According to (6) and (8), we can obtain

$$f'_{i,j}(m, n) - f_{i,j}(m, n) = \frac{1}{N} \Delta C_{i,j} \quad (9)$$

From (9) we can see that increasing the value of $\Delta C_{i,j}/N$ to each pixel in the spatial domain is equivalent to increasing $\Delta C_{i,j}$ to the DC coefficient obtained by DCT. Therefore, we can modify the pixel value in the spatial domain directly to accomplish the watermark embedding process and do not need the real DCT.

2.4 Selection of variable quantisation steps

As we all know, human eyes are sensitive to different colours of R, G, and B. This is because human cones have different sensitivity to these three colours. In detail, as for all the cones, about 65% of them are sensitive to R colour, 33% are sensitive to G colour, while only 2% are sensitive to B colour [24]. Therefore, different quantisation steps were determined according to the different sensitivity of human eyes to R, G, and B layers.

Generally, natural colour images are divided into three layers of R, G, and B, and there is usually a strong correlation between them. The correlation coefficients between the three layers are $r(B, R) \approx 0.78$, $r(R, G) \approx 0.98$, and $r(G, B) \approx 0.94$ [25]. Therefore, supposing the quantisation step of the R layer is T_1 , the G layer is T_2 , and the B layer is T_3 , there are the following relationships between them: $T_1 = 0.78 \times T_3$, $T_2 = 0.94 \times T_3$.

3 Proposed scheme

The implementation of the presented watermarking scheme includes two processes: watermark embedding and watermark extraction. The successful embedding and extraction of watermark images can effectively realise copyright protection.

3.1 Watermark embedding

Fig. 1 shows the diagram of the presented watermark embedding scheme, the specific steps are given as follows:

Step 1: Dividing a carrier image H sized $M \times M$ into three-layered carrier images H_i , i.e. R, G, and B three layers, then dividing each layered carrier image H_i to non-overlapping blocks sized $m \times m$, where $m=2, i=1, 2, 3$, and it is R, G, and B layers, respectively.

Step 2: Dividing a watermark image W sized $N \times N$ into three-layered watermark images of R, G, and B three layers. Meanwhile, scrambling each layered watermark using Arnold transform with key Ka_i to give the watermarking algorithm more security, and obtaining three scrambled layered watermark images W_i . Then, converting all the decimal pixel values of the layered watermark image W_i into binary information, and connecting them successively to get the watermark bit sequence SW_i which length is $8N^2$, where $i=1, 2, 3$, and it is R, G, and B layers, respectively.

$$f(x, y) = \frac{2}{\sqrt{MN}} \left[\sum_{u=0}^{M-1} \sum_{v=0}^{N-1} c(u) c(v) \times F(u, v) \times \cos \frac{(2x+1)u\pi}{2M} \cos \frac{(2y+1)v\pi}{2N} \right] \quad (4)$$

