Hindawi
Security and Communication Networks
Volume 2020, Article ID 8840779, 12 pages
https://doi.org/10.1155/2020/8840779

Research Article

A Novel Comprehensive Watermarking Scheme for Color Images

Shaohua Duan, Hanwen Wang, Yunpeng Liu, Li Huang, and Xiaoyi Zhou

School of Computer and Cyberspace Security, Hainan University, Haikou 570100, China

Correspondence should be addressed to Xiaoyi Zhou; xy.zhou.xy@gmail.com

Received 26 August 2020; Revised 6 November 2020; Accepted 6 December 2020; Published 31 December 2020

Academic Editor: Nanrun Zhou

Watermarking technology is commonly used to solve various problems in digital rights management and multimedia security. If a watermarking scheme with multiple purposes applies single method, it will easily cause the destruction of the hidden messages in particular attacks. For the copyright protection and tamper detection of color images, this research proposed a robust-fragile watermarking scheme. The two different embedding schemes embed the watermark into the *R* layer and *G* layer after NSST (nonsubsampled shearlet transform) and DWT (discrete wavelet transform) transformation. The hash sequence generated by the *R* layer and the *G* layer is served as fragile watermarks and is embedded into the *B* layer by the LSB (least significant bit) method. Finally, an improved rotation correction is applied to better extract the watermark under the rotation attack. Experimental results show that the proposed method is more accurate than the existing ones in terms of rotation angle correction and can effectively resist general attacks such as noise, filtering, and JEPG compression. Moreover, the proposed fragile watermark can locate the tamper position when malicious tamper occurs. Except cropping attack, the true-positive rate (TPR) reaches 1 for all attacks.

1. Introduction

Digital watermarking technology is an important research direction in information hiding. It refers to embed identification information (i.e., digital watermark) into the digital carrier, including multimedia, documents, and software, without affecting the useful values of the original carrier, and is not easy to be detected and modified. Therefore, it is an effective way to protect information security, such as anti-counterfeiting traceability and copyright protection. Earlier digital watermarking technologies [1, 2] focused on grayscale images, and watermarks were embedded in spatial or frequency domains. With the development of artificial intelligence and the special demand for host images, adaptive watermarking [3, 4], reversible watermarking [5], and deep learning watermarking [6] have received attention. In recent years, watermarking has been required to achieve higher robustness, and researchers expect more purposes are packed in a watermarking scheme; thus, it promotes the development of multipurpose watermarking.

Vaidya [7] proposed a multipurpose color image watermarking method. Three grayscale watermarks are embedded in the area after SVD, QR decomposition, and Schur decomposition to provide copyright protection and ownership verification of multimedia information. Darwish and Al-Khafaji [8] introduced a smart dual-watermark model that guarantees copyright protection for color images. It employs both successive and segmented watermarking techniques and uses the genetic algorithm to determine the embedding locations and scaling factors. Namratha and Kareemulla [9] used Lagrangian support vector regression methods to embed watermark in the frequency domains after DCT, DWT, and Fourier transformations. However, these methods have single purpose and apply only one embedding scheme, and thus, they increase the risk of watermark destruction. Singh et al. [10] exploited a self-recoverable dual-watermarking scheme to integrate copyright protection, tamper detection, and recovery into one scheme. The recovery watermark is embedded in the spatial domain, whereas robust watermark is embedded in the frequency domain. But it has poor invisibility, and the PSNR is around 30 dB. Shi et al. [11] proposed a region-adaptive semifragile dual-watermarking scheme, which embeds robust and fragile watermarks into the transformation domain after IWT and is independent of the embedded order. The PSNR value of the watermark image is about 40 dB.

Alyammahi et al. [12] developed a new multiple watermarking scheme for medical images which is based on spatial and discrete cosine transform domains; however, the scheme is only applicable to medical images. The methods [10–12] are used only for grayscale images and have poor invisibility. Peng et al. [13] proposed a multipurpose watermarking scheme, in which the robust watermark and the fragile watermark are embedded in the feature and nonfeature points, respectively, and the watermarks are mutually independent. Kunhu and Al-Ahmad [14] proposed a multiwatermarking algorithm which embeds the robust watermark in the DCT and hash authentication code in the spatial domain. Refs. [13, 14] are suitable for color images. However, they are not applicable to a wide range of color images. Ref. [13] is specialized in GIS applications and ref. [14] for vector maps.

The above methods have a common problem, that is, they cannot resist rotation attack. For that reason, Ye et al. [15] and Tian et al. [16] exploited SIFT (scale-invariant feature transform) and SURF (speeded up robust features) extraction feature points for rotation correction, respectively, and achieved remarkable results. Ye et al. [15] embedded the watermark in the center area of host image by using DCT and SVD and then saved the SIFT feature points of the watermark image to detect and correct possible geometric attacks. Tian et al. [16] designed a synchronization mechanism based on the SURF algorithm. Before embedding the watermark into the host image, the feature points in the original cover image are detected with the SURF algorithm and stored for rotation correction. But both options simply use the calculated average of the angle as the final rotation correction angle, which will cause a large deviation with such a small amount of dirty data.

In view of the above analysis, we have proposed a multiwatermarking scheme for color images that resists common robust and geometric attacks and has the ability to tamper detection. The contributions of the proposed method are as follows:

(1) Two different embedding methods are applied to embed robust watermarks on different layers. In this way, when one watermark is damaged, the other can be extracted, increasing the robustness for the watermark.

(2) Robust watermarks combined with fragile ones meet the needs of copyright protection and tamper detection.

(3) The rotation correction method is improved via quadtree decomposition and data cleansing, which reduces the number of feature points and impact from individual error data.

The rest of the paper is arranged as follows. Section 2 introduces background knowledge used, SIFT and NSST. Section 3 describes the embedding and extraction process of watermark in detail. Section 4 makes an experimental evaluation of the proposed method and compares the proposed scheme with the existing color image watermarking scheme. Finally, a summary is made in Section 5, and the next steps are planned.

2. Preliminaries

2.1. SIFT (Scale-Invariant Feature Transform). In 2004, Lowe proposed the famous scale-invariant feature transform (SIFT). The SIFT algorithm ensures that the local image features acquired still have good robustness in the face of rotation, scaling, projection transformation, and object occlusion through the following steps:

(1) Detect the extreme point in scale space: the scale space of a two-dimensional image is defined as follows:

$$L(x, y, \sigma) = G(x, y, \sigma) * Ix, y, \tag{1}$$

where $G(x, y, \sigma)$ represents the scaling variable Gaussian function and $I(x, y)$ represents the input image:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\left(x^2+y^2\right)/2\sigma^2}, \tag{2}$$

where (x, y) represents the spatial coordinate and σ represents the scale coordinate. The difference of the Gaussian function can be calculated by two similar scales separated by a constant multiplier k. It is defined as follows:

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma). \end{aligned} \tag{3}$$

(2) Extract the stable feature points: according to the extreme points obtained in step 1, filtering is used to select stable key points.

