Robust JPEG Steganography Using Singular Value Decomposition in DCT Domain

Xiaofeng Song[1](✉), Yi Zhang[2], and Jia Du[1]

[1] National University of Defense Technology, Xi'an 710106, China
[2] Special Police College, Beijing 102211, China

Abstract. Image steganography is an important technology for convert communication. When the stego images are transmitted through lossy network channel, the robustness of steganography algorithm is very crucial. Based on singular value decomposition in DCT domain, a robust JPEG steganography algorithm is proposed, which can resist image compression and correctly extract the embedded secret message from the compressed stego image. First, the robust embedding domain is constructed by exploiting the correlation of the maximum singular values got from two adjacent 8 × 8 DCT blocks. Then, the framework of the proposed JPEG steganography algorithm is given and the key steps are described in details. The experimental results show that the proposed JPEG steganography algorithm can achieve competitive robustness in contrast to the state-of-the-art robust steganography algorithms. Moreover, it can extract the secret messages correctly even if the stego image is compressed by WeChat.

Keywords: JPEG steganography · Robustness · DCT domain · Singular value · Correlation

1 Introduction

Digital steganography is a kind of covert communication technique that embeds secret messages in multimedia objects such as images, audio, video, text and so on [1]. It can realize the transmission of secret messages through the innocuous-looking stego objects. Due to the wide application of JPEG images on the Internet, JPEG image steganography has received extensive attentions. In recent years, many JPEG steganography algorithms have been proposed, such as Uniform embedding Distortion (UED) [2] steganography, JPEG UNIversal WAvelet Relative Distortion (J-UNIWARD) steganography [3], and so on. They usually constrain the embedding changes to the complex texture regions difficult to model and then achieve the good anti-detection ability. In other words, the primary goal of these content-adaptive steganography algorithm is the strong resistance ability to steganalysis technique. However, they are not robust to the lossy image processing such as image compression, Image resizing, etc. For example, in recent years, the instant communication tools, social platforms, and multimedia sharing websites are becoming more and more popular. These tools, platforms, and websites transmit and exchange massive amounts of digital images every day. With these massive images as cover, more

© Springer Nature Switzerland AG 2021
X. Sun et al. (Eds.): ICAIS 2021, CCIS 1424, pp. 278–290, 2021.
https://doi.org/10.1007/978-3-030-78621-2_22

secure covert communication can be achieved. However, in order to save transmission and storage costs, the images are often compressed during the process of transmission and sharing, which makes the extraction error rate of secret messages is very high when the message embedding is performed by non-robust steganography algorithms such as J-UNIWARD. Therefore, robust JPEG steganography against lossy image processing is becoming a research hotspot in field of information hiding.

For the design of robust JPEG steganographic schemes, Zhang et al. [4] constructed the robust embedding domain based on the relative relationship of inter-block DCT coefficients, and proposed a robust and adaptive JPEG steganography algorithm against JPEG compression; Qian et al. [5] proposed a robust steganography algorithm using texture synthesis, however, the extraction error rate of secret messages is relatively high; Zhang et al. [6] also proposed a JPEG compression and detection resistant steganography algorithm based on dither modulation when the quantization table of JPEG compression is assumed to be known; Zhao et al. [7] proposed a robust and adaptive JPEG image steganography algorithm based on transmission channel matching, however, the behavior of repeatedly uploading images for re-compression is very suspicious; Tao et al. [8] proposed a robust JPEG steganography by generating the "intermediate image" that is just the stego image after JPEG compression with special quality factor, however, the quality factor of JPEG compression must to be known previously; Yu et al. [9] proposed a robust image steganography algorithm based on generalized dither modulation and embedding domain expansion, which can achieve better robustness and anti-detection ability, however, the quantization table of JPEG compression is assumed to be known. Recently, Zhang et al. [10] proposed a robust steganography algorithm with multiple robustness enhancements, however, the anti-detection ability is quite weak.

In this paper, a robust JPEG steganography algorithm is proposed based on inter-block singular value correlation in DCT domain. As we know, the inter-block DCT coefficients of JPEG image have strong correlation. Moreover, the correlations are relatively stable even though some lossy processing are performed for the image. Furthermore, considering the stability of singular values [11], we construct the robust embedding domain by exploiting this correlation of the maximum singular values of the two matrixes generated using the DCT coefficients in middle frequency bands of two adjacent 8×8 DCT blocks. The binary cover elements can be got using the correlation of the maximum singular values of the generated matrixes. In addition, based on the embedding distortion function of J-UNIWARD, the embedding distortion of the proposed steganography algorithm is defined according to the embedding changes of DCT coefficients caused by modifying the maximum singular values of the generated matrixes. To reduce message extraction errors, the secret messages are encoded by Reed-Solomon (RS) error correcting code, and the encoded messages are embedded using STCs [12] which is widely used for minimal distortion steganography. Finally, the stego elements are embedded by modifying the maximum singular values of the corresponding matrixes and the stego image is generated using the modified DCT coefficients.

