Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-07902-9

Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization

Lina Zhang[1] · Deyun Wei[1]

Received: 9 August 2018 / Revised: 22 May 2019 / Accepted: 20 June 2019
Published online: 01 July 2019

Abstract
Robust invisible watermarking plays an important role in copyright protection. Such watermarking has high requirements for robustness and security, and transparency and capacity cannot be ignored. Although there are many algorithms using singular value decomposition, most algorithms do not take security and reliability into account. Moreover, a meaningful watermark cannot be extracted under some attacks, resulting in the failure of copyright protection. In this paper, combined with particle swarm optimization (PSO), a secure and robust dual-embedded watermarking algorithm is proposed. First, the watermark image is encrypted by the generalized Arnold transform, then the original host image and the encrypted watermark image are processed by discrete cosine transform and multi-level discrete wavelet transform, and the singular values of the watermark image are embedded into the low-frequency and high-frequency regions of the host image, respectively. In addition, the embedding factor matrices are optimized by PSO. The simulation results based on the normal and medical host and watermark images show that the algorithm can meet the four basic characteristics of the watermarking algorithm. Moreover, the proposed watermarking algorithm has high capacity and good robustness, and can extract watermark with good visual effect under most attacks, so it can be used in copyright protection.

Keywords Image watermarking · Particle swarm optimization · Generalized Arnold transform · Discrete cosine transform · Discrete wavelet transform · Singular value decomposition

1 Introduction

With the development of Internet technology, we can obtain data resources more conveniently and quickly [15, 21]. But at the same time, there is a problem of copyright ownership [32]. The emergence of information hiding technology provides an effective way to solve copyright

✉ Lina Zhang
linazhang2017@126.com

[1] School of Mathematics and Statistics, Xidian University, Xi'an 710126 Shaanxi, China

problems [46]. In recent years, digital watermarking technology has received more and more attention, and many watermarking algorithms have been proposed [2, 7, 8, 13, 16, 26, 32, 40, 46]. Digital watermarking is to embed the watermark that represents copyright information into the digital work without reducing its quality. When copyright disputes arise, the watermark is extracted to verify copyright.

According to the hidden position of the watermark, the watermarking algorithm is divided into two categories: spatial domain and transform domain [40]. Although the spatial domain algorithm is simple, its robustness is poor, while the transform domain watermarking has strong robustness [1]. Therefore, transform domain watermarking is the main research trend, and robust watermarking for copyright protection and fragile watermarking for image authentication are the focus of most current research. Discrete wavelet transform (DWT) and discrete cosine transform (DCT), as well as discrete Fourier transform (DFT), are the most commonly used transform methods [22]. The stability of singular value decomposition (SVD) is very good [38], but the computational requirements are high. Therefore, SVD is usually combined with the transform domain methods in the watermarking algorithm [5, 14, 24]. Because DCT has good energy compression capability [23], DWT has the advantages of good robustness and multi-scale analysis [35], it is common to combine DCT or DWT with SVD. This paper mainly studies the robust watermarking for copyright protection, and the four important features of such watermarking are invisibility, security, robustness and capacity. We aim to improve the robustness of watermarking algorithm as much as possible under the premise of ensuring security and meeting invisibility.

In recent years, many watermarking algorithms combining transform domain methods with SVD have been proposed, especially DWT and DCT [4, 6, 7, 10–12, 16–18, 29–31, 36, 37, 39, 41–45, 47, 48]. There are also many related algorithms [8, 13, 20, 26, 41, 47]. Furqan et al. [8] proposed applying one-level DWT to the cover image, then performing SVD on each sub-band and the watermark image, and finally using the singular value of the watermark to modify the singular value of the four sub-bands in the host image. Different from [8], Nandi et al. [26] only selected the low-frequency sub-band for the watermark embedding, and optimized the embedding factor by particle swarm optimization (PSO). In order to improve the security of the watermarking algorithm, Liu et al. [20] introduced the RSA algorithm to encrypt the parameters in the process of encrypting the watermark with the logistic map. Then, the host image was processed with one-level DWT, and the scrambled watermark was added directly to the singular value of the low frequency sub-band in the host image. Singh et al. [41] proposed the use of DCT on the basis of DWT and SVD. In this algorithm, the DCT and SVD were used to process the watermark image and the low-frequency sub-band in the host image, and the watermark was embedded by adding the singular value of the watermark to the singular value of the low-frequency region in the host image. In addition, Zear et al. [47] also used DWT, DCT and SVD in image watermarking. Firstly, the host image was decomposed with three-level DWT, then DCT and SVD were used to the selected medium sub-band LH_1 and the encrypted watermark. Finally, the singular value of the cover image was modified to embed the watermark. In watermark extraction, BP neural network was applied to the extracted watermark to remove noise and interference and improve its robustness. However, in the algorithm presented by Hurrah et al. [13], the one-level DWT was applied directly to the gray image, then the low-frequency sub-band LL was decomposed into non-overlapping 8*8 blocks, and each 8*8 block was further divided into four 4*4 sub-blocks, and each block was processed by DCT, then the encrypted watermark bit was embedded by modifying the difference between the selected two DCT coefficients. Although there are many such algorithms, the SVD-based algorithms generally have the false positive problem (FPP). Most of these algorithms do not take the security and reliability of the algorithm into account, and the algorithms cannot extract meaningful watermarks under some attacks, which will lead to the failure of copyright protection. To solve the above problems, we introduce the generalized Arnold transform, embedding factor matrix, multi-level DWT and double embedding method.

This paper propose a robust hybrid domain image watermarking algorithm based on DCT and DWT. The main contributions of this paper are as follows: Firstly, compared with the common Arnold transform, the use of the generalized Arnold transform improves the security of the algorithm due to the increase of keys. Secondly, the DCT and multi-level DWT are used successively, and the watermark is embedded into the high-level region of the DWT domain, which improves the robustness and invisibility of the algorithm. Thirdly, embedding watermark in low-frequency and high-frequency sub-bands will not increase the running time of the algorithm as choosing all sub-bands, and it will not have poor robustness like selecting only one sub-band. Fourthly, the use of embedded factor matrices and PSO greatly improves the robustness of the algorithm, and ensures the balance between the invisibility and robustness of the algorithm. The comparative analysis also shows that our algorithm has better robustness than other related algorithms and performs well in terms of invisibility, security, and watermark capacity.

The novelty of this paper mainly includes the following points:

1) The watermark image is encrypted using the generalized Arnold transform to avoid FPP, and the security of the proposed watermarking algorithm is improved due to the added keys.
2) The host image and encrypted watermark image are processed by combining DCT with multi-level DWT, and the use of multi-level DWT enhances the invisibility of the algorithm.
3) The watermark is hidden in the low-frequency and high-frequency sub-bands of the third-level DWT domain of the host image to achieve the double embedding of the watermark, which greatly improves the robustness of the algorithm.
4) Different embedding factors in the form of diagonal matrix are used in low and high frequency regions respectively, and they are optimized by PSO to obtain adaptive scale factor matrices.

This paper is organized as follows. Section 2 gives the theoretical knowledge used in the algorithm. The proposed watermarking algorithm and the optimization of the embedded factor matrix are described in detail in Section 3. Section 4 evaluates the algorithm from four aspects: transparency, security, robustness and capacity, and gives a comparison with the existing algorithms. The conclusion of this paper is given in the Section 5.

2 Theoretical background

2.1 Generalized Arnold transform (GAT)

The GAT formula for $N \times N$ image matrix can be expressed as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N, \tag{1}$$

where a and b are parameters, (x, y) and (x', y') are the positions of the pixel points in the original image and the scrambled image, respectively [48]. The purpose of the GAT is to mess up the position of the original image.