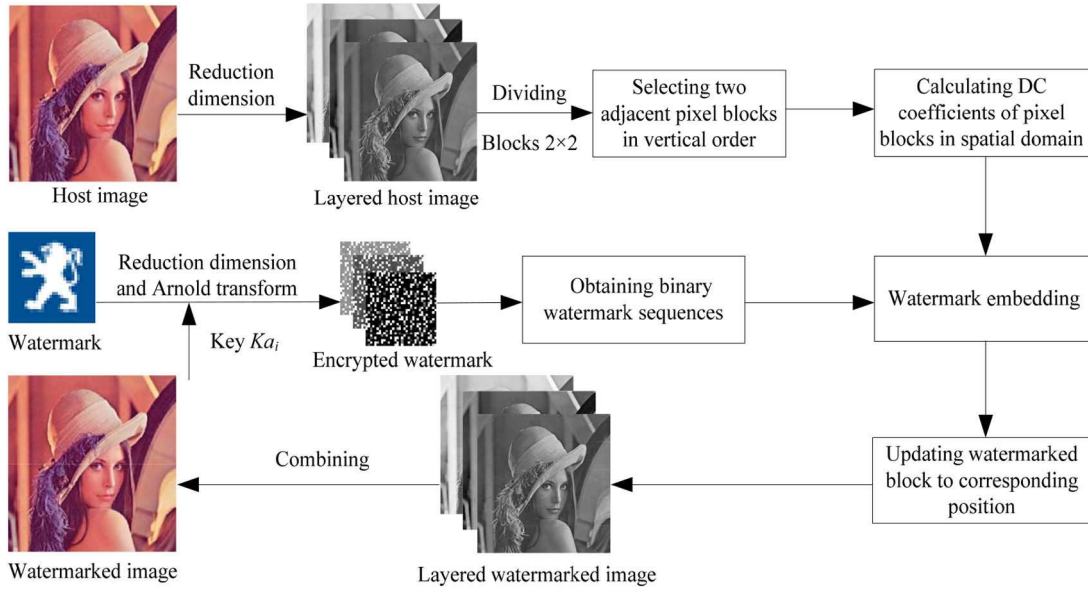


Fig. 1 Diagram of watermark embedding scheme

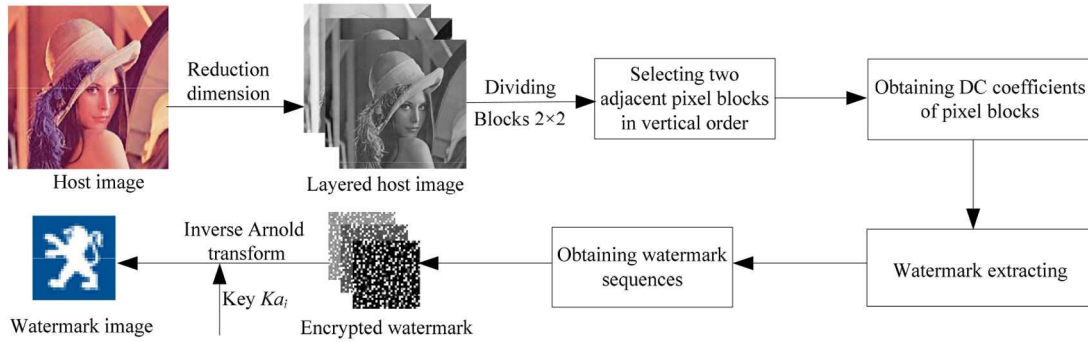


Fig. 2 Diagram of watermark extracting scheme

Step 3: Selecting the adjacent pixel blocks A and B from the layered carrier image H_i follow vertical order, where $i = 1, 2, 3$, and it is R, G, and B layers, respectively.

Step 4: According to (10), calculating the DC coefficients dc_p of pixel blocks A and B in the spatial domain directly

$$dc_p = \frac{1}{m} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} f_p(x, y) \quad (10)$$

where $p = 1$ and 2 represent the pixel blocks A and B , respectively, m is the size of the row or column of the pixel block, and $f_p(x, y)$ is the pixel value in position (x, y) of pixel block p .

Step 5: Selecting watermark bit w from watermark sequence SW_i in order. According to the correlation between the DC coefficients of adjacent pixel blocks, using (11) and (12) to obtain modified DC coefficients dc_p^* of pixel block p to accomplish the embedding of watermark bit w , where $p = 1$ and 2 represent pixel blocks A and B , respectively

$$dc_1^* = \begin{cases} \text{avg} - 0.5 \times T_i, & \text{if } w = '0' \text{ and } dc_1 - dc_2 > 0 \\ \text{avg} + 0.5 \times T_i, & \text{if } w = '1' \text{ and } dc_1 - dc_2 \leq 0 \\ dc_1 & \text{else} \end{cases} \quad (11)$$

$$dc_2^* = \begin{cases} \text{avg} + 0.5 \times T_i, & \text{if } w = '0' \text{ and } dc_1 - dc_2 > 0 \\ \text{avg} - 0.5 \times T_i, & \text{if } w = '1' \text{ and } dc_1 - dc_2 \leq 0 \\ dc_2 & \text{else} \end{cases} \quad (12)$$

where w is the watermark bit to be embedded, $\text{avg} = (dc_1 + dc_2)/2$, T_i is the quantisation step of i th layer, $i = 1, 2, 3$, and it is R, G, and B layer, respectively.

Step 6: According to (13), the pixel value $f_p(x, y)$ in the corresponding location of original pixel block p is replaced with the modified pixel value $f_p^*(x, y)$, and the watermarked pixel blocks A^* and B^* are obtained, $p = 1, 2$

$$f_p^*(x, y) = f_p(x, y) + \frac{1}{m} \times (dc_p^* - dc_p) \quad (13)$$

Step 7: Updating the watermarked pixel blocks A^* and B^* to their corresponding locations in the layered carrier image H_i , where $i = 1, 2, 3$, and it is R, G, and B layer, respectively.

Step 8: Repeating the above steps 3–7 of this process until embedding all the watermark information, and obtaining the layered watermarked image H_i^* . Finally, combining three-layered watermarked image H_i^* to obtain the colour watermarked image H^* , where $i = 1, 2, 3$, and it is R, G, and B layer, respectively.

3.2 Watermark extracting

Fig. 2 shows the diagram of the presented watermark extraction scheme, the specific steps are given as follows:

Step 1: The watermarked image H^* is divided into R, G, and B three-layered images H_i^* by the dimension reduction process. At the same time, dividing each watermarked layered image H_i^* to non-overlapping blocks sized $m \times m$, where $m = 2$, $i = 1, 2, 3$, and it is R, G, and B layers, respectively.

Step 2: Selecting adjacent watermarked pixel blocks A^* and B^* from the watermarked layered image H_i^* follow vertical order, where $i = 1, 2, 3$, and it is R, G, and B layers, respectively.

Step 3: According to (14), calculating the DC coefficients dc_p^* of watermarked pixel blocks A^* and B^* in the spatial domain directly

$$dc_p^* = \frac{1}{m} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} f_p^*(x, y) \quad (14)$$

where m represents the row or column size of the pixel block, $f_p^*(x, y)$ is the pixel value of watermarked pixel block p which position is (x, y) , $p=1$ and 2 , respectively, represent the watermarked pixel block A^* and B^* .