The rest of the paper is organized as follows: Sect. 2 introduces the construction of robust embedding domain; Section 3 proposes a robust JPEG steganography algorithm and the implementation details are described in details; Section 4 verifies the effectiveness of the proposed steganography algorithm by comparing it with the state-of-the-art robust image steganography algorithms; Section 5 is the conclusion.

2 Robust Embedding Domain Construction Using SVD

2.1 Singular Value Decomposition

SVD is a kind of orthogonal transforms used for matrix diagonalization. Let $\mathbf{A} \in \mathbf{R}^{m \times n}$ be a $m \times n$ matrix. Then, the matrix $\mathbf{A}$ can be represented by its SVD in the following form,

$$\mathbf{A} = \mathbf{USV}^T = (\mathbf{u_1}, \mathbf{u_2}, \cdots, \mathbf{u}_N)\begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_r & \\ & & & 0 \end{pmatrix}\begin{pmatrix} \mathbf{v}_1^T \\ \mathbf{v}_2^T \\ \vdots \\ \mathbf{v}_N^T \end{pmatrix} = \sum_{i=1}^{r} \lambda_i \mathbf{u}_i\, \mathbf{v}_i^T \qquad (1)$$

(1)

where $\mathbf{U}$ and $\mathbf{V}$ are orthogonal $M \times N$ and $N \times M$ matrices, respectively, and $\mathbf{S}$ is a diagonal matrix with nonnegative elements. Diagonal terms $\lambda_1, \lambda_2, \cdots, \lambda_r$ of matrix $\mathbf{S}$ are singular values of matrix $\mathbf{A}$ in a descending order and r is the rank of matrix $\mathbf{A}$.

There are many attractive mathematical properties of SVD, such as the singular values $\lambda_1, \lambda_2, \cdots, \lambda_r$ are unique and have good stability. In other words, when a small perturbation is added to a matrix, in contrast to the changes of matrix element values, the changes of singular values are very small.

2.2 DCT Coefficient Properties of JPEG Image

JPEG is one of the most popular image formats on the Internet because it can achieve good tradeoff between storage size and image quality. The basis for JPEG is the DCT (Discrete Cosine Transform) which is a lossy image compression technique. For JPEG compression, the image is performed two-dimensional (2D) DCT on 8 × 8 blocks, and then the DCT coefficients are quantized according to the quality factor or JPEG quantization table, finally, the DCT blocks are encoded using Huffman encoding.

As we know, a DCT block of JPEG image can be separated into low, middle, and high frequency bands as shown in Fig. 1. The DCT coefficients in low frequency band is most important for image quality and the small changes to the DCT coefficients will change the image quality significantly. On the other hand, although the changes of DCT coefficients in the high frequency band will no significantly degrade image quality, the DCT coefficients or their statistics are not robust for lossy image processing. Therefore, to get a high quality and robust stego image, middle frequency band is suitable for message embedding.

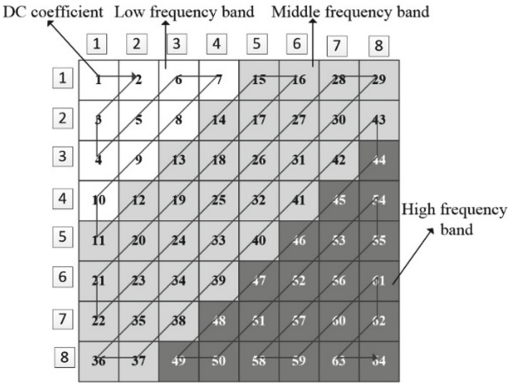


Fig. 1. Zig-zag ordering and frequency bands for DCT coefficients.

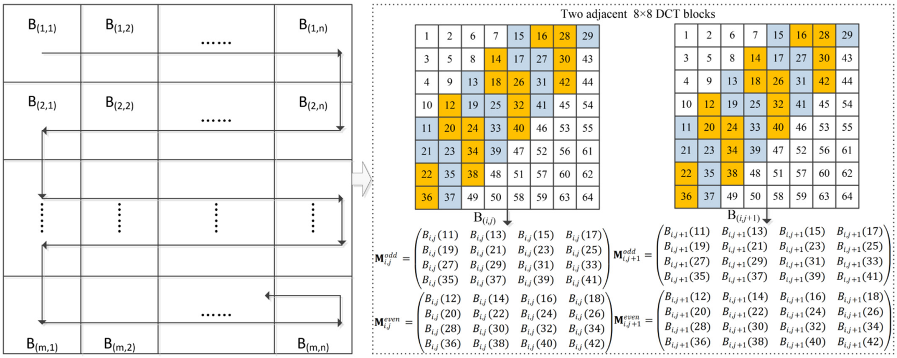
2.3 Robust Embedding Domain Construction