The inverse transformation formula of GAT can be written as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N. \tag{2}$$

For a given image, it is scrambled s times using Eq. (1) to get a scrambled image. In order to reduce the computational complexity, when decrypting the image, this paper uses Eq. (2) to performs iterations on the scrambled image instead of using the Eq. (1) to perform T − s iterations, where T is the period of the transform.

2.2 Discrete cosine transform (DCT)

The DCT is the real part of the DFT and has a stronger information concentration capability than DFT. For most natural images, the DCT can put most of the information on fewer coefficients, which improves the coding efficiency [9]. Because DCT domain has great advantages in resisting JPEG compression, it has important applications in digital watermarking.

For an $N \times N$ image matrix, its two-dimensional DCT can be expressed as [39]:

$$F(u,v) = c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j) \cos\left[\frac{(i+0.5)\pi}{N} u\right] \cos\left[\frac{(j+0.5)\pi}{N} v\right]. \tag{3}$$

The two-dimensional inverse discrete cosine transform (IDCT) can be defined as:

$$f(i,j) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u)c(v) F(u,v) \cos\left[\frac{(i+0.5)\pi}{N} u\right] \cos\left[\frac{(j+0.5)\pi}{N} v\right], \tag{4}$$

where

$$c(u) = \begin{cases} \sqrt{\frac{1}{N}}, u = 0 \\ \sqrt{\frac{2}{N}}, u \neq 0 \end{cases}, c(v) = \begin{cases} \sqrt{\frac{1}{N}}, v = 0 \\ \sqrt{\frac{2}{N}}, v \neq 0 \end{cases}. \tag{5}$$

2.3 Discrete wavelet transform (DWT)

The significance of wavelet decomposition lies in the ability to decompose the image matrix at different scales, and the selection of different scales can be determined according to different images [13]. Due to its good multi-resolution analysis, energy compression characteristics, and compatibility with compression standards, it has good robustness against noise and compression attacks.

Because of its good properties, DWT is widely used in image processing [27]. It can decompose an image into a low frequency sub-band LL and three high frequency sub-bands

HL, *LH*, *HH*, this process can be repeated for further decomposition [25]. The low frequency sub-band is the image's profile coefficient band, which has very good stability and plays an important role in watermark extraction. The high frequency is the detail sub-band, which reflects the original image's edge, outline, texture and other information.

2.4 Singular value decomposition (SVD)

The SVD of $M \times N$ matrix can be described as [16]:

$$A = USV^T, \tag{6}$$

where U and V are orthogonal matrices, $S = diag\,(\sigma_1, \sigma_2, \cdots, \sigma_r, 0, \cdots, 0)$ is the singular value matrix, $\sigma_i = \sqrt{\lambda_i}(i = 1, 2, \cdots, r)$, and r is the rank of A.

SVD plays an important role in image transformation, especially in digital watermarking technology. The singular value of the matrix characterizes the distribution characteristics of the matrix data and has good stability, the slight change of the singular value will not affect the visual effect of the image [34]. In addition, the SVD has no limitation on the size of the image matrix.

2.5 Particle swarm optimization (PSO)

The PSO finds the optimal solution by iterating the random solution, which is suitable for optimization in dynamic and multi-objective optimization environment. In the PSO, the solution of each optimization problem is initialized into a group of random particles [3], then all particles are searched in the D-dimensional space, and the fitness function is used to evaluate the current position. During the process, the particles update their speed based on their own flying experience and companion's flying experience [33].

Assuming that there are m particles in the D-dimensional space, the position and velocity of the $\mathrm{i-th}$ particles can be expressed as $x_i = (x_{i1}, x_{i2}, ..., x_{iD})$ and $v_i = (v_{i1}, v_{i2}, ..., v_{iD})$, $1 \leq i \leq m$, $1 \leq d \leq D$. The individual extremum searched by the $\mathrm{i-th}$ particle and the global extremum searched by the entire particle swarm are $p_i = (p_{i1}, p_{i2}, ..., p_{iD})$ and $p_{gbest} = (p_{g1}, p_{g2}, ..., p_{gD})$, respectively. The formula for updating the speed and position of each particle is given below [19].

The d-dimensional velocity and position update formulas of particle i can be written as:

$$v_{id}^{k+1} = \omega(k)^* v_{id}^k + c_1 r_1 \left(p_{id}^k - x_{id}^k\right) + c_2 r_2 \left(p_{gd}^k - x_{id}^k\right), \tag{7}$$

$$x_{id}^{k+1} = x_{id}^k + v_{id}^{k+1}, \tag{8}$$

where v_{id}^k and x_{id}^k represent the d-dimensional component of the flying velocity and position vector of the $\mathrm{k-th}$ iteration particle i; c_1, c_2 are learning factors; r_1, r_2 are random numbers between 0 and 1 to increase search randomness; w is inertia weight [28].

3 Proposed scheme

This part mainly shows the proposed algorithm. Section 3.1 describes the embedding steps of the algorithm in detail. Section 3.2 provides a detailed explanation of the specific extraction procedure, then the optimization process of the embedding coefficient matrices is given in Section 3.3.

3.1 Watermark embedding algorithm

In the embedding algorithm, the gray watermark is embedded into the gray host image. Firstly, GAT is used to encrypt the watermark image, and the embedding process is performed in the hybrid domain. Then the host image and the watermark image are processed by DCT and multi-level DWT, and the singular values of the watermark image are embedded into the singular values of the low-frequency and high-frequency in the mixed domain of the host image, in which the embedding factor matrix is optimized by PSO to obtain the adaptive values. The specific steps of the embedding process are given below, and shown more intuitively in Fig. 1.

Step1: First, DCT is performed on the original host image, then the three-level DWT is applied to get the third-level sub-bands LL_3, HL_3, LH_3, HH_3.

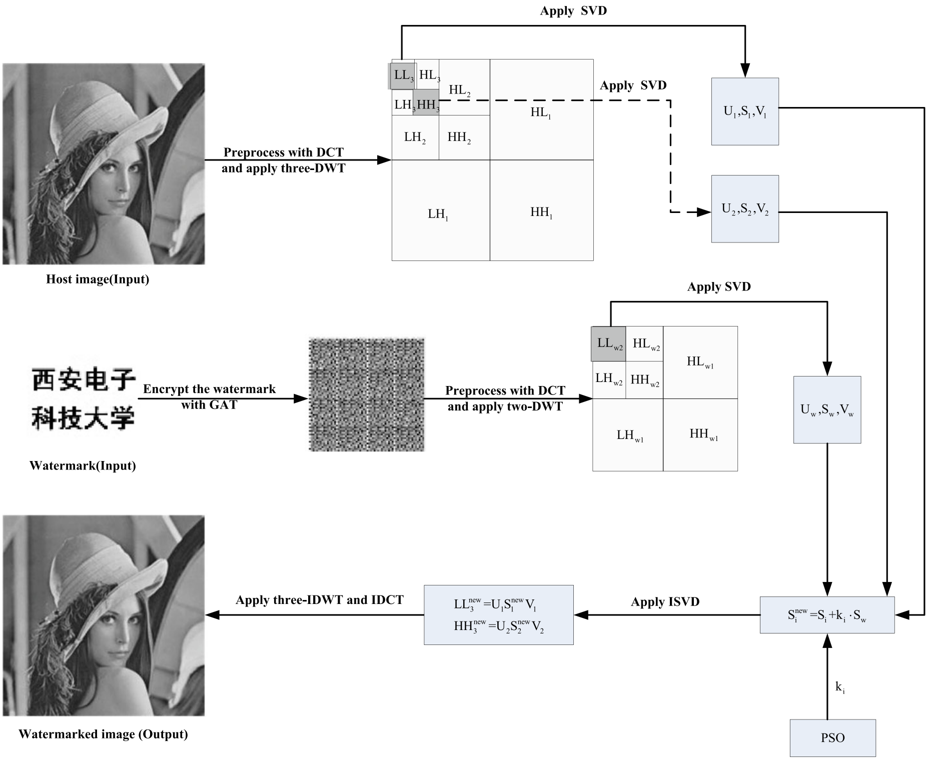

Fig. 1 Watermark embedding process

Step2: The watermark image is encrypted with GAT, and the second-level sub-bands LLw_2, HLw_2, LHw_2, HHw_2 are obtained by using DCT and two-level DWT to the encrypted watermark image.