(3) Orientation assignment: by using the gradient distribution feature of the pixels in the area around the feature point to specify the dominant direction of each feature point, the modulus formula and the gradient direction formula are as follows:

$$\begin{aligned} m &= \sqrt{\left(L_{x+1,y} - L_{x-1,y}\right)^2 - \left(L_{x,y+1} - L_{x,y-1}\right)^2}, \\ \theta &= \arctan\left(\frac{L_{x,y+1} - L_{x,y-1}}{L_{x+1,y} - L_{x-1,y}}\right). \end{aligned} \tag{4}$$

(4) Key point descriptor: in the neighbourhood of each key point, the selected scale is used to measure the local gradient of the image.

2.2. NSST (Nonsubsampled Shearlet Transform). To ensure the antirotation attack function of the embedded watermark, the nonsubsampled shearlet transform (NSST) is adopted. NSST, which eliminates the downsamplers and upsamplers, is compared to the shearlet transform. The NSST is a fully shift-invariant, multiscale, and multidirectional expansion.

$$\mathrm{NLSP}_{j+1} = A_j f = \left(Ah^1_{j \prod_{k=1}^{j-1} Ah^0_k} \right), \tag{5}$$

where f is an image, NLSP_{j+1} is the detail coefficients at scale $j+1$, and Ah^0_k and Ah^1_j are low-pass and high-pass filters of NSLP at scale j and k, respectively. Given $N \times N$ image f^0_a and the number of the direction D_j, the procedure of the NSST described above at a fixed resolution scale j can be summarized as follows:

(1) Apply the NSLP to decompose f^{j-1}_a into a low pass image f^j_a of size $N \times N$ and a high pass image f^j_d
(2) Compute $\hat{f}^j_d$ in pseudopolar grid and then get Pf^j_d
(3) Apply a band-pass filtering Pf^j_d to obtain $\left\{ \hat{f}^j_{d,k} \right\}_{k=1}^{D_j}$
(4) Apply inverse FFT to obtain NSST coefficients $\left\{ \hat{f}^j_{d,k} \right\}_{k=1}^{D_j}$ in pseudopolar grid.

3. The Proposed Methods

In this paper, the host image is a 24-bit color image of size of 512×512, and the watermark image is a binary image of 32×32. The proposed method is illustrated in Figures 1 and 2.

3.1. Preprocessing of Watermark. Many chaotic systems have been proposed in previous studies [17, 18] for image encryption. In our scheme, the logistic chaos sequence is modified and applied to the image preprocessing. The watermark image is converted into a sequence S_1, and equation (6) is used to generate the logistic chaos sequence S_2 with the same lengthS_1. Then, S_1 is permuted according to the corresponding position of S_2 to get the scrambled watermark sequence S_1'. The logistic map is in a chaotic state when$X_0 \in [0, 1]$. That is to say, with initial value X_0, the sequence produced by logistic mapping is nonperiodic and nonconverged, but the common permutation methods such as Arnold are cyclical. In this respect, using logistic mapping provides greater security.

$$X_{n+1} = X_n \times \mu \times (1 - X_n), \tag{6}$$

where $\mu \in [0, 4]$ and $X \in [0, 1]$.

3.2. Embedding Procedure. The proposed solution embeds three watermarks, two for copyright protection and one for tamper detection (Algorithms 1–8). The detailed description is drawn in Figure 1.

3.3. Extracting Procedure. When the watermark is extracted, the calculated hash sequence is compared with the extracted hash sequence. If the two hash sequences are different, rotate the correction and then extract the two robust watermarks. Otherwise, extract the two robust watermarks directly. A detailed description is drawn in Figure 2.

4. Results and Discussion

To evaluate the proposed method, eight famous color images have been selected from the USC-SIPI image database including Airplane, Baboon, Lena, Peppers, House, Sailboat, Splash, and Tiffany with the size of 512×512 pixels as the host images. Also, select a binary image with the size of 32×32 as the watermark image. The host images and the watermark image are shown in Figure 4.

Figure 5 shows the relationship between robustness and PSNR as the strength of the two watermark embedding increases. Avg NC is the average of the watermark NC values after the watermarked image has been attacked by common attacks including Gaussian noise, salt-pepper noise, speckle noise, Gaussian LPF 3×3, and Gaussian LPF 5×5. In order to balance between invisibility and robustness, this paper adopts a compromise value. The step length λ in Algorithm 1 is set to 72, and Δ in Algorithm 2 is set to 15.

4.1. Analysis of Transparency. Table 1 and Figure 6 show the PSNR and SSIM of the proposed method and the existing method. The proposed scheme has a better PSNR value than [21, 22]. Unfortunately, the proposed scheme shows a worse PSNR value than [23], but on the contrary, the proposed scheme has a better SSIM value than [23]. SSIM extracts and combines three features of image brightness, structure, and contrast to make the score reflect the sensitivity of human eyes to a greater extent. Therefore, in general, higher SSIM can reflect the image quality better. A lower PSNR (which means more modifications to the image) will lead to a better robustness performance with the same SSIM. Therefore, our scheme can theoretically obtain a better robust performance and ensure higher visual quality.

4.2. Testing the Watermark Robustness. To verify the robustness, we performed common image processing operations (such as JPEG compression, salt-pepper noise, addition of Gaussian noise, and filter ingesting attack) and rotation attacks on watermark images. At the same time, our scheme was compared with [21–25].

Figure 7 shows the NC values of different images under JPEG attacks of different intensities and the comparison of extracted watermarks by different methods. When QF is no less than 20%, the watermark quality extracted by our scheme is higher than all other schemes.

Figure 8 shows a comparison of the results of the extracted watermark from the watermarked Lena image after Gaussian noise attack and salt-pepper noise attack. The watermark extraction effect of the proposed method is better