For JPEG image, it is generally known that the inter-block DCT coefficients have strong correlation. That is to say, the DCT coefficients at the same positions in two adjacent DCT blocks have close values. Moreover, the correlations between them are relatively stable against lossy image processing. Unlike [4], we do not directly use the coefficient correlation to extract the cover elements. Considering the stability of singular values, we extract the cover elements by exploiting this correlation of the maximum singular value of the matrixes generated using the DCT coefficients in middle frequency bands of two adjacent 8 × 8 DCT blocks. Therefore, A binary cover element can be extracted based on two adjacent DCT blocks.

In Fig. 2, the adjacent relations of DCT blocks and the construction of matrix for SVD are both shown. To get the adjacent relations, all the DCT blocks are scanned in a snake-like order, and then each DCT block has an adjacent DCT block according to the scan order. To extract a binary cover element, two matrixes should be respectively constructed using the DCT coefficients in middle frequency band of two adjacent DCT blocks such as $B_{(i,j)}$ and $B_{(i,j+1)}$. Specially, to ensure the reference DCT coefficients are not altered during embedding process, the matrixes of two adjacent DCT blocks are constructed using the DCT coefficients at different positions. As shown in Fig. 2, if the traversing order of $B_{(i,j)}$ is an odd number, the matrixes of two adjacent blocks for SVD is $\mathbf{M}_{i,j}^{odd}$ and $\mathbf{M}_{i,j+1}^{odd}$. On the contrary; if the traversing order of $B_{(i,j)}$ is an even number, the matrixes of two adjacent blocks for SVD is $\mathbf{M}_{i,j}^{even}$ and $\mathbf{M}_{i,j+1}^{even}$.

After all the matrixes for SVD are constructed, SVD is performed for each matrix and the maximum singular value is got. Supposed the matrixes of two adjacent DCT blocks $B_{(i,j)}$ and $B_{(i,j+1)}$ are $\mathbf{M}_{i,j}^{odd}$ and $\mathbf{M}_{i,j+1}^{odd}$ respectively, the corresponding maximum singular values are $\lambda_{i,j}$ and $\lambda_{i,j+1}$. Then, a binary cover element can be extracted according to Eq. (2),

$$c_{i,j} = \begin{cases} 1, & if\, \lambda_{i,j} \geq \lambda_{i,j+1} \\ 0, & if\, \lambda_{i,j} < \lambda_{i,j+1} \end{cases}. \tag{2}$$



1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

$$\mathbf{M}_{i,j}^{odd} = \begin{pmatrix} B_{i,j}(11) & B_{i,j}(13) & B_{i,j}(15) & B_{i,j}(17) \\ B_{i,j}(19) & B_{i,j}(21) & B_{i,j}(23) & B_{i,j}(25) \\ B_{i,j}(27) & B_{i,j}(29) & B_{i,j}(31) & B_{i,j}(33) \\ B_{i,j}(35) & B_{i,j}(37) & B_{i,j}(39) & B_{i,j}(41) \end{pmatrix} \quad \mathbf{M}_{i,j+1}^{odd} = \begin{pmatrix} B_{i,j+1}(11) & B_{i,j+1}(13) & B_{i,j+1}(15) & B_{i,j+1}(17) \\ B_{i,j+1}(19) & B_{i,j+1}(21) & B_{i,j+1}(23) & B_{i,j+1}(25) \\ B_{i,j+1}(27) & B_{i,j+1}(29) & B_{i,j+1}(31) & B_{i,j+1}(33) \\ B_{i,j+1}(35) & B_{i,j+1}(37) & B_{i,j+1}(39) & B_{i,j+1}(41) \end{pmatrix}$$

$$\mathbf{M}_{i,j}^{even} = \begin{pmatrix} B_{i,j}(12) & B_{i,j}(14) & B_{i,j}(16) & B_{i,j}(18) \\ B_{i,j}(20) & B_{i,j}(22) & B_{i,j}(24) & B_{i,j}(26) \\ B_{i,j}(28) & B_{i,j}(30) & B_{i,j}(32) & B_{i,j}(34) \\ B_{i,j}(36) & B_{i,j}(38) & B_{i,j}(40) & B_{i,j}(42) \end{pmatrix} \quad \mathbf{M}_{i,j+1}^{even} = \begin{pmatrix} B_{i,j+1}(12) & B_{i,j+1}(14) & B_{i,j+1}(16) & B_{i,j+1}(18) \\ B_{i,j+1}(20) & B_{i,j+1}(22) & B_{i,j+1}(24) & B_{i,j+1}(26) \\ B_{i,j+1}(28) & B_{i,j+1}(30) & B_{i,j+1}(32) & B_{i,j+1}(34) \\ B_{i,j+1}(36) & B_{i,j+1}(38) & B_{i,j+1}(40) & B_{i,j+1}(42) \end{pmatrix}$$

Fig. 2. DCT blocks scan order and matrix construction for SVD.