Step 4: According to the size relationship between the DC coefficients dc_p^* of watermarked pixel blocks A^* and B^* , extracting the watermark bit w^* from watermarked pixel blocks A^* and B^* by (15), $p=1, 2$

$$w^* = \begin{cases} '1', & \text{if } dc_1^* - dc_2^* > 0 \\ '0', & \text{else} \end{cases} \quad (15)$$

Step 5: The above steps 2–4 of this process are repeated to obtain the extracted watermark sequence SW_i^* , dividing each 8-bit binary information of binary watermark sequence SW_i^* into a group and converting it into decimal pixel values to form the scrambled watermark layer, where $i=1, 2, 3$, and it is R, G, and B layers, respectively.

Step 6: Using inverse Arnold transform with key Ka_i on the scrambled watermark layer to get the extracted watermark W_i^* of each layer. Then combining three extracted layered watermarks W_i^* to form the final extracted colour watermark W^* , where $i=1, 2, 3$, and it is R, G, and B layers, respectively.

4 Simulation results

For testing the effectiveness of this presented scheme, many experiments have been carried out in this section. In the following experiments, four colour images with a size of 512×512 are selected as original carrier images namely 'Lena', 'House', 'Peppers', and 'F16', as shown in Figs. 3a–d. These colour carrier images are selected from the standard databases CVG-UGR [26]

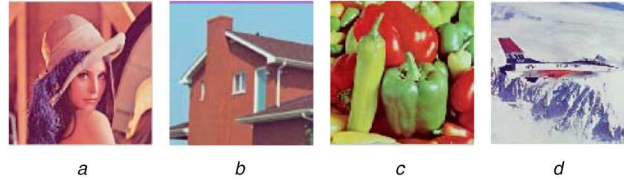


Fig. 3 Colour carrier images
(a) Lena, (b) House, (c) Peppers, (d) F16



Fig. 4 Watermark images
(a) Peugeot, (b) QQ

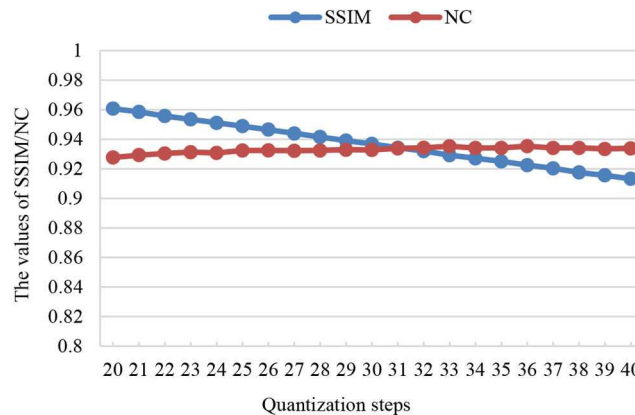


Fig. 5 Average values of SSIM and NC under various quantisation steps

and USC-SIPI [27]. Two colour digital images with a size of 32×32 are used as watermark images, as shown in Figs. 4a and b. For proving the effectiveness of the scheme, a variety of simulation attacks are carried out on the watermarked images, and a series of comparisons are made between the performance results of the presented scheme and the previous watermarking schemes, such as invisibility comparison, robustness comparison, embedding capacity comparison, real-time comparison, and security comparison. The relevant watermarking schemes compared with the presented scheme include blind colour image watermarking scheme using two times operations of DCT [9], blind RGB digital image watermarking scheme using singular value decomposition [19], robust watermarking algorithm using RGB channel correlation [18], and blind image watermarking method using QR decomposition [21].

Supposing the quantisation step of layer R is T_1 , that of layer G is T_2 , and that of layer B is T . As described in Section 2.4, the quantisation steps of layers R, G, and B have the following relationship: $T_1 = 0.78 \times T$, $T_2 = 0.94 \times T$. Therefore, after selecting the quantisation step T , we can get other two quantisation steps T_1 and T_2 .

For selecting a reasonable quantization step T , we embedded the watermark image 'Peugeot' in Fig. 4a into the carrier image 'Lena' in Fig. 3a with different values of quantization step T , then recorded the structural similarity index measurement (SSIM) value under different quantisation steps and obtained the average normalised cross-correlation (NC) value after different attacks. Experimental results are given as Fig. 5. Quantisation step T increases gradually between 20 and 40, at the same time SSIM values become smaller and smaller. In other words, while the quantisation step increases, the invisibility of watermark becomes worse and robustness of the watermarking becomes stronger, so we need to make a balance between them. Therefore, in this paper, considering the invisibility and robustness requirements of the watermarking scheme, quantisation step T is chosen at the

intersection point, that is $T=31$, and the corresponding quantisation steps T_1 and T_2 are 24.18 and 29.14, respectively.

4.1 Imperceptibility analysis

Invisibility is an important index to test the performance of the watermarking scheme. The invisibility is related to the human visual system, and it requires the watermarked image is indistinguishable from the original carrier image in perception when the watermark is embedded into the carrier image.