Step3: SVD is performed on the selected sub-bands LL_3, HH_3 and LLw_2 to obtain the singular value arrays S_1, S_2 and S_w, respectively, and the left and right singular vectors are saved.

$$LL_3 = U_1 S_1 V_1^T, HH_3 = U_2 S_2 V_2^T, LL_{w2} = U_w S_w V_w^T. \tag{9}$$

Step4: The S_w of the watermark image is embedded into the S_1 and S_2 of the host image respectively, then the double embedding of the watermark is realized by the additive criterion. In addition, the embedding factor matrices are optimized by the PSO.

$$S_i^w = S_i + k_i \cdot S_w, i = 1, 2, \tag{10}$$

where (·) represents the dot multiplication operator and k_i is the matrix form.

Step5: The inverse SVD is carried out on the modified low-frequency and high-frequency singular value matrices. Combined with other wavelet sub-bands, the three-level inverse DWT is used to get the image containing watermark information.

Step6: Finally, the image generated in Step5 is processed by inverse DCT, and the watermarked image is obtained.

The embedding factor matrices k_i, the singular value matrices S_1, S_2 of the host image, the left and right singular vectors of the watermark image and the other six sub-bands of the DWT, the parameters a, b and s of the GAT are all saved as keys for watermark extraction.

3.2 Watermark extraction algorithm

Extraction is the inverse of the embedding process. Next, a detailed extraction procedure is given, and the algorithm flow chart is shown in Fig. 2.

Step1: DCT is applied to the watermarked image that may be attacked, then the three-level DWT is used to obtain LL_{31}, HL_{31}, LH_{31}, HH_{31}.

Step2: Like the embedding algorithm, LL_{31} and HH_{31} are selected for further SVD to get two singular value matrices SI_1, SI_2.

Step3: Based on the saved keys, the singular value matrix of the watermark image is extracted from SI_1 and SI_2, and inverse SVD is performed. Then, the encrypted watermark image is extracted by using two-level inverse DWT and IDCT.

$$S_{wi}^{ext} = (SI_i - S_i)./k_i, i = 1, 2, \tag{11}$$

where (·/) is the dot division operator.

Step4: The watermark images obtained in Step3 is decrypted by GAT to obtain two watermark images, and the normalized correlation coefficient between the extracted watermark and the original watermark is calculated. Finally, the watermark with a larger NC value is taken as the final watermark.

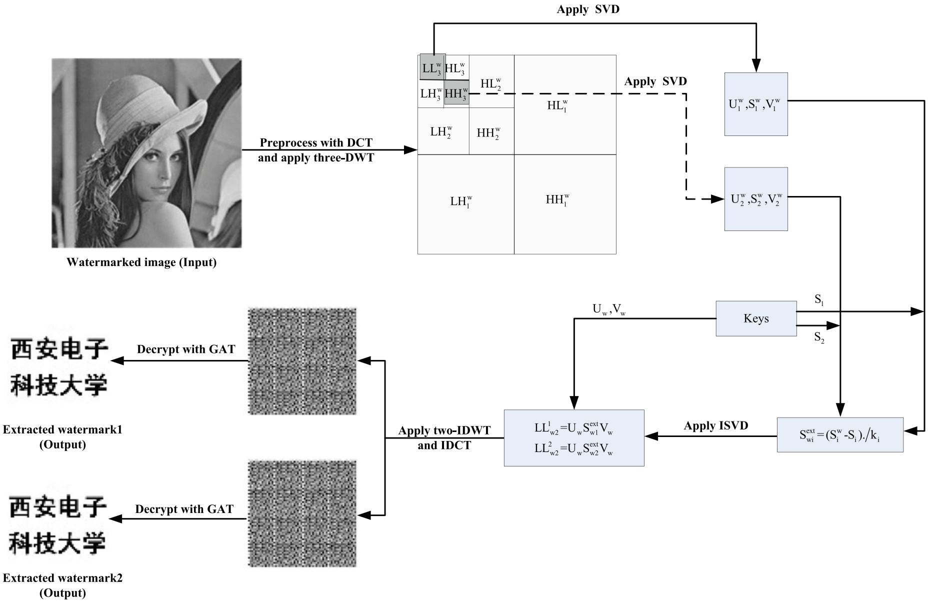

Fig. 2 Watermark extraction process

3.3 Determination of the embedding factor matrices

In this paper, the fitness function used to evaluate the particle position is defined as:

$$fitness = -\frac{\left(PSNR + \sum_{i=1}^{n} NC_i\right)}{n}, \tag{12}$$

where PSNR represents the peak signal-to-noise ratio between the watermarked image and the original image, and NC_i represents the correlation coefficient between the watermark which are extracted from the watermarked image subjected to the i − th attack and the original watermark image. n represents the total number of different attacks that performed on the watermarked image in the process of optimizing the embedding factor with PSO. At each iteration, when the watermark is embedded in the original image, the PSNR value is calculated; and the robustness of the watermarked image is tested with common attacks, the *NC* value is calculated.

Based on the formula (12) as fitness function, the PSO is used to obtain the optimal embedding coefficient matrices. In the PSO optimization process, the number of particles *m*, inertia weight *w*, maximum number of iterations *T*, and learning factors c_1, c_2 are set to the values shown in Table 1. Moreover, Eq. (13) gives the initial values of the low-frequency and high-frequency embedding factors.

$$k_1 = \begin{bmatrix} 0.01 & & & & \\ & 0.01 & & & \\ & & \ddots & & \\ & & & 0.01 & \\ & & & & 0.01 \end{bmatrix}, k_2 = \begin{bmatrix} 0.005 & & & & \\ & 0.005 & & & \\ & & \ddots & & \\ & & & 0.005 & \\ & & & & 0.005 \end{bmatrix}. \tag{13}$$

Table 1 Parameter settings for optimizing the embedding factors with PSO

Parameter	m	w	T	c_1	c_2
Value	50	0.7	100	2	2

4 Experimental results and analysis

This paper simulates on Matlab R2014a under Windows10 system. In this paper, we use two types of images as host images, namely normal image and medical image. The logo, medical image and normal image are taken as watermark images. The test images are shown in Fig. 3. The original host image is 512*512, and the watermark image is 128*128. Then the peak signal-to-noise ratio (PSNR) and normalized correlation coefficient (NC) are introduced to evaluate the algorithm [26]. The PSNR is used to measure the quality of the watermarked image, and NC is used to evaluate the quality of the extracted watermark image. The PSNR between the two images is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right), \tag{14}$$

where

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(I(i,j)-I_w(i,j)\right)^2. \tag{15}$$