Therefore, for each DCT block, we can extract a binary cover element and all the cover elements are used as the cover object. For example, suppose the size of cover image is 512 × 512, and then the number of 8 × 8 DCT blocks and the cover elements are both 4096. Finally, the extracted cover object is used for robust message embedding.

3 Proposed Robust JPEG Steganography Algorithm

3.1 Framework of Proposed JPEG Steganography Algorithm

In Fig. 3, the whole framework of the proposed robust JPEG steganography algorithm is shown, which includes the message embedding procedure and extracting procedure.

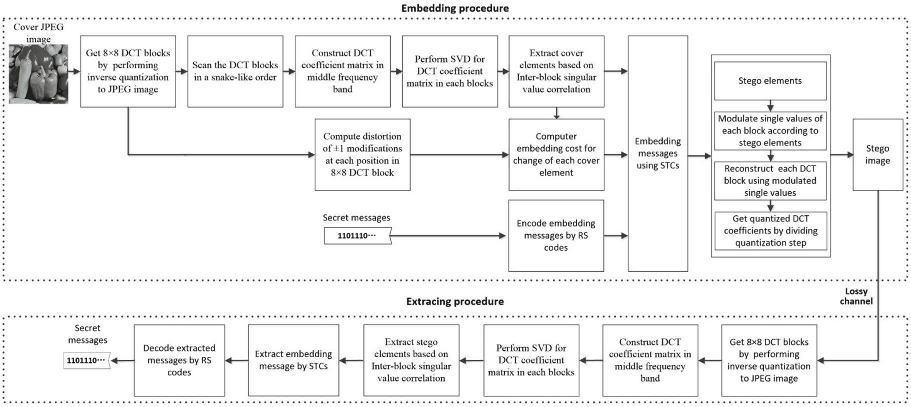

Embedding procedure
Cover JPEG image
Get 8×8 DCT blocks by performing inverse quantization to JPEG image
Scan the DCT blocks in a snake-like order
Construct DCT coefficient matrix in middle frequency band
Perform SVD for DCT coefficient matrix in each blocks
Extract cover elements based on Inter-block singular value correlation
Compute distortion of ±1 modifications at each position in 8×8 DCT block
Computer embedding cost for change of each cover element
Secret messages
1101110···
Encode embedding messages by RS codes
Embedding messages using STCs
Stego elements
Modulate single values of each block according to stego elements
Reconstruct each DCT block using modulated single values
Get quantized DCT coefficients by dividing quantization step
Stego image
Lossy channel
Extracting procedure
Secret messages
1101110···
Decode extracted messages by RS codes
Extract embedding message by STCs
Extract stego elements based on Inter-block singular value correlation
Perform SVD for DCT coefficient matrix in each blocks
Construct DCT coefficient matrix in middle frequency band
Get 8×8 DCT blocks by performing inverse quantization to JPEG image

Fig. 3. Framework of proposed robust and adaptive JPEG steganography algorithm.

As shown in Fig. 3, the embedding procedure gives the execution steps for message embedding. The inverse quantization operation is performed by multiplying the DCT coefficients by the corresponding quantization step, then all the 8 × 8 DCT blocks are scanned in a snake-like order shown in Fig. 2 and the adjacent relations of DCT blocks are determined according to the scan order. For each DCT block, a DCT coefficient matrix is constructed in middle frequency band and SVD is performed for the constructed DCT coefficient matrix, and then the cover elements are extracted according to the inter-block maximum singular value correlation. For embedding cost of each cover element, the distortion of ±1 modification at each position in 8 × 8 DCT block is firstly computed, and then the embedding cost is measured according to the changes caused by the modification of maximum singular value. In addition, to improve the robustness, the secret messages are encoded by RS codes which can correct some error bits. Then, based on the cover elements and the corresponding embedding costs, the encoded secret messages are embedded using STCs and the corresponding stego elements are generated. Finally, the maximum singular values of the constructed DCT coefficient matrixes are modified according to the stego elements, and then all the 8 × 8 DCT blocks are reconstructed and the stego image is generated.

For message extraction, as shown in Fig. 3, the stego image is performed inverse quantization operation and then the corresponding 8×8 DCT blocks are got. For each DCT block, the DCT coefficient matrix is constructed in middle frequency band and SVD is performed for the constructed DCT coefficient matrix. Then, the stego elements can be extracted according to the inter-block maximum singular value correlation. Finally, the encoded messages are extracted by STCs and then the secret messages are obtained using RS decoder.

