Multimedia Tools and Applications (2022) 81:36453–36472
https://doi.org/10.1007/s11042-022-13525-4

1213: COMPUTATIONAL OPTIMIZATION AND APPLICATIONS FOR HETEROGENEOUS MULTIMEDIA DATA

Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain

Xiaofeng Song[1] · Chunfang Yang[2] · Kun Han[1] · Shichang Ding[2,3]

Received: 31 January 2021 / Revised: 5 October 2021 / Accepted: 13 July 2022 /
Published online: 2 August 2022

Abstract
Social media platform such as WeChat provides rich cover images for covert communication by steganography. However, in order to save band-width, storage space and make images load faster, the images often will be compressed, which makes the image steganography algorithms designed for lossless network channels unusable. Based on DCT and SVD in nonsubsampled shearlet transform 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, by combining the advantages of nonsubsampled shearlet transform, DCT and SVD, the construction method for robust embedding domain is proposed. Then, based on minimal distortion principle, the framework of the proposed robust 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 and anti-detection capability in contrast to the state-of-the-art robust steganography algorithms. Moreover, it can extract the secret message correctly even if the stego image is compressed by WeChat.

Keywords JPEG steganography · Robustness · Anti-detection capability · Shearlet DCT · SVD

1 Introduction

Image steganography is an art of covert communication in which the secret message is hidden inside a cover image [5, 12]. Then, the secret message can be transmitted through an innocuous-looking stego image. Due to the wide application of JPEG images on the Internet,

✉ Xiaofeng Song
xiaofengsong@sina.com

[1] National University of Defense Technology, Xi'an 710106, China

[2] Zhengzhou Science and Technology Institute, Zhengzhou 450001, China

[3] University of Göttingen, Göttingen, Germany

JPEG image steganography has received extensive attentions. In recent years, many JPEG Image steganography algorithms have been proposed, such as JPEG UNIversal WAvelet Relative Distortion (J-UNIWARD) steganography [9], Uniform Embedding Distortion (UED) [8] steganography, and so on. These JPEG steganography algorithms are all content-adaptive and the embedding changes are constrained to the complex texture regions difficult to model. Therefore, they have strong anti-detection capability, however, they are not robust to the lossy image processing such as image compression, image resizing, etc. [24]. So, they are not suitable for some public transmission channel such as WeChat which often apply lossy compression for the stego images. To conduct covert communication using the rich images in social network as covers, the JPEG steganography algorithm must be robust to the lossy image compression. In other words, robust JPEG steganography not only should be able to resist the lossy image operations, but also should has good anti-detection capability. Compared with content-adaptive JPEG steganography, robust JPEG steganography has attracted relatively little attention in the past decades. However, in recent years, the researchers have proposed a series of robust JPEG steganography algorithms [16, 17, 23–27]. Robust JPEG steganography techniques against lossy operations are becoming a research hotspot in the field of information hiding.

For the design of robust JPEG steganographic schemes, Zhang et al. [24] 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. [16] proposed a robust steganography algorithm using texture synthesis, however, the extraction error rate of secret message is relatively high; Zhang et al. [25] also proposed a JPEG compression and detection resistant steganography algorithm based on dither modulation when the quality factor of cover JPEG image is no larger than the quality factor of JPEG compression channel; Tao et al. [17] 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; Zhao et al. [27] proposed a robust JPEG image steganography algorithm based on transmission channel matching, however, the behavior of repeatedly uploading images for recompression is very suspicious; Yu et al. [23] proposed a robust image steganography algorithm based on generalized dither modulation and embedding domain expansion, which can achieve better robustness and anti-detection capability than the method in [25], however, the quality factor of cover JPEG image is also no larger than the quality factor of JPEG compression channel; Zhang et al. [26] proposed a robust steganography algorithm with multiple robustness enhancements, however, the anti-detection capability is still relatively weak.