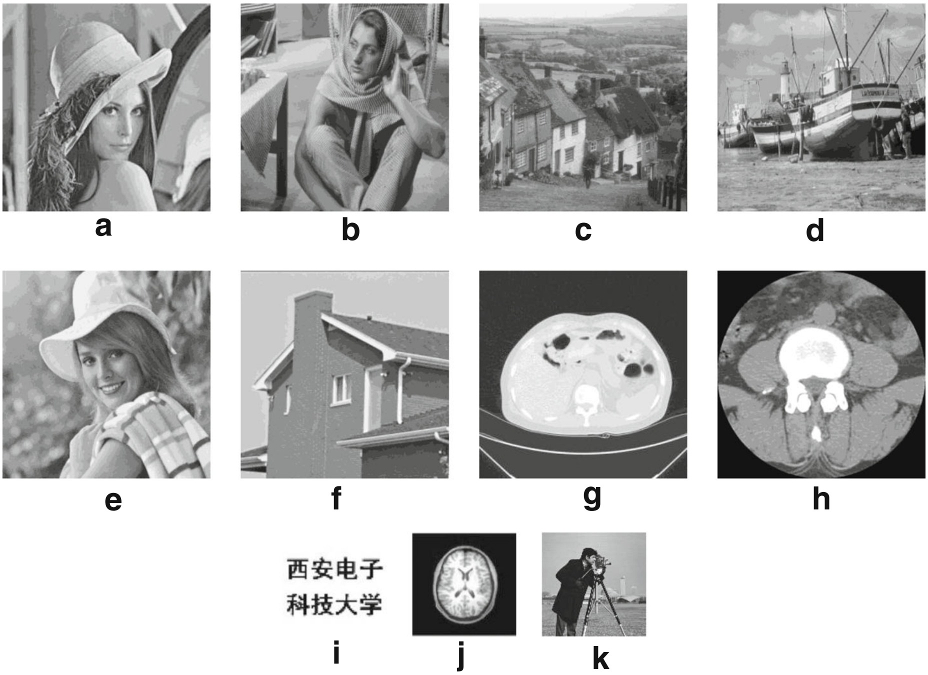

Fig. 3 Original host image and watermark image. a-h: Host image: Lena, Barbara, Goldhill, Boat, Girl, House, CT, MRI. i-k: Watermark image: Logo (W1), Brain (W2), Cameraman (W3)

The NC of the two images can be written as:

$$NC = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W(i,j)W_r(i,j)}{\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W^2(i,j)}\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W_r^2(i,j)}}. \tag{16}$$

This section mainly analyses the performance of the proposed algorithm, and evaluates the algorithm from four aspects: invisibility, security, robustness and capacity, then compares it with the related algorithms. Section 4.1 verifies the proposed scheme based on different host images and watermark images. Our scheme is compared with the existing algorithms based on the above mentioned aspects, and the results are given in Section 4.2. The host images and watermark images used in this part are shown in Fig. 3.

4.1 Algorithm performance analysis

4.1.1 Invisibility analysis

This part discusses the transparency of the proposed algorithm and measures the invisibility by the PSNR. First, the watermark images are embedded into different host images according to the embedding algorithm in Section 3.1, and the corresponding PSNR is calculated. The results are given in Table 2. The PSNR is an objective criterion for measuring image distortion. When the PSNR between the two images are larger, the more similar they are. The general benchmark is 30 dB, and the image degradation with PSNR below 30 dB is more obvious. In general, when PSNR is greater than 30 dB, the image quality is good, and the human eye cannot effectively detect the changes in the image. Therefore, the watermarking algorithm is invisible at this time. As shown in Table 2, the PSNR between the watermarked image and the original host image is about 45 dB in each case, which indicates that the algorithm has better invisibility. Because we use different types of test images and watermark images, the conclusion is universal. From the results, we can see that the proposed scheme can meet the invisibility requirement of the watermarking algorithm.

4.1.2 Security analysis

The encryption algorithm in this paper has three keys. In order to verify the security of the proposed algorithm, we assume that only one of the keys is incorrect at a time, and the other two are correct. Then we extract the watermark from the watermarked image according to the extraction algorithm in Section 3.2. This part takes the Lena watermarked image that embeds watermark W1 as an example, and the result is shown in Fig. 4. In the process of watermark extraction, when the first and second parameters of the GAT are respectively incorrect, the extracted watermarks are shown in

Table 2 The PSNR value of the proposed algorithm based on different images

Watermark	Lena	Barbara	Goldhill	Boat	Girl	House	CT	MRI
W1	44.5125	44.5182	43.9023	44.3900	44.2394	44.3835	46.9532	46.2999
W2	48.9906	46.9183	47.7360	48.1480	47.0857	46.9267	47.7372	47.3925
W3	45.2629	44.8512	44.5604	44.6076	44.4504	44.6136	44.4375	44.6074

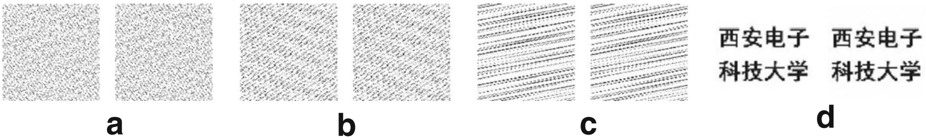

Fig. 4 Security analysis of the proposed algorithm

Fig. 4a,b. If the wrong number of scrambling is used, the extracted watermark is given in Fig. 4c. And Fig. 4d gives the extracted watermark using the correct keys. Obviously, when more than one key is incorrect, the extracted watermark will be even worse. From Fig. 4, it can be concluded that the algorithm proposed in this paper is secure. The correct and recognizable watermark can be extracted only when all keys are correct, otherwise, the extracted image is a noise-like image. This shows that the proposed scheme has high security.

4.1.3 Robustness analysis

In this section, we test the robustness of the proposed method by applying various attacks to the watermarked image. Different attacks are applied to the watermarked images embedded with different watermarks, then the watermarks are extracted from them. The NC between the extracted watermark and the original watermark is obtained, and the NC values are shown in Tables 3 and 4. If the NC is closer to 1, the algorithm has stronger ability to resist such attacks. Otherwise, the robustness is weak. It can be seen from Tables 3 and 4 that the algorithm shows strong robustness in most attacks by testing different images. Especially in JPEG compression and various cropping attacks, the algorithm shows greater resistance. Although the NC value of the extracted watermark is not very high when the image is sharpened, it can still be recognized. There are some differences in robustness between different images, but in general, our algorithm has good robustness. In addition, Fig. 5 shows the Lena watermarked image that was attacked and the watermark extracted from it. As can be seen from Fig. 5, even if the image has been severely degraded, a clear watermark can be extracted from it. According to the above analysis, our algorithm achieves the robustness requirement of the watermarking, and the clear and recognizable watermark can be extracted in most attacks.

4.1.4 Capacity analysis

For the 512*512 host image, the size of the third-level sub-band is 64*64 after three-level DWT, and the watermark image is embedded in the third-level sub-band of the host image. In the embedding process, the two-level DWT is used for the watermark image, so the maximum embeddable watermark size is 256*256. The capacity of the watermarking algorithm is measured by the ratio of the number of pixels of the watermark to the number of pixels in the host image. Therefore, the capacity of our algorithm is (256*256)/(512*512) = 0.25, which indicates that the scheme has high capacity.

4.2 Comparative analysis

In this part, we use Lena as the host image and W1 as the watermark image, and compare the algorithm in this paper with the existing schemes [8, 13, 20, 26, 41, 47] according to the four characteristics of the watermarking algorithm.