In this section, the invisibility of the digital watermarking algorithm is estimated by the peak-signal-to-noise ratio (PSNR) and SSIM. Among them, PSNR is an objective evaluation index, which is widely used in the digital watermarking algorithm. PSNR can compute the similarity between the watermarked image and the carrier image. Therefore, the higher the PSNR value is, the better the similarity between the carrier image and the watermarked image is. Generally, the PSNR value is >35 dB indicates good quality, while it is between 29 and 35 dB indicates acceptable quality. The critical point is 25 dB, which means that the watermark will be visible. When the PSNR value is <25 dB, it means that the watermarking algorithm will not meet the requirement of invisibility [28]. PSNR is defined as follows:

$$\text{PSNR}_k = 10 \lg \frac{M \times N \times 255^2}{\sum_{u=1}^M \sum_{v=1}^N [H(u, v, k) - H^*(u, v, k)]^2} \quad (16)$$

where $H(u, v, k)$ and $H^*(u, v, k)$, respectively, represent the pixel with coordinates (u, v) of the k channel of carrier image and watermarked image, M and N are the row size and column size of the test image.

Colour images can be divided into R, G, and B three layers, so its PSNR is defined as

$$\text{PSNR} = \sum_{k=1}^3 \text{PSNR}_k \quad (17)$$

SSIM is often used to measure the invisibility of a digital watermarking scheme. The larger the SSIM value is, the greater the similarities between images are, which means the better the invisibility of the watermarking scheme is. The definition of SSIM [21] is as follows:

$$\text{SSIM}(H, H^*) = l(H, H^*)c(H, H^*)s(H, H^*) \quad (18)$$

in which

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

where $l(H, H^*)$, $c(H, H^*)$, and $s(H, H^*)$ are brightness comparison function, contrast comparison function, and structural comparison function, respectively.

For measuring the invisibility of the presented scheme, the watermarks in Figs. 4a and b were embedded into eight standard carrier images in Figs. 3a–d, respectively, and the obtained values of PSNR and SSIM are given in Table 1. We can see that the average PSNR value of the extracted watermark image is >37 dB, and the average SSIM value is close to 1.

In addition, for comparing the presented watermarking scheme with the other relevant watermarking schemes in terms of invisibility, different watermarking schemes are used to embed the colour image digital watermark ‘Peugeot’ in Figs. 4a and ‘QQ’ in Fig. 4b into the colour carrier images in Figs. 3a–d, respectively. Experimental results are given in Table 2. Although PSNR and SSIM values of the scheme [9] are higher than the presented scheme, NC values of the watermarked image without attack are far smaller than the presented scheme, which indicates that the scheme proposed in [9] does not make a reasonable balance

between robustness and invisibility. Moreover, the average PSNR value of the presented scheme is >37 dB, the average SSIM value is close to 1, and the average NC value is equal to 1. Compared with the scheme proposed in [19, 21], the average values of PSNR and SSIM of the presented scheme are bigger, which indicates that the watermarked image and carrier image of the presented scheme are similar in perception, and this presented watermarking scheme has better invisibility.

4.2 Robustness analysis

The quality of digital media may decrease when it is transmitted through channels. Robustness represents the ability of watermarking technology to resist malicious attacks or signal processing, which is the vital characteristic of watermarking schemes. NC, as a fair and reliable evaluation standard for the robustness of the watermarking algorithm, can evaluate the robustness of the digital watermarking scheme by comparing the similarity between the original watermark image and the extracted watermark image. Therefore, NC is usually used to evaluate the robustness of the watermarking scheme. NC is a number that is >0 and <1 . When the NC value is >0.85 , it indicates that the original watermark and extracted watermark have high similarity and the robustness of the mentioned scheme is strong [28].

The NC value of digital colour images can be calculated by

$$\text{NC} = \frac{\sum_{k=1}^3 \sum_{u=1}^m \sum_{v=1}^n (W(u, v, k) \times W^*(u, v, k))}{\sqrt{\sum_{k=1}^3 \sum_{u=1}^m \sum_{v=1}^n [W(u, v, k)]^2} \sqrt{\sum_{k=1}^3 \sum_{u=1}^m \sum_{v=1}^n [W^*(u, v, k)]^2}} \quad (20)$$

where $W(u, v, k)$ and $W^*(u, v, k)$ are pixel values of the original watermark and extracted watermark at the position (u, v) in the k th layer, respectively, m and n , respectively, represent the size of the row and column of the colour digital watermark, $1 \leq u \leq m$, $1 \leq v \leq n$.

In the following experiments, for evaluating the robustness of the presented watermarking scheme, the watermark images ‘Peugeot’ and ‘QQ’ of Fig. 4 are embedded to carrier image ‘Lena’ of Fig. 3a and carrier image ‘House’ of Fig. 3b, respectively. Then, the robustness performance of this presented watermarking scheme under seven different attacks was tested, including JPEG compression attack, JPEG2000 compression attack, Salt & Pepper noise attack, Gaussian noise attack, median filter attack, low-pass filter attack, and scaling attack. The visual effect of watermarks

Table 1 Results of watermarking invisibility when watermarks are embedded in carrier images (PSNR/SSIM)

	Peugeot	QQ
Lena	37.4377/0.9343	37.4091/0.9346
House	37.2156/0.9351	37.2863/0.9297
Peppers	36.4911/0.9381	36.3710/0.9370
F16	37.7981/0.9262	37.4263/0.9230
average	37.2356/0.9334	37.1232/0.9311