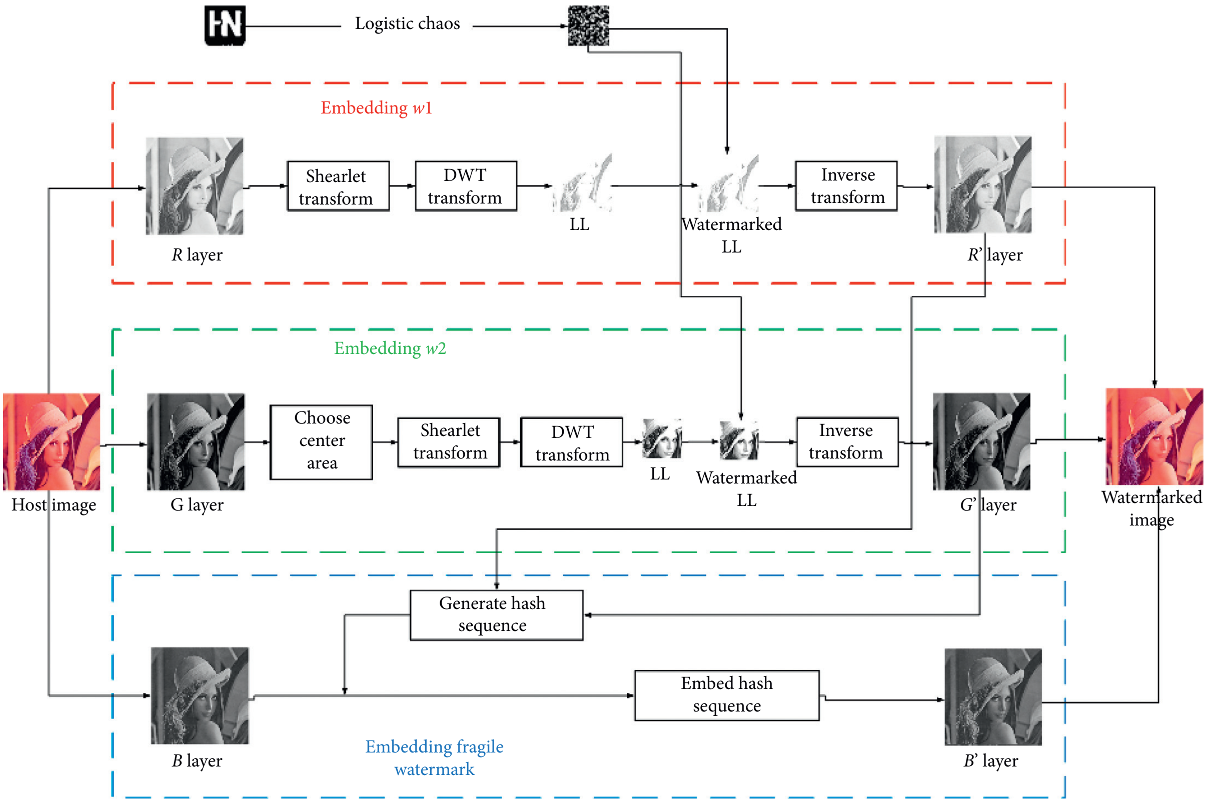


Figure 1: Flow diagram of the watermark embedding.

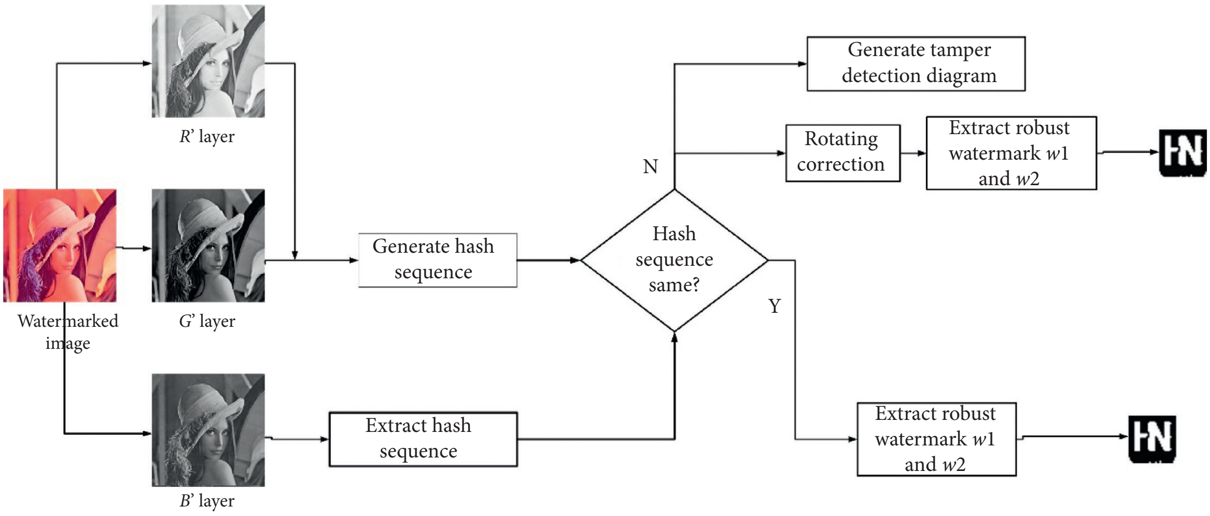


Figure 2: Flow diagram of the watermark extracting.

than [21, 22, 25] in Gaussian noise (0.1%) and better than [24] in salt-pepper noise (0.1%).

Figure 9(a) shows the comparison of the proposed method and the scheme proposed by [24] under different filters on the image Peppers. In [24], the PSNR value of the watermarked image is 43.79 dB. It can be seen that with a better PSNR, the effect of the proposed scheme in the mean and the Gaussian filtering is better than [24], but is slightly worse in the median filtering.

Figure 9(b) compares the proposed method and [21] under different filters on the image Lena. In [21], set the embedding parameter value alpha to 16.27, in which case the PSNR of the image Lena is 45.605 dB, while the PSNR is 45.7669 dB in our scheme, which indicates the proposed scheme performs better.

Table 2 shows a comparison of the number of feature points to be stored by the proposed method with [15], showing that the proposed method stores fewer points in

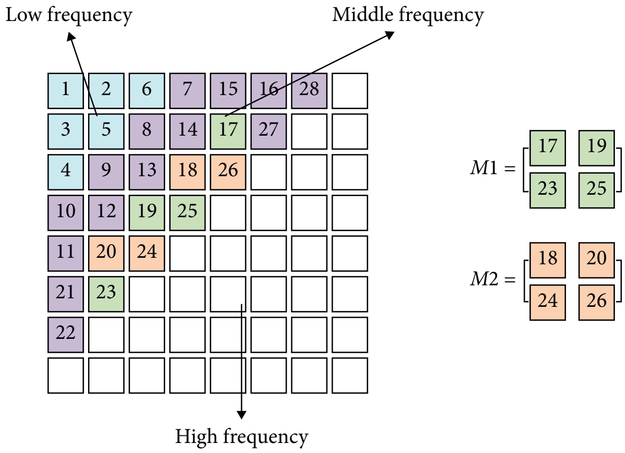


Figure 3: Construction of matrices $M1$ and $M2$ with the middle frequency of the DCT coefficients.