3.2 Extract Cover Elements

Let **X** denotes the cover JPEG image of size $M \times N$ and $B_{(i,j)}$ denotes the (i, j)-th 8 × 8 DCT blocks. According to the steganography framework shown in Fig. 3, the DCT blocks are scanned in snake-like order and a binary cover element can be extracted using two adjacent DCT blocks such as $B_{(i,j)}$ and $B_{(i,j+1)}$.

For ease of description, according to the block scanning order, we denote the B_k as the k-th DCT block and its adjacent DCT block is B_{k+1}. The number of DCT blocks is $\lfloor M/8 \rfloor \times \lfloor N/8 \rfloor$ where $\lfloor \cdot \rfloor$ denotes the floor function. Then, matrix $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$ are respectively constructed using the DCT coefficients in middle frequency band of DCT blocks B_k and B_{k+1}. Next, SVD is performed for $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$, the corresponding maximum singular values are λ_k and λ_{k+1}. Finally, the cover element c_k can be extracted according to Eq. (3),

$$c_k = \begin{cases} 1, \ \textit{if} \ \lambda_k \geq \lambda_{k+1} \\ 0, \ \textit{if} \ \lambda_k < \lambda_{k+1} \end{cases}. \tag{3}$$

According to Eq. (3), we know that the cover element c_k equals 0 or 1. For each block can generate a cover element, L cover elements $c_1, c_2, \cdots, c_L$ are generated in total and L equals $\lfloor M/8 \rfloor \times \lfloor N/8 \rfloor$. These cover elements construct the cover object which is a binary sequence.

3.3 Define Embedding Costs of Cover Elements

As shown in Fig. 3, the cover object is constructed based on the maximum singular value correlation in DCT domain and then the secret messages are embedded by STCs.

Therefore, an embedding cost need to be defined for each cover element. We know that J-UNIWARD is one of the most powerful JPEG steganography algorithms and it has good anti-detection ability against the state-of-the-art steganalysis techniques. Therefore, we use the embedding distortion function of J-UNIWARD to measure the cost of ±1 modification for DCT coefficient.

The embedding distortion function of J-UNIWARD is defined in Eq. (4),

$$D(X,Y) = \sum\nolimits_{k=1}^{3} \sum\nolimits_{i,j} \frac{\left| W_{ij}^{(k)}(X) - W_{ij}^{(k)}(Y) \right|}{\varepsilon + \left| W_{ij}^{(k)}(X) \right|}, \tag{4}$$

where X,Y denote the cover image and stego image respectively, $W_{ij}^{(k)}(X)$ and $W_{ij}^{(k)}(Y)$ denote the (i, j)-th wavelet coefficient got using k-th wavelet filter, ε is a stabilizing constant to avoid dividing by zero.

Furthermore, $D(X, Y)$ can be denoted as additive form as follows,

$$D(X,Y) = \sum\nolimits_{i,j} \rho_{ij}(X, Y_{ij}), \tag{5}$$

where $\rho_{ij}(X, Y_{ij})$ denotes the embedding distortion with only (i,j)-th element changed. In other words, $\rho_{ij}(X, Y_{ij})$ is the cost of ±1 modification for (i,j)-th DCT coefficient.

For the proposed robust and adaptive JPEG steganography algorithm, the cover element is extracted by modifying the maximum singular values of the matrix $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$ constructed using the DCT coefficients in middle frequency bands of two adjacent DCT blocks. Therefore, the modification of a cover element will cause the changes of multiple elements. Then, the embedding cost of the cover element is measured by summing all the embedding costs of the corresponding DCT coefficients. The specific form is shown in Eq. (6),

$$\rho(c_k) = \sum\nolimits_{Y_{i,j \in \mathbf{M}_k}} d_{ij}\big(X, Y_{ij}\big) \times \rho_{ij}\big(X, Y_{ij}\big) + \sum\nolimits_{Y_{i,j \in \mathbf{M}_{k+1}}} d_{ij}\big(X, Y_{ij}\big) \times \rho_{ij}\big(X, Y_{ij}\big), \tag{6}$$

where $d_{ij}\big(X, Y_{ij}\big)$ denotes the modifications of (i,j)-th DCT coefficients that are caused by modification to the cover element c_k.

3.4 Embed Stego Elements by Modifying Maximum Singular Values

Based on the cover object and the corresponding embedding cost, the encoded secret messages can be embedded by STCs. Then, the stego object is generated and it includes L binary stego elements. According to the steganography framework shown in Fig. 3, the stego elements need to be embedded by modifying the maximum singular value correlation.