Table 3 NC values of the watermark extracted from watermarked image under various attacks

Attack	Lena			Barbara			Goldhill			Boat		
	W1	W2	W3	W1	W2	W3	W1	W2	W3	W1	W2	W3
No attack	1	1	1	1	1	1	1	1	1	1	1	1
JPEG compression (QF = 10)	0.9997	0.9987	0.9997	0.9996	0.9987	0.9991	0.9991	0.9980	0.9986	0.9988	0.9954	0.9972
Rotate 45 degrees	0.9805	0.9932	0.9852	0.9707	0.9802	0.9737	0.9988	0.9835	0.9937	0.9798	0.9968	0.9846
Gaussian low pass filter 9*9	0.9998	0.9996	0.9997	0.9988	0.9983	0.9984	0.9994	0.9984	0.9988	0.9993	0.9981	0.9987
Crop 1/4 in the lower right corner	0.9968	0.9988	0.9991	0.9981	0.9989	0.9942	0.9987	0.9981	0.9968	0.9969	0.9978	0.9982
Rescaling (0.125,8)	0.9976	0.9897	0.9951	0.9964	0.9869	0.9932	0.9969	0.9877	0.9933	0.9970	0.9872	0.9939
Sharpen	0.9617	0.9432	0.9527	0.9566	0.9456	0.9458	0.9453	0.9488	0.9511	0.9501	0.9531	0.9542
Gamma correction 0.9	0.9898	0.9511	0.9818	0.9890	0.9777	0.9841	0.9974	0.9906	0.9925	0.9863	0.9638	0.9776
Speckle noise 0.01	0.9782	0.9591	0.9739	0.9955	0.9821	0.9873	0.9769	0.9660	0.9889	0.9871	0.9646	0.9777
Median filtering 9*9	0.9980	0.9978	0.9966	0.9930	0.9884	0.9937	0.9974	0.9970	0.9937	0.9982	0.9929	0.9963
Average filtering 9*9	0.9969	0.9865	0.9942	0.9929	0.9869	0.9932	0.9940	0.9833	0.9927	0.9907	0.9852	0.9919
Rectangular cropping (50 pixels per side)	0.9879	0.9975	0.9866	0.9873	0.9860	0.9819	0.9886	0.9964	0.9875	0.9935	0.9971	0.9897
Crop 1/4 in the center	0.9931	0.9967	0.9954	0.9974	0.9991	0.9997	0.9971	0.9977	0.9956	0.9974	0.9983	0.9929
Crop 1/4 in the upper left corner	0.9702	0.9757	0.9704	0.9673	0.9723	0.9677	0.9674	0.9718	0.9672	0.9683	0.9741	0.9690
Crop 1/4 in the lower left corner	0.9758	0.9906	0.9803	0.9890	0.9970	0.9957	0.9807	0.9926	0.9822	0.9725	0.9884	0.9779
Crop 1/4 in the upper right corner	0.9742	0.9894	0.9783	0.9965	0.9946	0.9899	0.9805	0.9975	0.9841	0.9790	0.9930	0.9826
Circular cropping	0.9775	0.9884	0.9816	0.9749	0.9909	0.9828	0.9964	0.9909	0.9957	0.9929	0.9875	0.9967
Randomly delete 100 rows and 100 columns	0.9812	0.9964	0.9839	0.9941	0.9961	0.9852	0.9775	0.9920	0.9790	0.9775	0.9910	0.9798
Wiener filtering 9*9	0.9981	0.9927	0.9963	0.9965	0.9889	0.9941	0.9973	0.9897	0.9942	0.9973	0.9891	0.9945
Motion blur (45, 45)	0.9969	0.9855	0.9943	0.9910	0.9839	0.9929	0.9941	0.9817	0.9925	0.9912	0.9822	0.9919
Salt & pepper noise 0.01	0.9881	0.9798	0.9742	0.9930	0.9870	0.9906	0.9879	0.9780	0.9916	0.9924	0.9793	0.9853
Gaussian noise 0.01	0.9711	0.9675	0.9685	0.9693	0.9593	0.9702	0.9551	0.9587	0.9638	0.9636	0.9616	0.9669

Host image: Lena, Barbara, Goldhill, Boat

Table 4 NC values of the watermark extracted from watermarked image under various attacks

Attack	Girl			House			CT			MRI		
	W1	W2	W3	W1	W2	W3	W1	W2	W3	W1	W2	W3
No attack	1	1	1	1	1	1	1	1	1	1	1	1
JPEG compression (QF = 10)	0.9985	0.9959	0.9966	0.9987	0.9961	0.9981	0.9989	0.9974	0.9980	0.9996	0.9993	0.9992
Rotate 45 degrees	0.9842	0.9977	0.9911	0.9874	0.9985	0.9926	0.9956	0.9917	0.9896	0.9813	0.9895	0.9901
Gaussian low pass filter 9*9	0.9991	0.9976	0.9984	0.9999	0.9998	0.9999	0.9995	0.9995	0.9996	0.9997	0.9995	0.9997
Crop 1/4 in the lower right corner	0.9963	0.9963	0.9891	0.9978	0.9978	0.9961	0.9820	0.9978	0.9869	0.9813	0.9981	0.9860
Rescaling (0.125,8)	0.9976	0.9917	0.9943	0.9974	0.9912	0.9948	0.9965	0.9900	0.9942	0.9971	0.9917	0.9954
Sharpen	0.9590	0.9543	0.9526	0.9643	0.9578	0.9558	0.9493	0.9549	0.9582	0.9588	0.9535	0.9571
Gamma correction 0.9	0.9921	0.9758	0.9794	0.9942	0.9861	0.9912	0.9605	0.9617	0.9791	0.9865	0.9904	0.9893
Speckle noise 0.01	0.9768	0.9689	0.9869	0.9769	0.9686	0.9774	0.9960	0.9977	0.9977	0.9974	0.9980	0.9983
Median filtering 9*9	0.9982	0.9972	0.9956	0.9985	0.9981	0.9972	0.9974	0.9912	0.9958	0.9978	0.9935	0.9963
Average filtering 9*9	0.9929	0.9880	0.9938	0.9970	0.9884	0.9946	0.9966	0.9876	0.9940	0.9970	0.9907	0.9949
Rectangular cropping (50 pixels per side)	0.9963	0.9964	0.9912	0.9890	0.9942	0.9823	0.9954	0.9956	0.9970	0.9874	0.9971	0.9951
Crop 1/4 in the center	0.9927	0.9965	0.9852	0.9927	0.9965	0.9977	0.9940	0.9952	0.9964	0.9957	0.9947	0.9916
Crop 1/4 in the upper left corner	0.9675	0.9719	0.9671	0.9678	0.9728	0.9681	0.9685	0.9733	0.9687	0.9678	0.9727	0.9680
Crop 1/4 in the lower left corner	0.9771	0.9949	0.9819	0.9730	0.9905	0.9787	0.9703	0.9844	0.9745	0.9745	0.9900	0.9791
Crop 1/4 in the upper right corner	0.9806	0.9961	0.9855	0.9818	0.9949	0.9834	0.9979	0.9983	0.9991	0.9980	0.9925	0.9918
Circular cropping	0.9845	0.9964	0.9874	0.9772	0.9817	0.9845	0.9851	0.9956	0.9837	0.9945	0.9975	0.9962
Randomly delete 100 rows and 100 columns	0.9851	0.9907	0.9821	0.9923	0.9930	0.9854	0.9934	0.9916	0.9922	0.9948	0.9911	0.9915
Wiener filtering 9*9	0.9980	0.9938	0.9953	0.9983	0.9950	0.9968	0.9978	0.9940	0.9967	0.9977	0.9942	0.9966
Motion blur (45, 45)	0.9929	0.9825	0.9926	0.9970	0.9855	0.9943	0.9966	0.9848	0.9940	0.9873	0.9862	0.9877
Salt & pepper noise 0.01	0.9905	0.9812	0.9913	0.9865	0.9739	0.9780	0.9845	0.9869	0.9872	0.9867	0.9888	0.9866
Gaussian noise 0.01	0.9603	0.9640	0.9565	0.9655	0.9656	0.9635	0.9673	0.9578	0.9556	0.9674	0.9631	0.9560