(1) Step 1: apply the one-level shearlet transform on the R layer of the color image, thus to obtain a low pass subband A_0.
(2) Step 2: apply the DWT transformation to A_0 $[\mathrm{LL}, \mathrm{HL}, \mathrm{LH}, \mathrm{HH}] = \mathrm{DWT}(A_0)$.
(3) Step 3: divide the low-frequency area (LL) into nonoverlapping blocks of 8×8, and apply DCT on each block.
(4) Step 4: select the middle frequency of the DCT coefficients from one block [16], which consists of two matrices, M_1 and M_2. The construction of matrices with middle frequency is given in Figure 3.
(5) Step 5: use SVD to decompose M_1 and M_2 to get singular value matrices. The singular value matrices of M_1 and M_2 are S_1 and S_2, respectively.
(6) Step 6: use the following equations to embed the watermark [16]: $S_1(1,1) = \begin{cases} E + \lambda, & if\, W_e = 1, \\ E - \lambda, & if\, W_e = 0 \end{cases}$ and $S_2(1,1) = \begin{cases} E - \lambda, & if\, W_e = 1, \\ E + \lambda, & if\, W_e = 0 \end{cases}$.
(7) Step 7: repeat steps 4–6 until all watermarks are embedded, and then perform a reverse transformation to get a watermarked R' layer.

Algorithm 1: Embedding robust watermark $w1$.

(1) Step 1: select the layer G of the color image and the inscribed circle's inscribed square of the carrier image I as the watermark embedding area x, for the reason that the image information in the inscribed circle S of I will not lose due to the rotation.
(2) Step 2: apply the one-level shearlet transform on x, and obtain a low pass subband A_x.
(3) Step 3: apply DWT to A_x $[\mathrm{LL}, \mathrm{HL}, \mathrm{LH}, \mathrm{HH}] = \mathrm{DWT}(A_x)$.
(4) Step 4: divide the low-frequency area (LL) into nonoverlapping blocks of 4×4 sizes, and SVD decomposition is carried out on each block.
(5) Step 5: get the value of $S(1,1)$ from the singular value matrix $(1,1)$. The quantization step size is Δ, set $\delta = \mathrm{mod}(S(1,1), \Delta)$. Embed the watermark by quantifying $S(1,1)$ using the following equations. The following equations are one kind of optimal quantization formulas proved in [19]: $S(1,1)' = S(1,1) - \delta + (1/4)\Delta$, where $W_e = 0$ and $\delta \in [0, (3/4)\Delta)$
$S(1,1)' = S(1,1) - \delta + (5/4)\Delta$, where $W_e = 0$ and $\delta \in ((3/4)\Delta, \Delta)$
$S(1,1)' = S(1,1) - \delta - (1/4)\Delta$, where $W_e = 1$ and $\delta \in [0, (1/4)\Delta)$
$S(1,1)' = S(1,1) - \delta + (3/4)\Delta$, where $W_e = 1$ and $\delta \in [(1/4)\Delta, \Delta)$.
(6) Step 6: repeat step 5 until all watermarks are embedded, and then perform a reverse transformation to get the watermarked G' layer.

Algorithm 2: Embedding robust watermark $w2$.

(1) Step 1: divide the color image which is embedded robust watermarks $w1$ and $w2$ into nonoverlapping blocks of 16×16.
(2) Step 2: use the layer R and the layer G to generate hash sequence.
(3) Step 3: embed the watermark sequence in the layer B using the LSB embedding method [20].
(4) Step 4: repeat steps 2–3 until all the blocks are processed.

Algorithm 3: Embedding fragile watermark.

(1) Step 1: use SIFT for feature point extraction [15].
(2) Step 2: use the quadtree to decompose the watermark image, leaving only one feature point in each block, and the points are recorded as a rotary recovery key.

Algorithm 4: Feature point extraction.

(1) Step 1: divide the attacked image into nonoverlapping small pieces of 16 × 16.
(2) Step 2: use the layer R and the layer G to generate the hash sequence.
(3) Step 3: extract the stored watermark sequence from the layer B using the LSB algorithm and compared with the generated sequence by step 2 [20].
(4) Step 4: repeat steps 2-3 until the full picture is traversed. If the comparison is successful, no action is taken; otherwise, it is marked on the image.

Algorithm 5: Extracting fragile watermark.

(1) Step 1: extract the feature points of the attacked image through the SIFT method, and generate collection **S.**
(2) Step 2: compare corresponding points in collection **S** and the collection of recorded feature points as **T**, and if the comparison is successful, record the coordinates of the feature points on the original graph and attacked image to produce the feature point pair.
(3) Step 3: take any two matching successful feature point pairs, and the two points from **S** and the two points from **T** are recorded to generate vectors **a** and **b**, respectively. The angle φ between the vector **a** and the vector **b** is calculated as $\varphi = \arccos(a \cdot b/|a| \cdot |b|)$, where $|a|$ and $|b|$ represent the module of a and b, respectively. Traverse all the point pairs to generate collection A which consists of all angles φ [15].
(4) Step 4: use the box plot to clean collection **A**. Calculate the next quartile Q_1, upper quartile Q_3, and intermediate quartile extreme difference IQR. Remove the outlier values which are greater than $Q_3 + 1.5IQR$ or less than $Q_1 - 1.5IQR$, and generate collection **B**.
(5) Step 5: calculate the mean of all angles in collection **B**: $\beta = (1/n)\sum_{i=1}^{n}\varphi_i$, where **n** represents the number of elements in collection **B**. Refer to it as the rotation recovery angle.

Algorithm 6: Rotation correction.

(1) Step 1: transform the layer R of the attacked image with the same transformation when embedding watermark $w1$. For more information, refer to steps 1–5 in Algorithm 1.
(2) Step 2: get the singular value matrix S_1' and S_2' through step 1, and then use the following equation for watermark extraction [16]:

$$W_e' = \begin{cases} 1, \; if \; S_1'(1,1) > S_2'(1,1), \\ 0, \; if \; S_1'(1,1) < S_2'(1,1) \end{cases}.$$

Algorithm 7: Extracting robust watermark $w1$.

(1) Step 1: transform the G layer of the attacked image with the same transformation as the embedding procedure of watermark $w2$. For more information, refer to steps 1–4 in Algorithm 2.
(2) Step 2: get the singular value matrix S' through the steps above, set $\delta' = \mathrm{mod}(S'(1,1), \Delta)$, and then use the following equation for watermark extraction [19]: $W_e' = \begin{cases} 0, \text{ if } \delta' < (1/2)\Delta, \\ 1, \text{ if } \delta' > (1/2)\Delta \end{cases}$.

Algorithm 8: Extracting robust watermark $w2$.

each image than [15]. Figure 10 presents the difference between the quality of watermark extraction and rotation angle correction before and after data cleaning, and data cleaning plays a big role when large angle rotation attacks. Table 3 shows that the proposed scheme works better against rotation attacks than [23, 24].