Suppose the maximum singular values of matrixes $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$ are λ_k and λ_{k+1} respectively, and s_k denote the k-th stego element. Then, the stego element s_k can be embedded by modifying λ_k and λ_{k+1} according to Eq. (7) and Eq. (8),

$$\lambda'_k = \begin{cases} E + \alpha \\ E - \alpha \end{cases}, \; if \; s_k = 1 \tag{7}$$

$$\lambda'_{k+1} = \begin{cases} E - \alpha \\ E + \alpha \end{cases}, \; \mathit{if}\ s_k = 0 \tag{8}$$

where λ'_k and λ'_{k+1} denotes the modified maximum singular values, $E = (\lambda_k + \lambda_{k+1})/2$ and α is the embedding strength factor. After the modification for λ_k and λ_{k+1}, the new matrixes $\mathbf{M}'_k$ and $\mathbf{M}'_{k+1}$ are reconstructed using λ'_k and λ'_{k+1}, and the corresponding DCT coefficients are also modified.

In Eq. (7) and Eq. (8), it can be seen that the parameter α is the key factor for the robustness of stego elements against lossy image processing. The large α means strong robustness whereas the corresponding modifications are large which led to the weak anti-detection ability. Therefore, a suitable parameter α should be selected which can achieve good tradeoff between steganography robustness and anti-detection ability.

3.5 Extract Stego Elements

As shown in Fig. 3, for message extraction, the stego object $S = (s_1, s_2, \cdots, s_L)$ should be firstly extracted and then the embedded messages are extracted by STCs and RS decoder.

According to the embedding rule of stego elements in Eq. (7) and (8), the stego elements can be extracted using Eq. (9),

$$s_k = \begin{cases} 1, \mathit{if}\, \lambda'_k \geq \lambda'_{k+1} \\ 0, \mathit{if}\, \lambda'_k < \lambda'_{k+1} \end{cases}. \tag{9}$$

where λ'_k and λ'_{k+1} respectively denote the maximum singular values of two matrixes constructed using two adjacent DCT blocks of stego image.

To summarize, the embedding procedure and extraction procedure of the proposed robust and adaptive JPEG steganography can be respectively described in Algorithm 1 and 2.

Algorithm 1 Embedding algorithm

```
Input: Cover image $\mathbf{X}$, message $\mathbf{m}$, embedding strength factor $\alpha$
Output: Stego image $\mathbf{Y}$
Step1: The inverse quantization operation is performed for cover JPEG image by multiplying the DCT coefficients with the corresponding quantization step.
Step2: All DCT blocks are scanned in a snake-like order from the upper left to the lower right and the adjacent relations of DCT blocks are determined.
Step3: For each DCT block, a matrix $\mathbf{M}_k$ is constructed using the DCT coefficients in middle frequency band and the corresponding matrix $\mathbf{M}_{k+1}$ is constructed using its adjacent block.
Step4: SVD is performed for matrixes $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$, a cover element $c_k$ can be extracted according to Eq.(3), and the other cover elements are extracted in the same way.
Step5: The embedding costs of the cover elements are computed according to Eq.(4), Eq.(5) and Eq.(6).
Step6: The secret messages are encoded by RS code.
Step7: The stego elements are generated by embedding the encoded secret messages based on cover elements, embedding costs and STCs.
Step8: The stego elements are embedded according to Eq.(7) and Eq.(8).
Step9: The corresponding DCT coefficients of each DCT block are modified according to the modified maximum singular values.
Step10: The stego image is got by quantizing the DCT coefficients.
```

Algorithm 2 Extracting algorithm

```
Input: Stego image $\mathbf{Y}$, embedding strength factor $\alpha$
Output: message $\mathbf{m}$
Step1: The inverse quantization operation is performed for stego JPEG image
Step2: All DCT blocks are scanned in a snake-like order and the adjacent relations of DCT blocks are determined.
Step3: For each DCT block, a matrix $\mathbf{M}_k$ is constructed using the DCT coefficients in middle frequency band and the corresponding matrix $\mathbf{M}_{k+1}$ is constructed for its adjacent block.
Step4: SVD is performed for matrixes $\mathbf{M}_k$ and $\mathbf{M}_{k+1}$, a stego element $s_k$ can be extracted according to Eq.(9), and the other stego elements are extracted in the same way.
Step5: The encoded secret messages are extracted using STCs.
Step6: The secret messages are got by RS decoder.
```

4 Experimental Results and Analyses

In the experiments, the robustness against JPEG compression attack and the anti-detection ability of the proposed steganography algorithm are compared with the other robust JPEG steganography algorithms. Moreover, the proposed steganography algorithm is used in WeChat platform and the corresponding experiment results are shown. For the robustness and anti-detection experiments, the 10000 grayscale images from

BOSSbase1.01 [13] are used as sample images. The size of sample images is 512×512 and all the sample images with PGM format are converted to JPEG image with quality factor (QF) 85. The parameter of RS code is (31, 19).