Table 2 Comparison results of PSNR, SSIM, and NC values of various schemes

Scheme	Watermark	PSNR	SSIM	NC
scheme [9]	Peugeot	45.4137	0.9863	0.7520
	QQ	45.1636	0.9849	0.9240
scheme [19]	Peugeot	36.9364	0.9104	0.9886
	QQ	35.4400	0.8901	0.9827
scheme [21]	Peugeot	36.3303	0.8983	1.0000
	QQ	36.7298	0.9053	1.0000
presented scheme	Peugeot	37.2356	0.9334	1.0000
	QQ	37.1232	0.9311	1.0000















Attack	JPEG (70)	JPEG 2000 (5:1)	Gaussian white noise (0, 0.001)	Salt & Peppers noise (0.2%)	Butterworth low-pass filtering (100, 2)	Median filtering (3×3)	Zoom-in (3:1)
Watermark							
Peugeot							
	0.9573	0.9603	0.9044	0.9945	0.9164	0.9142	0.9811
QQ							
	0.9781	0.9999	0.9215	0.9936	0.9587	0.9478	0.9821

Fig. 6 Extract the watermarks from the watermarked image after various attacks and their NC values

Table 3 Main parameters in this paper

Parameters	Meaning	Parameters	Meaning
RGB	colour channel	dc_p	DC coefficient
DC	direct current components	$f_p(x, y)$	pixel value at location (x, y)
M, N	image size	$f_p^*(x, y)$	modified pixel value at location (x, y)
Ka_i	secret key	w	watermark bit
H	carrier image	u, v, x, y	pixel position of the pixel block
H_i	layered carrier image	T_i	quantization step
W	watermark image	H^*	watermarked image
W_i	scrambled layered watermark	W^*	extracted watermark image
SW_i	layered watermark bit sequence	PSNR	peak-signal-to-noise ratio
A, B	index of image block	SSIM	structural similarity index measurement
m	block size	NC	normalised correlation

extracted by the presented watermarking scheme after various attacks and its corresponding NC value is shown in Fig. 6.

What is more, the main parameters that appeared in our paper are listed in Table 3.

Similarly, the watermark image ‘Peugeot’ in Fig. 4a is embedded to the carrier image ‘Lena’ in Fig. 3a with various watermarking schemes to obtain a watermarked image, and a series of attacks are carried out on the watermarked image, then compared robustness performance of mentioned watermarking schemes by calculating the NC value of the original watermark image and the extracted watermark image.

JPEG compression is a common image compression technique, which can compress watermarked images with different quality factors from 0 to 100. At the same time, the JPEG compression attack is also an effective attack method to verify the robustness of the watermarking scheme. In the following experiments, we, respectively, used compression factors 30 and 90 for image compression and compared the simulation results with many related schemes. The simulation results are shown in Fig. 7. It

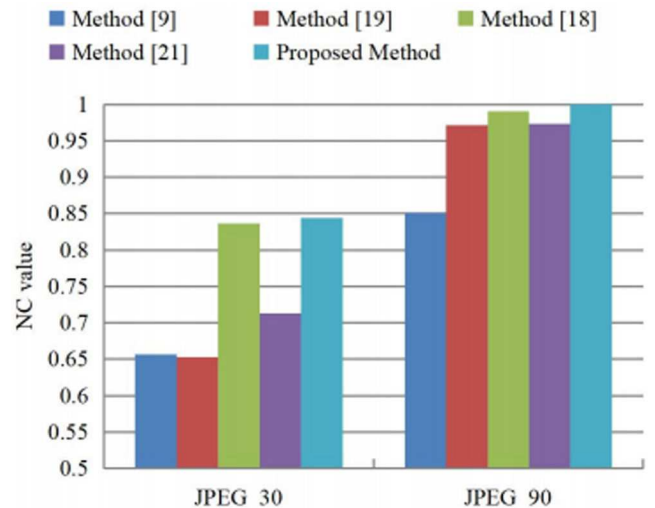


Fig. 7 Comparison of NC between various schemes after JPEG compression attacks

proves that this presented scheme can resist JPEG compression attack effectively.

The watermark image is sometimes affected by noise in the transmission process, which affects the quality of the extracted watermark. For testing the effectiveness of various watermarking schemes in terms of noise attack, we carried out a Salt & Pepper noise attack on watermarked images. The attack noise intensities of Salt & Pepper noise are 2 and 10%. The experimental results are shown in Fig. 8. According to the NC value of the extracted watermark from the attacked watermarked image, we can find that the presented watermarking scheme has obvious robust advantages compared with the schemes proposed in [9, 19], has a similar robust effect to that of schemes proposed in [18, 21] when the noise intensity is 2%. When the noise intensity increase to 10%, compared with other watermarking schemes, the presented scheme shows strong robustness.