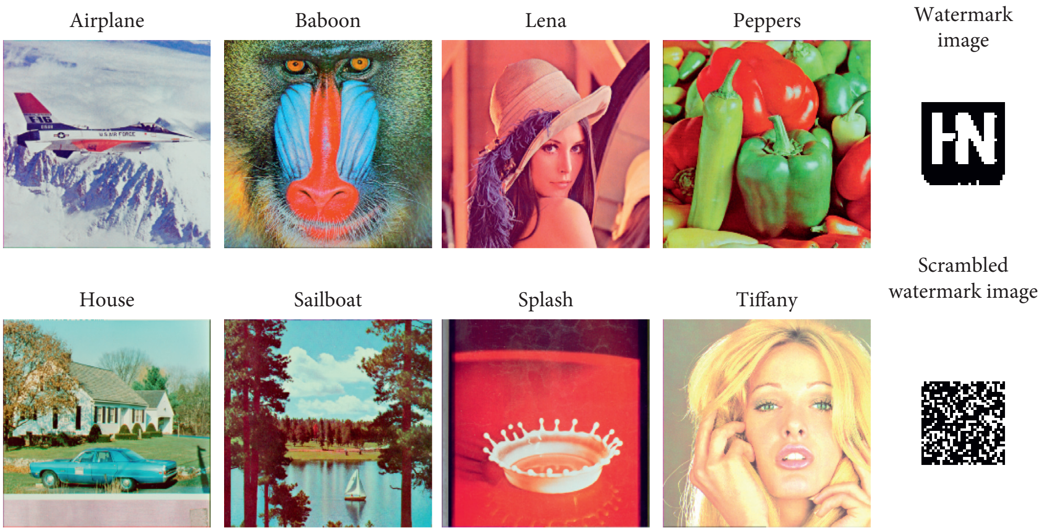
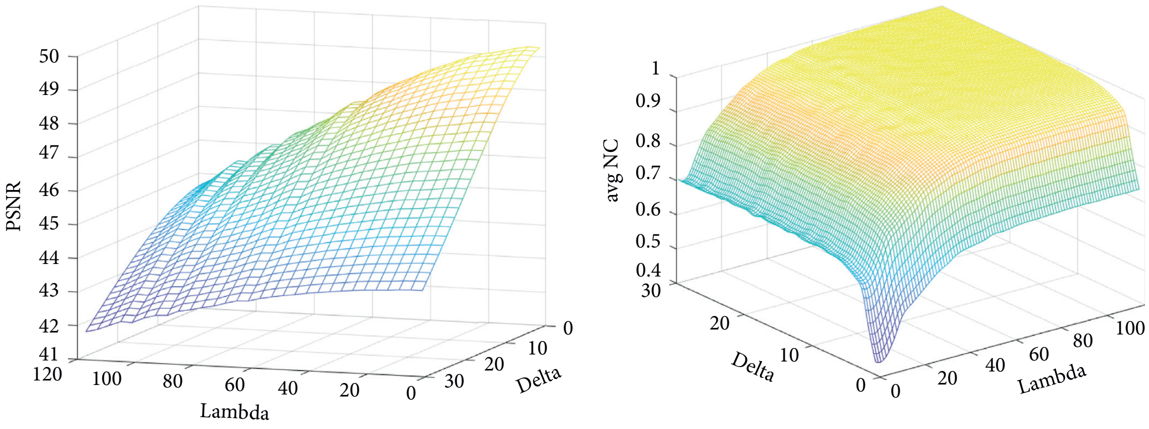


Figure 4: Original host images and a watermark image.



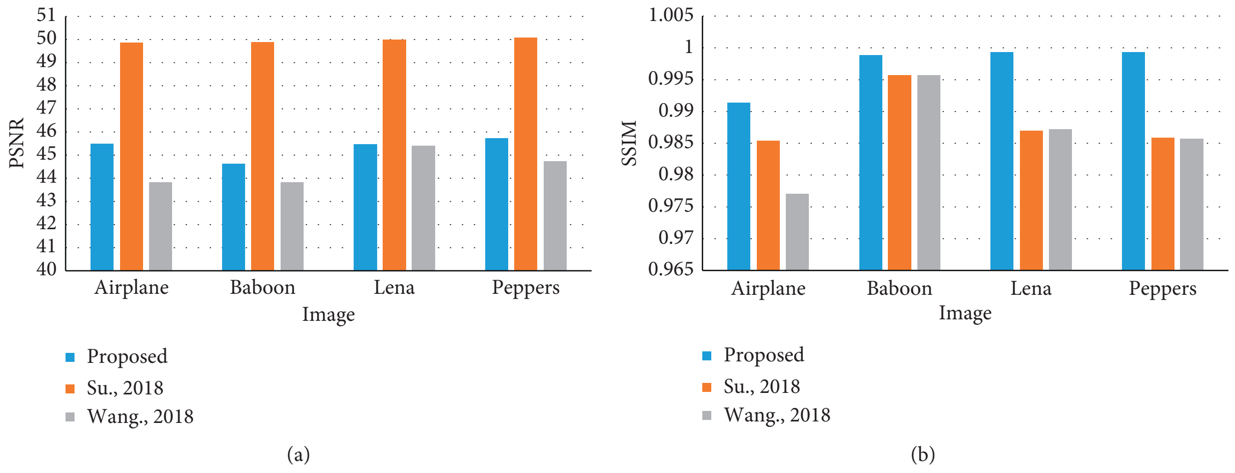
(a)

(b)

Figure 5: The average NC value in different lambda and delta: (a) the relationship between embedded strength and PSNR, and (b) the relationship between embedded strength and robustness.

Table 1: The PSNR comparison results between the proposed method and [21].