In this paper, a robust JPEG steganography algorithm is proposed based on DCT and SVD in nonsubsampled shearlet domain [6, 19]. As we know, the low frequency information of the image is more robust for lossy image compression. Therefore, the cover image is firstly decomposed by single scale nonsubsampled shearlet transform (NSST) and the low frequency band is used for message embedding. Furthermore, taking the advantages of DCT and SVD for robust message embedding [1, 11, 18], the low frequency band is divided into 8×8 blocks and DCT is performed for each block, and then SVD is performed for a special matrix constructed using the DCT coefficients in low and middle frequency domain of 8×8 block. Then, the maximum singular values of all the blocks are used for the construction of robust embedding domain and quantization index modulation (QIM) is used for message embedding

and extracting [3]. The binary cover elements can be extracted using QIM for the maximum singular values. The embedding distortion of each cover element is defined according to the texture complexity of the corresponding block and the embedding changes caused by modulating the maximum singular value. To reduce extraction errors, the secret message is encoded by Reed-Solomon (RS) error correcting code. Next, the encoded messages are embedded using syndrome-trellis codes (STCs) [7] which is widely used for minimal distortion steganography and the stego elements are got. Finally, the stego elements are embedded using QIM on the maximum singular values of the corresponding blocks, and the stego image is generated based on the modulated maximum singular values and inverse SVD, DCT and nonsubsampled shearlet transform.

The rest of this paper is organized as follows: Section 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

In this section, we firstly introduce the characteristic of image decomposition using NSST, and then the procedure of DCT and SVD for image block is described. Finally, the method for robust element extraction is discussed.

2.1 Image decomposition using NSST

Shearlet transform is an effective tool for image multiscale geometric analysis [6, 22]. It can not only provide a more flexible theoretical tool for the geometric representation of multidimensional data, but also is more natural for implementation. Shearlets exhibit highly directional sensitivity and they are spatially localized and optimally sparse. The NSST is a shift-invariant version of the shearlet transform and eliminates the down-samples and up-samples. It combines the nonsubsampled Laplacian pyramid transform with different combinations of the shearing filters. The highly directional sensitivity of NSST and its optimal approximation properties lead to improvements in many image processing applications. In [19], a blind robust image watermarking approach is proposed based NSST.

In Fig. 1, the original Barbara image and the subband images are shown. The subband images are generated by performing NSST for Barbara image with single scale and four directions. According to Fig. 1, it can be found that the Barbara image is decomposed into a low frequency approximation subband and four high frequency directional subbands. As we know, the JPEG compression will significantly impact the high frequency image characteristics such edge, texture, etc. At the same time, the anti-detection capability can be improved by preserving the image texture characteristics which are difficult to model. Therefore, for robust image steganography, the image can be decomposed by NSST firstly and then the low frequency approximate subband is used for message embedding. In contrast to image steganography in spatial domain which directly modifies the image pixels, the image steganography in NSST domain will have stronger robustness and anti-detection capability.

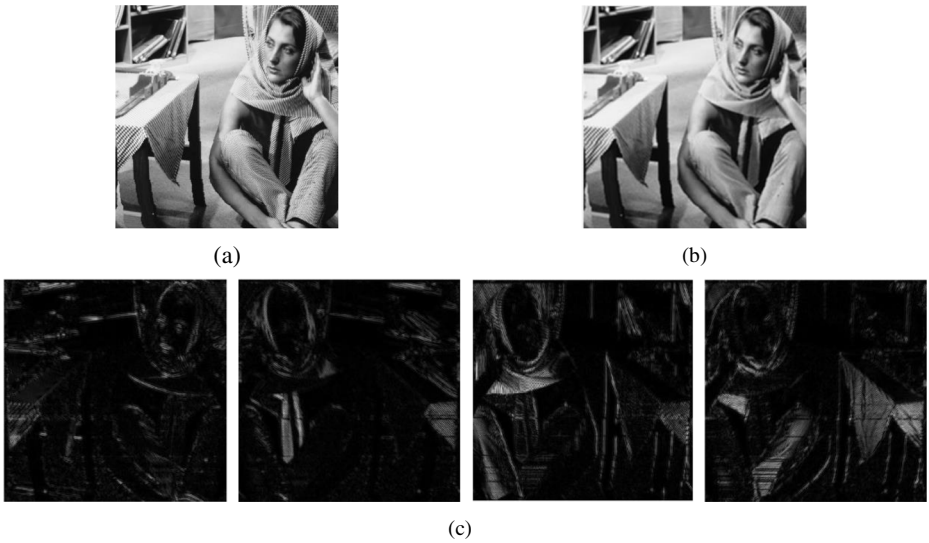

Fig. 1 The NSST on Barbara image: **a** Original Barbara, **b** Low frequency approximate subband, **c** High frequency directional subbands

2.2 Apply DCT and SVD to image block

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 which is a lossy image compression technique. For JPEG compression, the image is performed two-dimensional (2D) DCT on 8 × 8 image 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.