Filtering is a common image processing technology, which can effectively smooth the details of the image. A median filter and Butterworth low-pass filter are two common filters used in image processing. In the following experiments, the robustness of various watermarking schemes is compared using these two filtering attacks. Fig. 9 shows the simulation results of the median filtering

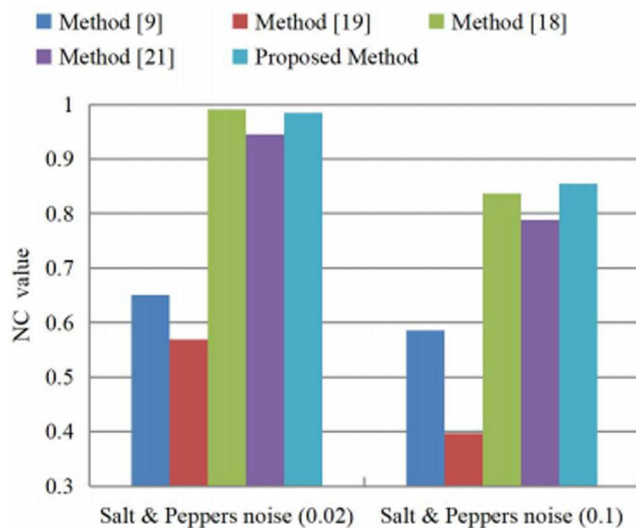


Fig. 8 Comparison of NC between various schemes after Salt &Peppers noising attacks

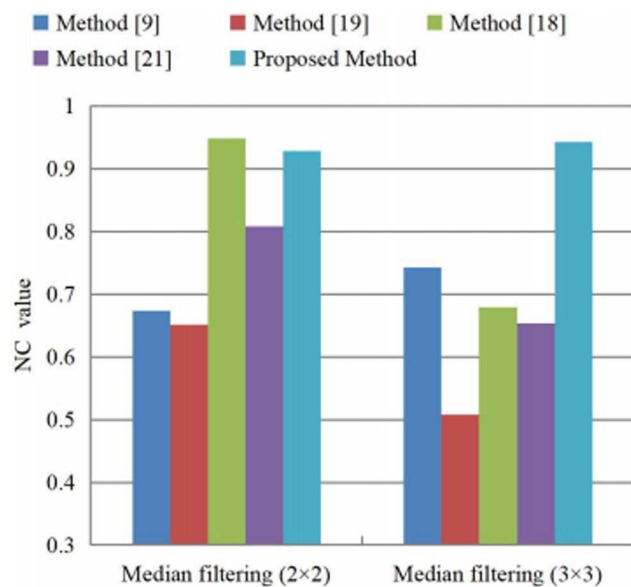


Fig. 9 Comparison of NC between various schemes after median filtering attacks

Table 4 Average NC of different schemes after various attacks

Scheme	Average NC
scheme [9]	0.721320
scheme [19]	0.608890
scheme [18]	0.921910
scheme [21]	0.823700
presented scheme	0.931480

attack with a filter order of 2×2 and 3×3 . It can be seen that, in terms of resisting median filtering attack, when the filter order is 3×3 , the NC value of the presented scheme is much higher than that of other relevant watermarking schemes. In addition, Fig. 10 shows the simulation results of Butterworth low-pass filtering attack which filter orders are 3 and 5, respectively. Compared with other watermarking schemes, the scheme provides strong robustness against filtering attacks.

Scaling is a common geometric attack. In Fig. 11, we can see the simulation results after the watermarked image was enlarged by 400% and reduced by 25%. It can be seen that the watermarking scheme is generally robust to zoom-in attack. Although all watermarking schemes are less robust to zoom-out attack since it

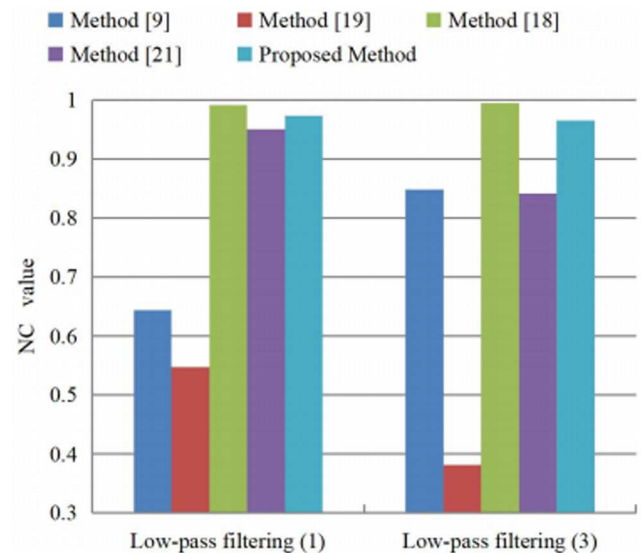


Fig. 10 Comparison of NC between various schemes after Butterworth low-pass filtering attacks