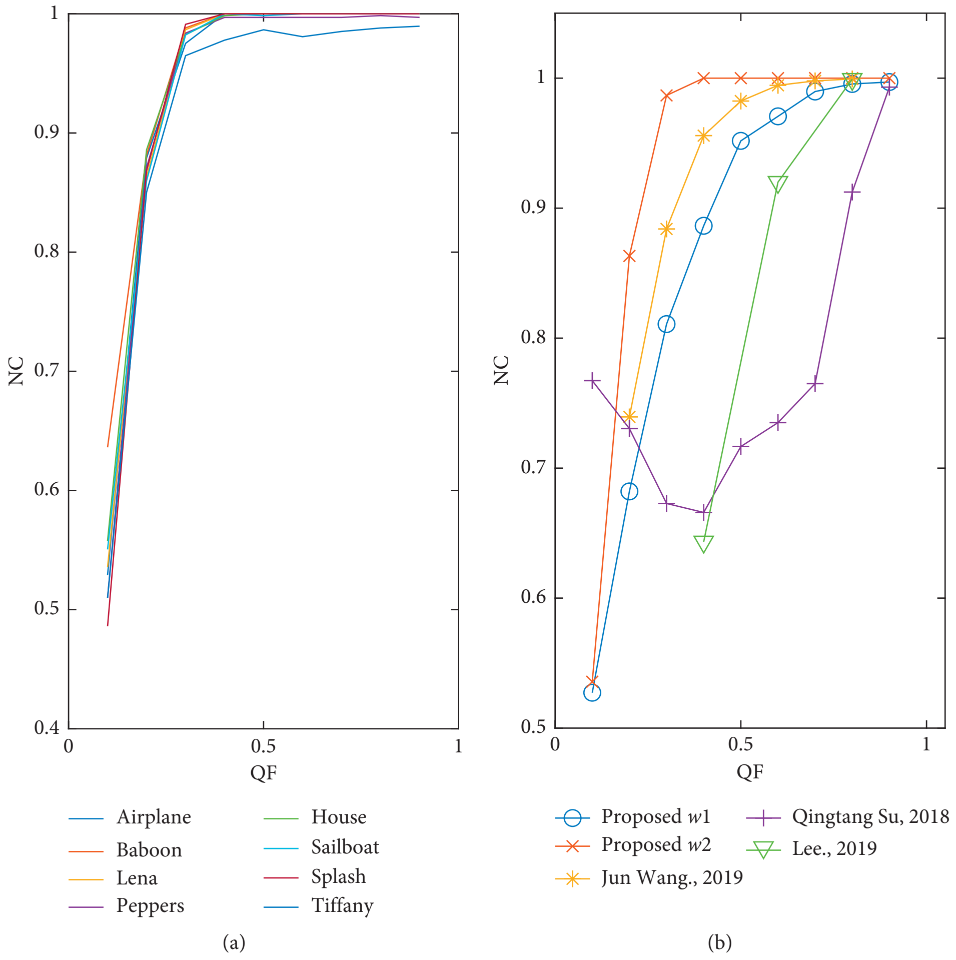
Image	Airplane	Baboon	Lena	Peppers	House	Sailboat	Splash	Tiffany
Proposed	45.29	44.44	45.46	45.73	45.05	45.40	46.22	46.27
[21]	40.63	40.19	40.35	40.26	40.76	40.22	39.95	40.61



(a)

(b)

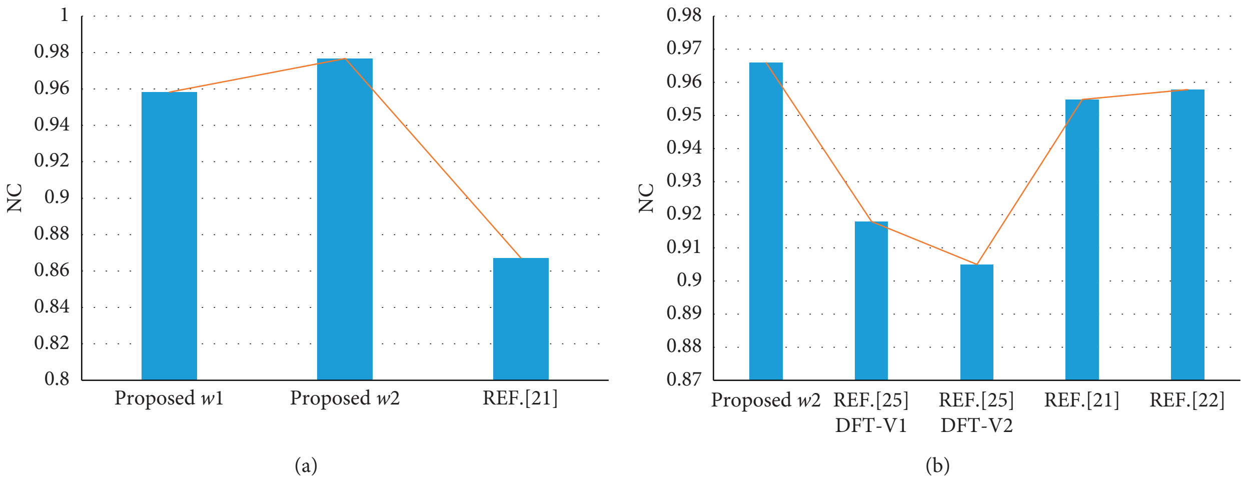
Figure 6: The invisibility comparison results about the different methods in terms of PSNR and SSIM: (a) PSNR and (b) SSIM.



(a)

(b)

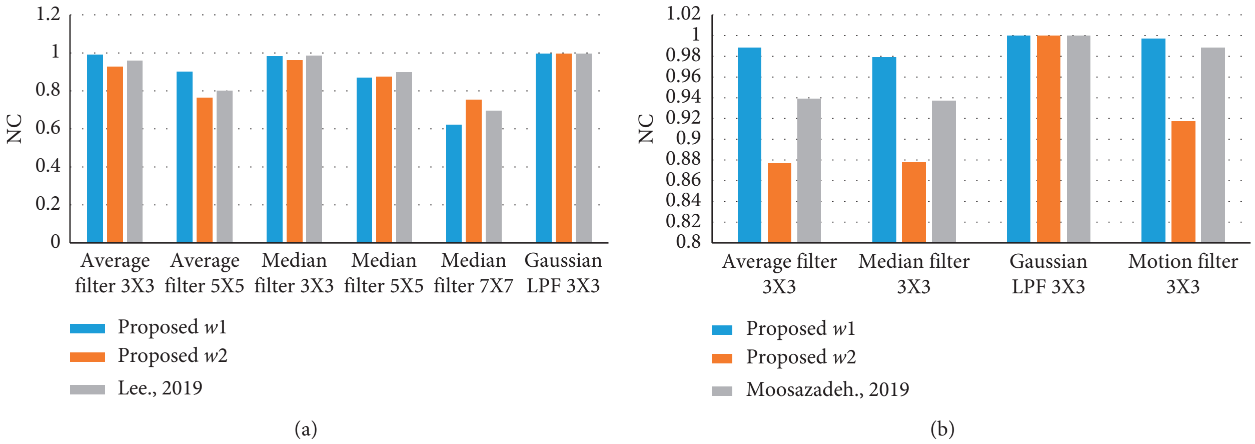
Figure 7: The results after the JPEG attack: (a) the watermark extraction effect after JPEG attacks of different intensities and (b) the comparison of extracted watermarks by different methods after JPEG attacks.



(a)

(b)

Figure 8: The results of noise attacks: (a) the comparison of extracted watermarks by different methods after salt-pepper noise attacks and (b) the comparison of extracted watermarks by different methods after Gaussian noise attacks.