4.1 Robustness Against JPEG Compression Attack

As we know, the complex image has strong resistance to the detection. Therefore, we should select some images with complex texture for messages embedding. Here, one-level wavelet transform is performed for the image and the energy of wavelet coefficients of the three high-pass subbands is used to measure the complexity of the image.

To evaluate the robustness against JPEG compression attack of the proposed steganography algorithm, the most complex 2000 images from BOSSbase1.01 are used to generate the stego images. The robust steganography algorithms used for comparison are MREAS-P_S and MREAS-P_J [10]. For the proposed steganography algorithm, the number of cover elements is 4096 because the image size is 512 × 512 and DCT block size is 8 × 8. Therefore, the length of the embedded message bits cannot exceed 4096. The payload is set to 0.001, 0.002, 0.003, 0.004, 0.005 bpnzAC (bit per non-zero AC DCT coefficient) respectively. Then, for each robust steganography algorithm, we have one group of cover images and five groups of stego images.

Table 1. Average extraction error rates of three robust steganography algorithms for the 2000 complex images in BOSSbase1.01. ($\mathbf{x10^{-3}}$)

QF	Algorithm	Payload (bpnzAC)				
		0.001	0.002	0.003	0.004	0.005
65	Proposed	0.74	0.71	0.72	0.63	0.68
	MREAS-P_S	248	249	251	253	255
	MREAS-P_J	245	248	247	250	249
75	Proposed	3.7	3.6	3.7	3.9	3.7
	MREAS-P_S	12.3	12.5	13.1	13.3	13.0
	MREAS-P_J	0.92	1.00	1.20	1.50	1.50
85	Proposed	0.50	0.40	0.44	0.43	0.51
	MREAS-P_S	0.88	1.00	1.10	1.30	1.30
	MREAS-P_J	0.13	0.12	0.28	0.36	0.44
95	Proposed	0.51	0.42	0.45	0.44	0.52
	MREAS-P_S	0.60	0.56	0.75	0.91	0.88
	MREAS-P_J	0.13	0.12	0.25	0.42	0.47

According to the average extraction error rates shown in Table 1, the proposed robust and adaptive JPEG steganography algorithm has achieved the competitive robustness.

As shown in Table 1, for MREAS-P_J, the average extraction error rates are low when the QFs of JPEG compression attack are 85 and 95. However, the extraction error rates become very high when the QF of JPEG compression attack is 65 which means strong attack.

4.2 Detection Resistance for Typical Steganalysis Features

The anti-detection ability is important for robust image steganography. Here, the proposed steganography algorithm is compared with MREAS-P$_s$ and MREAS-P$_J$ using CC-PEV [14] and DCTR [15] which are the typical steganalysis features.

Same with Sect. 4.1, the most complex 2000 images from BOSSbase1.01 are used to generate stego images. The payloads are from 0.001 to 0.050 bpnzAC. The ensemble classifier [16] is trained by the steganalysis feature and used as the final detector. The ratio of training and test images is 0.5:0.5. The detection accuracy is quantified using the minimal total error probability under equal priors $P_E = min_{P_{\mathrm{FA}}}(P_{\mathrm{FA}} + P_{\mathrm{MD}})/2$, where P_{FA} denotes the false-alarm probabilities and P_{MD} denotes the missed-detection probabilities. The value of $\bar{P}_E$ is averaged over ten random image database splits.

According to the detection performances, we find that the detection resistance of the proposed steganography algorithm is relatively weak in contrast to MREAS-P$_S$ and MREAS-P$_{J.}$ It is possible that the embedding changes of the proposed algorithm is larger.

4.3 Application in WeChat Platform

WeChat is the most popular chat app in China and it provide a good public channel for covert communication by image steganography. However, the compression algorithm of WeChat is unknown. Therefore, UEDR-P cannot realize robust steganography by WeChat channel. Therefore, only the robustness of MREAS-P$_J$ and the proposed steganography is evaluated for WeChat channel.

Fig. 4. Cover image for covert communication by WeChat. (a) '8.jpg' in BOSSbase1.01 and (a) '4226.jpg' in BOSSbase1.01.

The two cover images are shown in Fig.4 and the image sizes are both 512 × 512. The left cover image is '8.jpg' in BOSSbase1.01 with 157 KB and the right cover image is ‘4226.jpg’ with 258 KB. First, the stego images are generated by MREAS-P$_J$ and the proposed steganography algorithm with (31,19) RS codes and the payload is 0.01 bpnzAC. Next, the stego images are posted on the moment of WeChat. Then, the stego images are downloaded from the moment of WeChat and the file size of the downloaded WeChat images are 54 KB and 105 KB respectively. Finally, the embedded messages are extracted from the downloaded WeChat image and the extraction error rates are calculated. The experimental results are shown in Table 2.