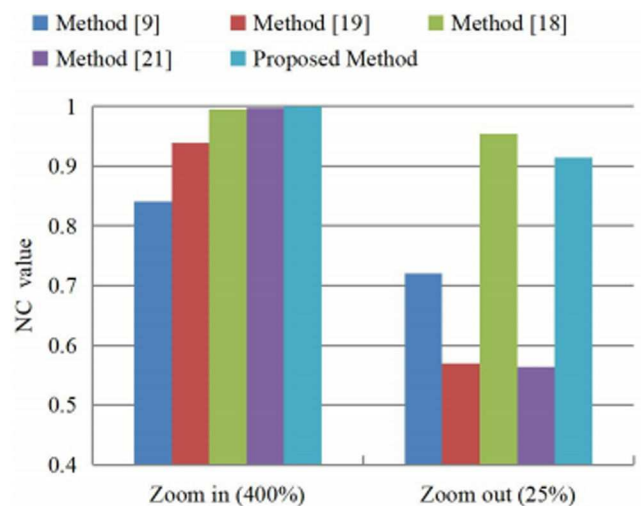


Fig. 11 Comparison of NC between various schemes after scaling attacks

will lead to the loss of pixel value, the presented scheme is more robust than other schemes.

Finally, for estimating the robustness of the presented watermarking scheme more accurately, the comparisons of the average NC values of various schemes which are mentioned above are given in Table 4. The average NC value of the presented scheme is 0.93148, while the average NC value of other schemes is lower than that of the presented scheme.

4.3 Maximum embedding capacity analysis

The embedding capacity is a vital factor to estimate the quality of the watermarking scheme. In the presented watermarking scheme, the colour watermark of size 32×32 is embedded into the carrier image of sized 512×512 , and its block size is 2×2 , so the embedding capacity of the presented watermarking scheme is 0.03125(bit/pixel). Table 4 compares the maximum embedding capacity of different schemes. According to Table 5, we can see that the maximum watermark embedding capacity of the presented scheme is much larger than that of schemes proposed in [18, 19, 21], and is equal to that of the scheme proposed in [9]. It is because the watermark image used in the scheme proposed in [9] is the 24-bit colour watermark image. In addition, one watermark bit is embedded into the DC coefficient of the pixel block after DCT which size is 8×8 , and seven watermark bits are embedded into the AC coefficient of the pixel block in the scheme proposed in [9]. Therefore, the maximum watermark embedding capacity of the

Table 5 Comparison of maximum embedding capacity of various watermarking schemes

Scheme	Maximum embedded watermark, bit	Watermark, bit	Host image, pixel	Bit/pixel
scheme [9]	64 × 64 × 24	64 × 64 × 24	512 × 512 × 3	0.12500
scheme [19]	32 × 32 × 24	32 × 32 × 24	512 × 512 × 3	0.03125
scheme [18]	170 × 170	32 × 32 × 24	512 × 512 × 3	0.03675
scheme [21]	128 × 128 × 3	32 × 32 × 24	512 × 512 × 3	0.06250
presented	128 × 128 × 6	32 × 32 × 24	512 × 512 × 3	0.12500

Table 6 Comparison of running time of different schemes (in seconds)

Scheme	Watermark embedding time	Watermark extracting time	Cumulative time
scheme [9]	3.4375	61.1250	64.5625
scheme [19]	1.9091	0.9060	2.8151
scheme [18]	0.7123	0.4279	1.1402
scheme [21]	0.6870	0.4270	1.1140
presented	0.6057	0.2552	0.8609

scheme proposed in [9] is larger than that of other relevant watermarking schemes.

4.4 Real-time feature analysis

All algorithms mentioned in this paper were performed on platform 2.60 GHz CPU, 4.00 GB RAM, Win10, MATLAB (R2017a). Table 6 shows the execution time of this presented scheme, including watermark embedding and extraction time, which is shorter than that of other schemes. This is because the presented scheme achieves the embedding and blind extraction of the colour digital watermark in the spatial domain but does not need real DCT, so this presented algorithm has a short running time. The average total running time of the presented scheme is 0.8609 s, which has better real-time performance and can meet the needs of current multimedia big data for rapid copyright protection.

5 Conclusion

For solving the copyright protection problem of a colour image, a new fast and robust image watermarking scheme combining DCT in the spatial domain is presented in this paper. According to the unique features of DC coefficient and the relativity of DC coefficients between adjacent pixel blocks, the different quantisation steps in R, G, and B layers are used to complete watermark embedding and blind extraction directly in the spatial domain, which does not need the real DCT. The presented scheme is simple and has low complexity. A series of simulation results indicate that this presented watermarking scheme has good performance of invisibility, and simultaneously achieve the robustness requirement and real-time requirement, which is suitable for the copyright protection of the colour image.

6 Acknowledgments

The work was supported by the National Natural Science Foundations of China (nos. 61771231, 61772253, 61872170, and 61873117), and the Key Research and Development Program of Shandong Province (no. 2019GGX101025).