(a)

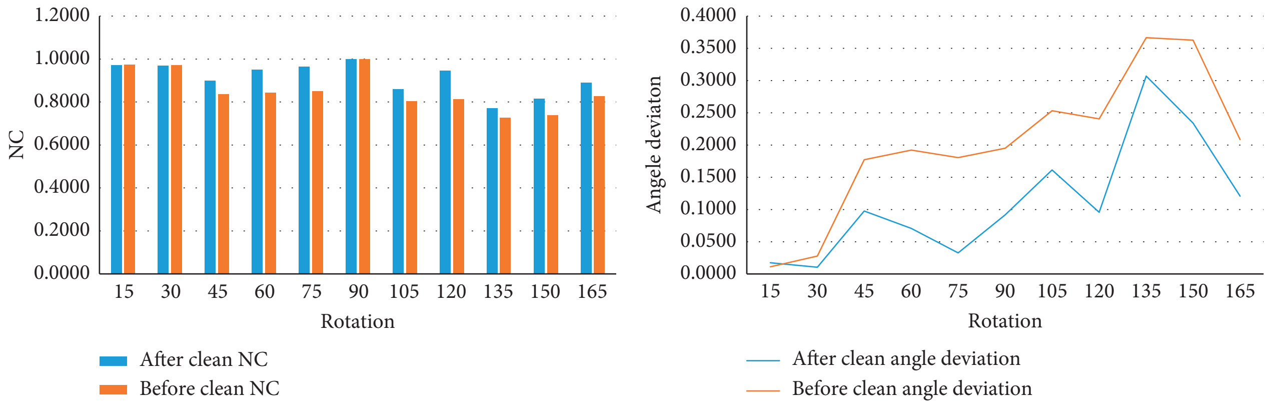
(b)

Figure 9: The result of filtering attacks: (a) the comparison of extracted watermarks after filtering attack and (b) the comparison of extracted watermarks after filtering attack.

Table 2: The number of key points extracted from different images.

Image	Airplane	Baboon	Lena	Peppers	House	Sailboat	Splash	Tiffany
Proposed	**176**	**262**	**73**	**43**	**237**	**283**	**22**	**16**
[15]	280	264	91	48	291	385	38	23

4.3. Tamper Detection Tests. The performance of the tamper detection was tested by blurring, sharpening, adding salt and pepper noise, adding Gaussian noise, average filtering, cropping, and so on. The proposed scheme splits the image into small blocks of 16×16, which is smaller than the blocks in [26] (small blocks split to 32×32), so the tamper detection is more accurate. Random block attacks on the watermark Lena image are shown in Figure 11, and the corresponding experimental data are shown in Table 4. The true-positive rate (TPR) is 1, and the false-negative rate (FNR) is 0 for all attacks except cropping. The TPR of cropping attack is no more than 0.55. The average false-positive rate (FPR) is 0.060, and the average accuracy (ACC) is 0.939.



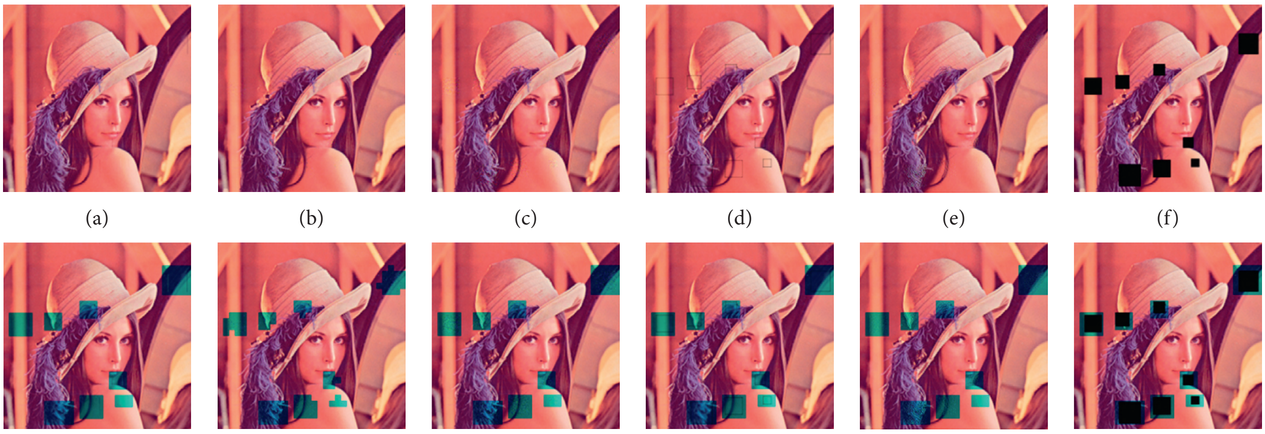
(a)

(b)

Figure 10: The result of data cleansing: (a) the value of NC of extracted watermarks before and after the data cleaning and (b) the angle deviation before and after the data cleaning.

Table 3: The comparison of extracted watermarks after rotation attacks.

Rotation	Proposed	[24]	[23]
30	**0.9722**	0.9368	0.7612
60	**0.9692**	0.9475	0.7709
90	**1**	1	0.8917



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

Figure 11: Random block attacks of the watermark Lena image: (a) blurring, (b) salt and pepper noise, (c) Gaussian noise, (d) average filter, (e) sharpening, (f) cropping, and (g–l) detection of the tampered regions of the watermarked image.

Table 4: Tamper detection results under random block attacks.

	FPR	FNR	TPR	ACC
Blurring	**0.0532**	0	1	0.9498
Salt and pepper noise	**0.0922**	0	1	0.9092
Gaussian noise	**0.0531**	0	1	0.9499
Average filter	**0.0532**	0	1	0.9499
Sharpening	**0.0531**	0	1	0.9499
Cropping	**0.0532**	0.4599	0.5401	0.9235

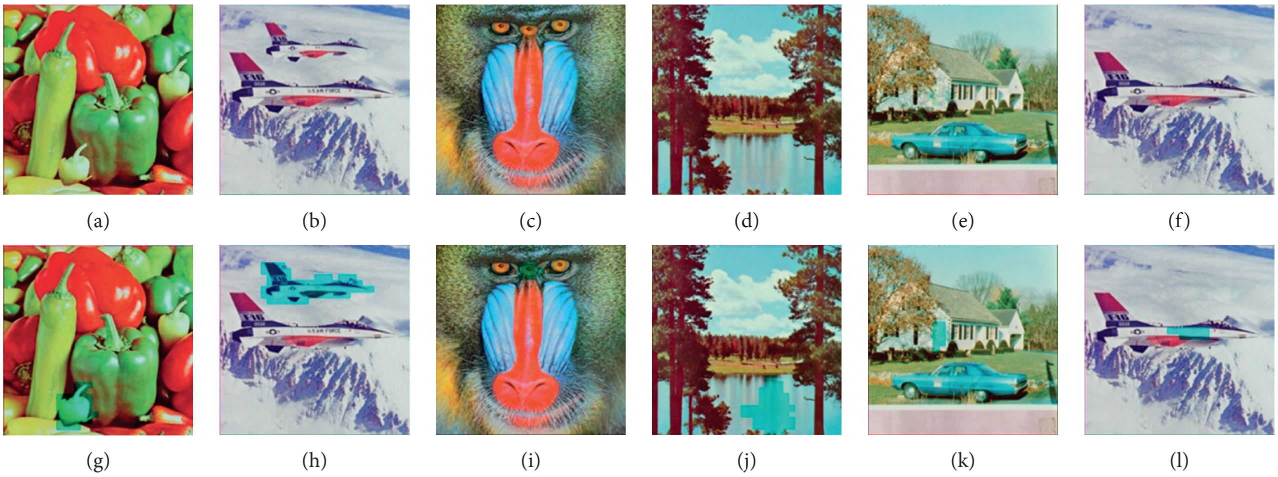


Figure 12: Results of object attacks: (a) attacked image in "Peppers" by adding a new pepper, (b) attacked image in "Airplane" by adding another airplane, (c) attacked image in "Baboon" by adding an eye, (d) attacked image in "Sailboat" by removing the boat, (e) attacked image in "House" by removing a window, and (f) attacked image in "Airplane" by removing the "USA AIR FORCE", and (g–l) results of mark detection.