Host image: Girl, House, CT, MRI

Attack type	Damaged watermarked image	Extracted watermark	Attack type	Damaged watermarked image	Extracted watermark
No attack		西安电子 科技大学 NC=1	Rectangular cropping (50 pixels per side)		西安电子 科技大学 NC=0.9879
JPEG compression (QF=10)		西安电子 科技大学 NC=0.9997	Crop 1/4 in the center		西安电子 科技大学 NC=0.9931
Rotate 45 degrees		西安电子 科技大学 NC=0.9805	Crop 1/4 in the upper left corner		西安电子 科技大学 NC=0.9702
Gaussian low pass filter 9*9		西安电子 科技大学 NC=0.9998	Crop 1/4 in the lower left corner		西安电子 科技大学 NC=0.9758
Crop 1/4 in the lower right corner		西安电子 科技大学 NC=0.9968	Crop 1/4 in the upper right corner		西安电子 科技大学 NC=0.9742
Rescaling (0.125,8)		西安电子 科技大学 NC=0.9976	Circular cropping		西安电子 科技大学 NC=0.9775
Sharpen		西安电子 科技大学 NC=0.9617	Randomly delete 100 rows and 100 columns		西安电子 科技大学 NC=0.9812
Gamma correction 0.9		西安电子 科技大学 NC=0.9898	Wiener filtering 9*9		西安电子 科技大学 NC=0.9981
Speckle noise 0.01		西安电子 科技大学 NC=0.9782	Motion blur (45, 45)		西安电子 科技大学 NC=0.9969
Median filtering 9*9		西安电子 科技大学 NC=0.9980	Salt & pepper noise 0.01		西安电子 科技大学 NC=0.9881
Average filtering 9*9		西安电子 科技大学 NC=0.9969	Gaussian noise 0.01		西安电子 科技大学 NC=0.9711

Fig. 5 Degraded Lena watermarked image and the extracted watermark

4.2.1 Invisibility comparison

The watermark W1 is embedded into the Lena image by the algorithm [8, 13, 20, 26, 41, 47] and the proposed scheme, respectively, and the corresponding watermarked image is obtained. The PSNR between the watermarked image and the original host image is calculated, and the result is given in Table 5. It can be concluded from Table 5 that the PSNR of the proposed algorithm is slightly different from that of [26], but it is higher than Furqan et al. [8], Hurrah et al. [13], Zear et al. [47], Singh et al. [41] and Liu et al. [20]. This indicates that our algorithm has advantages in terms of transparency.

4.2.2 Security comparison

Furqan et al. [8] directly applied SVD to the watermark image, which not only has low security, but also has the FPP. Because the singular value of the watermark image was embedded in the singular value of the host image. Like Furqan et al. [8], Nandi et al. [26] directly performed SVD on the watermark image, so it has the same security problems as Furqan et al. [8]. Moreover, Singh et al. [41] used DCT to process the watermark image before SVD, but still did not encrypt the watermark, and embedded the singular value of the watermark into the singular value of the host image, there are the same security problems as [8, 26]. Zear et al. [47] encrypted the watermark with the commonly used narrow Arnold transform before applying DCT and SVD on it, so there was no FPP in this algorithm. In this case, the encryption algorithm has only one key, namely the number of scrambling, so the security of the algorithm is low. In the scheme presented by Liu et al. [20], the watermark image was first encrypted by logistic mapping. Then, the parameter pairs $x(0)$ and u were further encrypted by RSA to obtain ciphertext, which enhanced the security of the watermark. Because the watermark image was encrypted before the use of the SVD, this algorithm avoids the FPP. Hurrah et al. [13] first encrypted the binary watermark image with the Arnold transform, then encrypted the obtained image again with 32-bit key. There is no FPP in this algorithm.

In this paper, we use the GAT to encrypt the watermark image, the encryption algorithm has three keys: parameters a, b and scrambling times s. The security of this algorithm is analyzed in Section 4.1.2, it can be found that only one key is not correct, it is impossible to recover the distinguishable watermark.

4.2.3 Robust contrast

In this part, the proposed algorithm is compared with the existing algorithms based on robustness. The watermark W1 is embedded into the Lena image according to the schemes [8, 13, 20, 26, 41, 47] and our algorithm, respectively. Then these Lena watermarked images are subjected to different degradation processing. Finally, the watermarks are extracted from them, and the corresponding NC values are given in Table 6. As shown in Table 6, under all 21 attacks, there are six cases in which no meaningful watermark can be extracted from the scheme [26], four cases in scheme [47], two cases

Table 5 Transparency comparison of the algorithms based on PSNR value

Scheme metrics	Furqan et al. [8]	Nandi et al. [26]	Hurrah et al. [13]	Zear et al. [47]	Singh et al. [41]	Liu et al. [20]	Proposed method
PSNR (dB)	32.9505	44.8564	40.12	38.7100	34.9145	42.4657	44.5125

Table 6 Robustness comparison of different algorithms based on NC values

Attack type	Furqan et al. [8]	Nandi et al. [26]	Hurrah et al. [13]	Zear et al. [47]	Singh et al. [41]	Liu et al. [20]	Proposed scheme
No attack	1	1	1	0.9921	1	0.9994	1
JPEG compression (QF = 10)	0.9911	0.9981	0.9993	–	0.9937	0.9547	0.9997
Rotate 45 degrees	0.7530	0.9813	0.9580	0.3911	0.9815	0.8688	0.9805
Gaussian low pass filter 9*9	0.9954	0.9991	0.9996	0.9943	0.9958	0.9845	0.9998
Crop 1/4 in the lower right corner	0.8867	–	0.9789	0.9676	0.9785	0.8853	0.9968
Rescaling (0.125,8)	0.5649	0.9153	0.9124	0.0724	0.9245	0.8596	0.9976
Sharpen	0.8781	0.9126	0.9712	0.9912	0.8661	–	0.9617
Gamma correction 0.9	0.9862	0.9551	0.9632	0.9999	–	0.9850	0.9898
Speckle noise 0.01	0.8938	0.9734	0.9587	0.9755	0.9355	0.8989	0.9782
Median filtering 9*9	0.7875	0.9576	0.9650	0.0692	0.9453	0.8542	0.9980
Average filtering 9*9	0.5188	0.9016	0.9588	0.0799	0.8926	0.7859	0.9969
Rectangular cropping (50 pixels on each side)	0.6861	–	0.9695	0.8444	0.9803	0.9121	0.9879
Crop 1/4 in the center	0.8637	–	0.9387	–	0.9732	0.8884	0.9931
Crop 1/4 in the upper left corner	0.6809	0.9666	0.9823	0.9805	0.9684	0.9603	0.9702
Crop 1/4 in the lower left corner	–	0.9499	0.9760	0.8499	0.9776	0.9071	0.9758
Crop 1/4 in the upper right corner	0.4652	–	0.9652	–	0.9746	0.9017	0.9742
Circular cropping	0.6947	0.9813	0.9133	0.8478	0.9829	0.8742	0.9775
Randomly delete 100 rows and 100 columns	0.9978	–	0.8866	–	0.9797	0.8802	0.9812
Wiener filtering 9*9	0.8717	0.9715	0.9785	0.8819	0.9610	0.9394	0.9981
Motion blur (45, 45)	–	–	0.8964	0.0822	0.8731	0.8564	0.9969
Salt & pepper noise 0.01	0.8938	0.9694	0.9453	0.9748	0.9317	0.9324	0.9881
Gaussian noise 0.01	0.6757	0.9149	0.8927	0.9626	0.8585	0.8619	0.9711