Table 2. Comparisons of robustness of MREAS-P$_J$ and the proposed steganography algorithm against WeChat compression.

Image	Algorithm	Error rate	Communication
8.jpg	Proposed	0	Success
	MREAS-P$_J$	0	Success
4226.jpg	Proposed	0	Success
	MREAS-P$_J$	0	Success

Table 2 shows that MREAS-P$_J$ and the proposed algorithm both can realize the correct message transmission under lossy WeChat channel.

5 Conclusions

Robust image steganography techniques are important for covert communication under lossy transmission channels. Based on the singular value decomposition in DCT domain, a robust JPEG steganography algorithm is proposed. Considering the inter-block DCT coefficient correlation and the stability of singular value, the robust embedding domain is constructed using the correlation of the maximum singular values generated from two adjacent DCT blocks. Then, the whole frame of the proposed steganography algorithm is given and the procedure of message embedding and extraction are described in details. The experimental results show the proposed JPEG steganography is effective against JPEG compression and WeChat channel compression.

Furthermore, we also notice that the anti-detection ability of the current robust image steganography techniques is all weak when the detection is performed by the classifier trained using the cover images and the corresponding stego images. This is because that the embedding changes of the robust JPEG steganography scheme are much larger than the non-robust JPEG steganography scheme such as J-UNWARD. In other words, to achieve the robustness, the embedding changes will be large. In the future, the robust embedding domain which can led to the stronger robustness and anti-detection ability should be studied.

Acknowledgements. This research was supported by National Natural Science Foundation of China (Grant Nos 61872448, U1804263).

References

1. Fridrich, J.: Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge (2010)
2. Guo, L., Ni, J., Shi, Y.: Uniform embedding for efficient JPEG steganography. IEEE Trans. Inf. Forensics Secur. **9**(5), 814–825 (2014)
3. Holub, V., Fridrich, J.: Digital image steganography using universal distortion. In: 1st Workshop on ACM Information Hiding and Multimedia Security, Montpellier, France, pp.59–68. ACM (2013)
4. Zhang, Y., Luo, X., Yang, C., Ye, D., Liu, F.: A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients. In: Proc. of the 10th International Conference on Availability, Reliability and Security, Toulouse, France, pp. 461–66. IEEE (2015)
5. Qian, Z., Zhou, H., Zhang, W., Zhang, X.: Robust steganography using texture synthesis. In: Pan, J.S., Tsai, P.W., Huang, H.C. (eds.) Intelligent Information Hiding and Multimedia Signal Processing, vol. 63, pp. 25–33. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-50209-0_4
6. Zhang, Y., Zhu, X., Yang, C., Luo, X., Qin, C.: Dither modulation based adaptive steganography resisting JPEG compression and statistic detection. Multimed. Tools Appl. **77**(14), 17913–17935 (2018)
7. Zhao, Z., Guan, Q., Zhang, H., Zhao, X.: Improving the robustness of adaptive steganographic algorithms based on transport channel matching. IEEE Trans. Inf. Forensics Secur. **14**(7), 1843–1856 (2018)
8. Tao, J., Li, S., Zhang, X., Wang, Z.: Towards robust image steganography. IEEE Trans. Circ. Syst. Video Technol. **29**(2), 594–600 (2018)
9. Yu, X., Chen, K., Wang, Y., Li, W., Zhang, W., Yu, N.: Robust adaptive steganography based on generalized dither modulation and expanded embedding domain. Signal Process. **168**, 1–12 (2019)
10. Zhang, Y., Luo, X., Guo, Y., Qin, C., Liu, F.: Multiple robustness enhancements for image adaptive steganography in lossy channels. IEEE Trans. Circ. Syst. Video Technol. 1–13 (2019)
11. Bao, P., Ma, X.: Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans. Circ. Syst. Video Technol. **15**(1), 96–102 (2005)
12. Filler, T., Judas, J., Fridrich, J.: Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans. Inf. Forensics Secur. **6**(3), 920–935 (2011)
13. Bas, P., Filler, T., Pevný, T.: Break our steganographic system: the ins and outs of organizing BOSS. In: Filler, T., Pevný, T., Craver, S., Ker, A. (eds.) IH 2011. LNCS, vol. 6958, pp. 59–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24178-9_5
14. Pevny, T., Fridrich, J.: Multiclass detector of current steganographic methods for JPEG format. IEEE Trans. Inf. Forensics Secur. **3**(4), 635–650 (2008)
15. Holub, V., Fridrich, J.: Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Trans. Inf. Forensics Secur. **10**(2), 219–228 (2015)
16. Kodovský, J., Fridrich, J., Holub, V.: Ensemble classifiers for steganalysis of digital media. IEEE Trans. Inf. Forensics Secur. **7**(2), 432–444 (2012)