Table 5: Tamper detection results under object attacks.

	FPR	FNR	TPR	ACC
Blurring	**0.0161**	0	1	0.9842
Salt and pepper noise	**0.0060**	0	1	0.9940
Gaussian noise	**0.0071**	0	1	0.9929
Average filter	**0.0198**	0	1	0.9809
Sharpening	**0.0047**	0	1	0.9953
Cropping	**0.0362**	0	1	0.9653

Figure 12 clearly shows that the proposed method is successfully able to detect and locate some types of tampering attacks. The corresponding experimental data are shown in Table 5, which shows that the proposed scheme has good tamper detection capability.

5. Conclusions

We have proposed a new comprehensive watermarking scheme for color images. Two robust watermarking methods and one fragile watermarking method are applied to guarantee copyright protection and tamper detection, and an improved SIFT method is used for rotation correction. This research uses different ways to embed two robust watermarks, so it can effectively resist more attacks compared to single watermarking schemes. Moreover, the angle collection is cleaned before rotation detection, and some outliers are removed, thus to improve the accuracy of rotation correction angle. For tamper detection, except cropping, the TPR is 1 for all attacks. However, there are still some issues need to be solved in the future, such as adaptively adjusting the embedding intensity according to the features of the image and reducing the length of the key used for rotation correction.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported in part by the Hainan Provincial High-level Talent Project (Grant no. 2019RC044) and in part by the Research Project of Education and Teaching Reform of Hainan University (Grant no. hdjy2053) and Natural Science Foundation of Hainan Province (Grant no. 618QN218).

References

[1] N. S. Kumaran and S. Abinaya, "Comparison analysis of digital image watermarking using DWT and LSB technique," in *Proceedings of the 2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, India, April 2016.

[2] M. A. Khan, U. Khan, and A. Ali, "Chaos based spatial domain robust image watermarking scheme," in *Proceedings of the 2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, Malaysia, August 2018.

[3] X. Zhou, C. Cao, J. Ma, and L. Wang, "Adaptive digital watermarking scheme based on support vector machines and

optimized genetic algorithm," *Mathematical Problems in Engineering*, vol. 2018, Article ID 2685739, 9 pages, 2018.

[4] J. Zhang, X. Zhou, J. Yang, C. Cao, and J. Ma, "Adaptive robust blind watermarking scheme improved by entropy-based SVM and optimized quantum genetic algorithm," *Mathematical Problems in Engineering*, vol. 2019, Article ID 7817809, 16 pages, 2019.

[5] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.

[6] Z. Yue, S. Ding, L. Zhao et al., "Privacy-preserving time series medical images analysis using a hybrid deep learning framework," *ACM Transactions on Internet Technology*, vol. 37, no. 4, pp. 1–22, 2019.

[7] S. P. Vaidya, "Multipurpose color image watermarking in wavelet domain using multiple decomposition techniques," in *Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, April 2018.

[8] S. M. Darwish and L. D. S. Al-Khafaji, "Dual watermarking for color images: a new image copyright protection model based on the fusion of successive and segmented watermarking," *Multimedia Tools and Applications*, vol. 79, no. 9-10, pp. 6503–6530, 2020.

[9] C. M. Namratha and S. Kareemulla, "Multi image watermarking using Lagrangian support vector regression," in *Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, May 2016.

[10] P. Singh, S. Agarwal, S. Agarwal, and S. Agarwal, "A self recoverable dual watermarking scheme for copyright protection and integrity verification," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6389–6428, 2017.

[11] H. Shi, M.-c. Li, C. Guo et al., "A region-adaptive semi-fragile dual watermarking scheme," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 465–495, 2016.

[12] S. Alyammahi, F. Taher, H. Al-Ahmad, and T. McGloughlin, "A new multiple watermarking scheme for copyright protection and image authentication," in *Proceedings of the 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Abu Dhabi, United Arab Emirates, October 2016.

[13] Y. Peng, H. Lan, M. Yue, and Y. Xue, "Multipurpose watermarking for vector map protection and authentication," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 7239–7259, 2018.

[14] A. Kunhu and H. Al-Ahmad, "Multi watermarking algorithm based on DCT and hash functions for color satellite images," in *Proceedings of the 2013 9th International Conference on Innovations in Information Technology (IIT)*, Abu Dhabi, United Arab Emirates, March 2013.

[15] X. Ye, X. Chen, M. Deng, and Y. Wang, "A SIFT-based DWT-SVD blind watermark method against geometrical attacks," in *Proceedings of the 2014 7th International Congress on Image and Signal Processing*, Dalian, China, October 2014.

[16] C. Tian, R. Wen, W. Zou, and L. Gong, "Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 7515–7541, 2020.

[17] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[18] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, p. 105816, 2020.

[19] L. I. Xu-dong, "Optimization analysis of formulas for quantization-based image watermarking," *Opto-Electronic Engineering*, vol. 37, no. 2, pp. 96–102, 2010.

[20] W. N. Lie and L. C. Chang,, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system," in *Proceedings of the 1999 International Conference on Image Processing (Cat. 99CH36348)*, pp. 286–290, IEEE, Kobe, Japan, 1999.

[21] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-Based optimization," *Journal of Information Security and Applications*, vol. 47, pp. 28–38, 2019.

[22] J. Wang, W. B. Wan, X. X. Li, J. D. Sun, and H. X. Zhang, "Color image watermarking based on orientation diversity and color complexity," *Expert Systems with Applications*, vol. 140, p. 112868, 2020.

[23] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, no. 1, pp. 91–106, 2018.

[24] Y.-S. Lee, Y.-H. Seo, and D.-W. Kim, "Blind image watermarking based on adaptive data spreading in n-level DWT subbands," *Security and Communication Networks*, vol. 2019, Article ID 8357251, 11 pages, 2019.

[25] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, Article ID 164562, 2020.

[26] E. Gul and S. Ozturk, "A novel hash function based fragile watermarking method for image integrity," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 17701–17718, 2019.