in scheme [8], and one case in scheme [41] and [20]. However, our proposed scheme and scheme [13] can extract meaningful and identifiable watermark in each case. [13] is weaker under the attacks of rotation, scaling, median filtering, and average filtering. The robustness of [20] is not very good, especially in rotation, scaling, average filtering, center cropping, etc. [41] has poor performance in motion blur, average filtering and sharpening, and NC is less than 0.9. When the watermarked image is corrected with a gamma value of 0.9, a meaningless watermark can be extracted. Although [47] has slight advantages in sharpening and gamma correction, it cannot extract the effective watermark under four attacks: JPEG compression with factor 10, center cropping, right-upper corner cropping and random deletion. Moreover, when the watermarked image is subjected to 45 degree rotation, scaling, median filtering and average filtering, etc., the extracted watermark has an NC value lower than 0.4. In six cases, such as rectangle cropping, center cropping and random deletion and so on, the watermark extracted in [26] is invalid, but in the other 15 cases, the NC is greater than 0.9. In the eight cases of rotation, scaling, median filtering and rectangular cropping, etc., the NC of the watermark extracted by [8] is very low, with a minimum of 0.46. And this algorithm cannot provide copyright protection when the watermarked image suffers from the lower left corner cropping and motion blur.

Compared with the existing algorithms, the proposed algorithm has obvious advantages in JPEG compression, scaling, cropping, Gaussian filtering, median filtering, average filtering and wiener filtering. Because embedding the watermark information in DCT domain can effectively resist lossy compression, filtering and other image processing attacks. Moreover, if the watermark is embedded in the low frequency of the DWT domain, the algorithm is robust to blur attack, rescaling, and JPEG compression, while embedding the watermark in the high frequency region is robust to attacks such as noise and cropping. In addition, the robustness of high-level region in DWT domain is higher than that of low-level region. In this paper, the DCT and multi-level DWT are combined to process the host image and the watermark image, and the low-frequency and high-frequency regions are selected for embedding the watermark, which improves the robustness of the algorithm. In addition, the embedding factor matrix is used to replace the embedding factor, and PSO is used to optimize the matrix, which also contributes a lot to the robustness of the algorithm.

4.2.4 Capacity comparison

For the 512*512 host image, Furqan et al. [8] used one-level DWT, then applied SVD directly to the watermark image, and embedded the singular value of the watermark into the singular value of the four first-level sub-bands of the host image. Therefore, the capacity is 0.25. Unlike Furqan et al. [8], Nandi et al. [26] only embedded the watermark into the first-level low-frequency sub-band of the host image, and the capacity is 0.25 as in Furqan et al. [8]. In Singh et al. [41], one-level DWT was applied to the host image, and the low-frequency sub-band was taken to further perform DCT, then the DCT was directly applied to the watermark image. Finally, the singular value of the watermark was embedded into the singular value of the host image, and the capacity is also 0.25. In the scheme presented by Zear et al. [47], three-level DWT was applied to the 512*512 host image. The size of the first-level sub-band was 256*256, they chose the medium sub-band LH_1 for watermark embedding, and directly performed DCT on the encrypted watermark image, so the capacity of their algorithm is 0.25. In Liu et al. [20], the one-level DWT was applied to 512*512 host image, and the size of the first-level sub-band was 256*256. The encrypted watermark was directly added to the singular value of the first-level low-frequency sub-band, so the capacity of this algorithm is (256*256)/(512*512) = 0.25. Hurrah et al. [13] performed one-level DWT on 512*512 gray image,

Table 7 Comparison of the watermark capacity between the proposed scheme and the existing algorithms

Scheme	Furqan et al. [8]	Nandi et al. [26]	Hurrah et al. [13]	Zear et al. [47]	Singh et al. [41]	Liu et al. [20]	Proposed method
Capacity	0.25	0.25	0.015625	0.25	0.25	0.25	0.25

then decomposed the low frequency sub-band LL into 32*32 non-overlapping 8*8 blocks, and further divided each 8*8 block into four 4*4 sub-blocks. Therefore, the maximum embeddable watermark bit is 32*32*4 = 64*64, the algorithm's capacity is (64*64)/(512*512) = 0.015625.

The capacity comparison results are shown in Table 7. As shown in Section 4.1.4, the capacity of our algorithm is 0.25. Based on the above analysis and Table 7, we can see that other related algorithms other than [13] have the same capacity as the proposed algorithm. However, the capacity of [13] is about 0.015, and our algorithm is 16 times larger.

5 Conclusions

In this paper, a dual-embedded hybrid domain image watermarking algorithm based on PSO is proposed. Combining the DCT with DWT, the encrypted watermark and host images are processed by DCT, and the DCT coefficients are decomposed by multi-level wavelet transform. The watermark image is encrypted by the GAT, and the added keys improves the security of the algorithm. Moreover, embedding the watermark in high frequency and low frequency enhances the robustness of the algorithm against attacks. In addition, compared with a single embedding factor, the embedding matrices has more advantages and contributes greatly to the improvement of robustness. Furthermore, the optimization with PSO better balances the relationship between robustness and invisibility. Experiments show that the proposed algorithm satisfies the requirements of robust watermarking in four aspects: invisibility, security, robustness and capacity. Compared with the existing related watermarking algorithms, the proposed algorithm has good invisibility and security, and shows advantages in robustness. The robustness of this algorithm is improved under the condition of meeting the invisibility and security requirements.

There are four main research directions in the future: (1) The algorithm can be extended for the copyright protection of color image, as well as audio and video. (2) Our second consideration is to enhance the security of the watermarking algorithm. A more secure encryption scheme can be designed by combining GAT with other methods. (3) In order to increase the watermark capacity of the algorithm, the host image can be processed with redundant wavelet transform. (4) The singular values of the host image and the watermark image can be obtained by the block SVD, which can improve the robustness of the watermarking algorithm.

Acknowledgments This work was supported in part by the National Natural Science Foundation of China under Grant 11601406, the Natural Science Foundation of Shaanxi Province under Grants 2018JM6044 and 2018JQ1024.