7 References

- [1] Sahu, N., Sur, A.: 'SIFT based video watermarking resistant to temporal scaling', *J. Vis. Commun. Image Represent.*, 2017, **45**, pp. 4549–4564
- [2] Cedillo-Hernandez, A., Cedillo-Hernandez, M., Miyatake, M.N., et al.: 'A spatiotemporal saliency-modulated JND profile applied to video watermarking', *J. Vis. Commun. Image Represent.*, 2018, **52**, pp. 106–117
- [3] Makbol, N.M., Khoo, B.E., Rassem, T.H., et al.: 'A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection', *Inf. Sci.*, 2017, **417**, pp. 381–400
- [4] Su, Q., Chen, B.: 'Robust color image watermarking technique in the spatial domain', *Soft Comput.*, 2017, **22**, (1), pp. 91–106
- [5] Abraham, J., Paul, V.: 'An imperceptible spatial domain color image watermarking scheme', *J. King Saud Univ. Comput. Inf. Sci.*, 2019, **31**, (1), pp. 125–133
- [6] Su, Q., Yuan, Z., Liu, D.: 'An approximate Schur decomposition-based spatial domain color image watermarking method', *IEEE Access*, 2019, **7**, (1), pp. 4358–4370
- [7] Moosazadeh, M., Ekbatanifard, G.: 'An improved robust image watermarking method using DCT and YCoCg-R color space', *Optik – Int. J. Light Electron Opt.*, 2017, **140**, pp. 975–988
- [8] Loan, N.A., Hurrah, N.N., Parah, S.A., et al.: 'Secure and robust digital image watermarking using coefficient differencing and chaotic encryption', *IEEE Access*, 2018, **6**, pp. 19876–19897
- [9] Su, Q., Wang, G., Jia, S., et al.: 'Embedding color image watermark in color image based on two-level DCT', *Signal Image Video Process.*, 2015, **9**, (5), pp. 991–1007
- [10] Ermauan, F., Kabir, M.N.: 'A robust image watermarking technique with an optimal DCT-psychovisual threshold', *IEEE Access*, 2018, **6**, (4), pp. 20464–20480
- [11] Koohpayeh, A.T., Abd, M.A., Kohpayeh, A.S.: 'A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition', *Expert Syst. Appl.*, 2018, **112**, pp. 208–228
- [12] Abdulrahman, A.K., Ozturk, S.: 'A novel hybrid DCT and DWT based robust watermarking algorithm for color images', *Multimedia Tools Appl.*, 2019, **78**, (12), pp. 17027–17049
- [13] Ying, Q., Lin, J., Qian, Z.: 'Robust digital watermarking for color images in combined DFT and DT-CWT domains', *Math. Biosci. Eng.*, 2019, **16**, (5), pp. 4788–4801
- [14] Hamidi, M., Haziti, M.E., Cherifi, H.: 'Hybrid blind robust image watermarking technique based on DFT–DCT and Arnold transform', *Multimedia Tools Appl.*, 2018, **77**, (20), pp. 27181–27214
- [15] Li, J., Yu, C., Gupta, B.B., et al.: 'Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition', *Multimedia Tools Appl.*, 2018, **77**, (4), pp. 4545–4561
- [16] Su, Q., Chen, B.: 'A novel blind color image watermarking using upper Hessenberg matrix', *AEU – Int. J. Electron. Commun.*, 2017, **78**, pp. 64–71
- [17] Rasti, P., Samiei, S., Agoyi, M., et al.: 'Robust non-blind color video watermarking using QR decomposition and entropy analysis', *J. Vis. Commun. Image Represent.*, 2016, **38**, pp. 838–847
- [18] Zhang, F., Luo, T., Jiang, G., et al.: 'A novel robust color image watermarking method using RGB correlations', *Multimedia Tools Appl.*, 2019, **78**, (14), pp. 20133–20155
- [19] Golea, N.E.H., Seghir, R., Benzid, R.: 'A blind RGB color image watermarking based on singular value decomposition'. IEEE/ACS Int. Conf. on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 2010, pp. 1–5
- [20] Su, Q., Niu, Y., Wang, Q., et al.: 'A blind color image watermarking based on DC component in the spatial domain', *Optik – Int. J. Light Electron Opt.*, 2013, **124**, (23), pp. 6255–6260
- [21] Su, Q., Wang, G., Jia, S., et al.: 'Color image blind watermarking scheme based on QR decomposition', *Signal Process.*, 2014, **94**, (1), pp. 219–235
- [22] Pandey, M.K., Parmar, G., Gupta, R.: 'Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space', *Microsyst. Technol.*, 2019, **25**, (8), pp. 3071–3081

- [23] Ariatmanto, D., Ernawan, F.: 'An improved robust image watermarking by using different embedding strengths', *Multimedia Tools Appl.*, 2020, **79**, pp. 1–27
- [24] Gonzalez, R.C., Woods, R.E.: '*Digital image processing*' (Pearson Education, India, 2002, 2nd edn)
- [25] Sangwine, S., Horne, R.: '*The colour image processing handbook*', vol. 29, issue (5) (Springer, Berlin, 1998), p. 461
- [26] University of Granada, Computer Vision Group. 'CVG-UGR Image Database'. Available at <http://decsai.ugr.es/cvg/dbimagenes/c512.php>, accessed 20 November 2019
- [27] University of Southern California, Signal and Image Processing Institute. 'USC-SIPI Image Database'. Available at <http://sipi.usc.edu/database/>, accessed 20 November 2019
- [28] Moosazadeh, M., Ekbatanifard, G.: 'A new DCT-based robust image watermarking method using teaching-learning-based optimization', *J. Inf. Secur. Appl.*, 2019, **47**, pp. 28–38