References

1. Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik 125:428–434

2. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans Image Process 10(5):783–791
3. Beheshti Z, Shamsuddin SM (2015) Non-parametric particle swarm optimization for global optimization. Appl Soft Comput 28:345–359
4. Bekkouch S, Faraoun KM (2015) Robust and reversible image watermarking scheme using combined DCT-DWT-SVD transforms. J Inf Process Syst 11:406–420
5. Benoraira A, Benmahammed K, Boucenna N (2015) Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP J Adv Sig Pr 2015:55
6. Divecha N, Jani NN (2013) Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images. 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)
7. Fazli S, Moeini M (2016) A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik 127:964–972
8. Furqan A, Kumar M (2015) Study and analysis of robust DWT-SVD domain based digital image watermarking technique using MATLAB. 2015 IEEE International Conference on Computational Intelligence & Communication Technology
9. Hafed ZM, Levine MD (2001) Face recognition using the discrete cosine transform. Int J Comput Vis 43: 167–188
10. Handito KW, Fauzi Z, Ma'ruf FA (2018) The comparison between SVD-DCT and SVD-DWT digital image watermarking. International Conference on Data and Information Science. IOP Conf. Series: Journal of Physics: Conf. Series 971
11. Harjito B, Suryani E (2017) Robust image watermarking using DWT and SVD for copyright protection. AIP Conf Proc 1813. https://doi.org/10.1063/1.4975968
12. Hu H-T, Hsu L-Y (2017) Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. Multimed Tools Appl 76(5):6575–6594
13. Hurrah NN, Parah SA, Loan NA, Sheikh JA, Elhoseny M, Muhammad K (2019) Dual watermarking framework for privacy protection and content authentication of multimedia. Futur Gener Comput Syst 94: 654–673
14. Jane O, Elbaşi E, Ilk HG (2014) Hybrid non-blind watermarking based on DWT and SVD. J Appl Res Technol 12:750–761
15. Jing P, Su Y, Nie L, Bai X, Liu J, Wang M (2018) Low-rank multi-view embedding learning for micro-video popularity prediction. IEEE Trans Knowl Data Eng 30(8):1519–1532
16. Joseph A, Anusudha K (2013) Robust watermarking based on DWT SVD. International Journal of Signal & Image Processing 1(1)
17. Kasana G, Kasana SS (2017) Reference based semi blind image watermarking scheme in wavelet domain. Optik 142:191–204
18. Kaur R, Singh H (2015) An improved performance of watermarking in DWT domain using SVD. Int J Latest Trends Eng Technol (IJLTET) 5:459–465
19. Li C, Yang S, Nguyen TT (2012) A self-learning particle swarm optimizer for global optimization problems. IEEE T Syst Man Cy B 42:627–646
20. Liu Y, Tang S, Liu R, Zhang L, Ma Z (2018) Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Syst Appl 97:95–105
21. Liu M, Nie L, Wang X, Tian Q, Chen B (2019) Online data organizer: micro-video categorization by structure-guided multimodal dictionary learning. IEEE Trans Image Process 28(3):1235–1247
22. Maloo S, Lakshmi N, Pareek NK (2017) Study of digital watermarking techniques for against security attacks. In: Satapathy S, Joshi A (eds) Information and communication Technology for Intelligent Systems (ICTIS 2017) - volume 1. ICTIS 2017, Smart innovation, systems and technologies, vol 83. Springer, Cham, pp 509–515
23. Mehto A, Mehra N (2016) Adaptive lossless medical image watermarking algorithm based on DCT & DWT. Procedia Comput Sci 78:88–94
24. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm. Expert Syst Appl 41:7858–7867
25. Muthumanickam S, Arun C (2018) An efficient blind detection watermarking algorithm using range conversion method. Microsyst Technol 24:1565–1575
26. Nandi S, Santhi V (2016) DWT–SVD-based watermarking scheme using optimization technique. In: Dash S, Bhaskar M, Panigrahi B, Das S (eds) Artificial intelligence and evolutionary computations in engineering systems, Advances in intelligent systems and computing, vol 394. Springer, New Delhi, pp 69–77
27. Nayak DR, Dash R, Majhi B (2016) Brain MR image classification using two-dimensional discrete wavelet transform and AdaBoost with random forests. Neurocomputing 177:188–197

28. Nayak DR, Dash R, Majhi B (2018) Discrete ripplet-II transform and modified PSO based improved evolutionary extreme learning machine for pathological brain detection. Neurocomputing 282:232–247
29. Niu Y, Cui X, Li Q, Ding J (2016) A SVD-based color image watermark algorithm in DWT domain. Adv Graphic Commun Packag Technol Mater 369:303–309
30. Pandey P, Kumar S, Singh SK (2014) Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking. Multimed Tools Appl 72:723–748
31. Poonam, Arora SM (2018) A DWT-SVD based robust digital watermarking for digital images. Procedia Comput Sci 132:1441–1448
32. Rajpal A, Mishra A, Bala R (2019) A novel fuzzy frame selection based watermarking scheme for MPEG-4 videos using bi-directional extreme learning machine. Appl Soft Comput 74:603–620
33. Ratnaweera A, Halgamuge SK, Watson HC (2004) Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients. IEEE Trans Evol Comput 8:240–255
34. Run R-S, Horng S-J, Lai J-L, Kao T-W, Chen R-J (2012) An improved SVD-based watermarking technique for copyright protection. Expert Syst Appl 39:673–689
35. Saikrishna N, Resmipriya MG (2016) An invisible logo watermarking using Arnold transform. Procedia Comput Sci 93:808–815
36. Saxena S, Todwal V. Performance analysis of semi-blind hybrid DWT-SVD based watermarking algorithm using Daubechies wavelet. Int J Electron Comput Sci Eng (IJECSE) 4, ISSN- 2277-1956
37. Saxena P, Garg S, Srivastava A (2012) DWT-SVD semi-blind image watermarking using high frequency band. 2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April 28–29, 2012, p 138–142
38. Singh AK (2017) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed Tools Appl 76:8881–8900
39. Singh D, Singh SK (2017) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl 76:13001–13024
40. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic concepts in information security. P Natl A Sci India A 84(3):345–359
41. Singh AK, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain. Natl Acad Sci Lett 37(4):351–358
42. Wang Y, Li T (2012) Digital watermarking algorithm based on singular value decomposition and wavelet transformation. International Conference on Automatic Control and Artificial Intelligence (ACAI 2012), p 911–914
43. Wang C, Zhang Y, Zhou X (2017) Review on digital image watermarking based on singular value decomposition. J Inf Process Syst 13:1585–1601
44. Wu X, Sun W (2013) Robust copyright protection scheme for digital images using overlapping DCT and SVD. Appl Soft Comput 13:1170–1182
45. Yadav B, Kumar A, Kumar Y (2018) A robust digital image watermarking algorithm using DWT and SVD. In: Pant M, Ray K, Sharma T, Rawat S, Bandyopadhyay A (eds) Soft computing: theories and applications, Advances in intelligent systems and computing, vol 583. Springer, Singapore
46. You X, Du L, Cheung Y (2010) A blind watermarking scheme using new nontensor product wavelet filter banks. IEEE Trans Image Process 19(12):3271–3284
47. Zear A, Singh AK, Kumar P (2018) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77:4863–4882
48. Zhang Z, Wang C, Zhou X (2016) Image watermarking scheme based on Arnold transform and DWT-DCT-SVD. 2016 IEEE 13th International Conference on Signal Processing (ICSP)

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

Lina Zhang , a master's degree in mathematics and statistics from Xidian University, specializes in computational mathematics. The research direction is information security, mainly digital watermarking and image encryption. She won the second prize of the National College Student Mathematics Competition and the third prize of the National College Student Mathematical Modeling Competition.

Deyun Wei received the B.S. degree from Qufu Normal University, Qufu, China, in 2006, the M.S. degree in applied mathematics and the Ph.D. degree in Physical Electronics from Harbin Institute of Technology, Harbin, China, in 2008 and 2012. Now he is an associate professor with the School of mathematics and Statistics, Xidian University, Xi'an, China. His research interests include time-frequency analysis, image processing, sampling theory. He has over 40 refereed journal articles published. He was a recipient of the 2016 IET Signal Processing Premium Awards. He served as Editorial Board Member for Signal Processing: An International Journal (SPIJ).