The 2D DCT is defined by (1) and (2) as follow:

$$F(u,v) = \frac{1}{\sqrt{m \times n}} c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) cos \frac{(2x+1)u\pi}{2M} cos \frac{(2y+1)v\pi}{2N}, \quad (1)$$

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

where x, $u = 0, 1, 2, \cdots, M-1$ and y, $v = 0, 1, 2, \cdots, N-1$.

The corresponding inverse DCT is defined by (3) as follow:

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

where $f(x, y)$ is the pixel value of image and $F(u, v)$ is the DCT coefficient.

As we know, a DCT block of JPEG image can be separated into low, middle, and high frequency bands as shown in Fig. 2. The DCT coefficients in low and middle frequency band concentrates the most energy of the image. Therefore, they are relatively stable for lossy JPEG

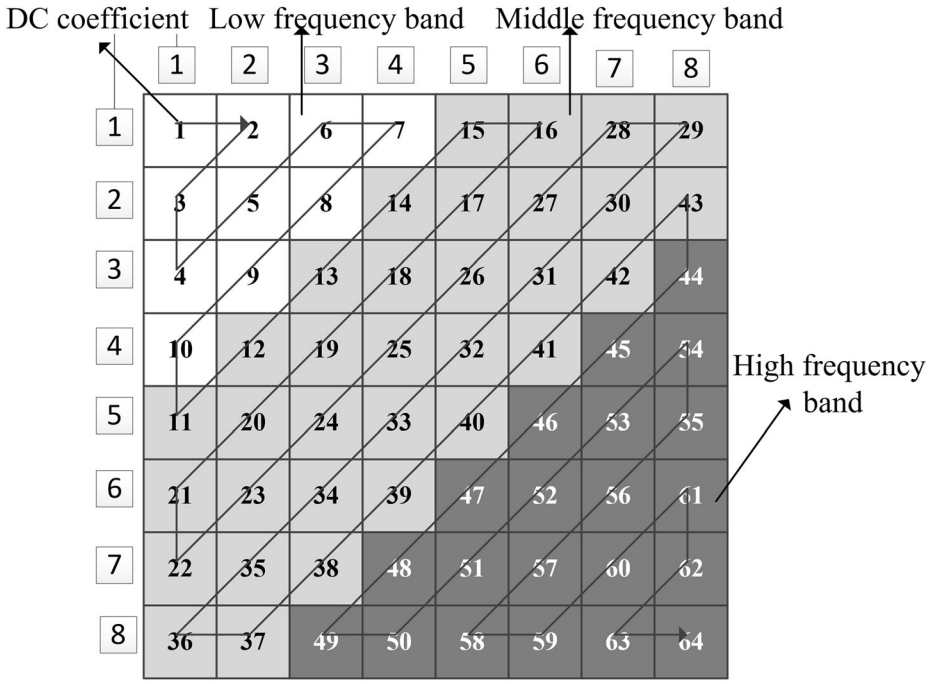

Fig. 2 Zig-zag ordering and frequency bands for DCT coefficients

compression. On the contrary, the DCT coefficients in high frequency band are easy to remove in lossy compression. Therefore, to get a robust stego image, some DCT coefficients in low and middle frequency bands are used for robust element extraction.

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 as (4),

$$\mathbf{A} = \mathbf{USV}^T = (\mathbf{u_1}, \mathbf{u_2}, \cdots, \mathbf{u}_N) \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_r & \\ & & & 0 \end{pmatrix} \begin{pmatrix} \mathbf{v}_1^T \\ \mathbf{v}_2^T \\ \vdots \\ \mathbf{v}_N^T \end{pmatrix} = \sum_{i=1}^{r} \lambda_i \mathbf{u}_i \mathbf{v}_i^T, \quad (4)$$

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. When a small perturbation is added to a matrix, the changes of singular values are very small. Therefore, SVD has been widely used for robust image watermarking techniques [1, 11, 18] and the singular values or singular vectors are often used for watermarking embedding. In this paper, we will employ the maximum singular values of the constructed DCT coefficient matrixes from the 8×8 image blocks to generate the robust elements against JPEG compression.

2.3 Robust elements extraction

Let $\mathbf{I}_c$ denotes the cover JPEG image and it is decompressed to the spatial domain image $\mathbf{I}_{sp}$. The $\mathbf{I}_{sp}$ is decomposed by **NSST**, and $\mathbf{A}_0$ denotes the low frequency subband, $\mathbf{D}_{k,l}$ denotes the high frequency directional subband at scale k and direction l, $k = 1, 2, \cdots, K$, $l = 1, 2, \cdots, L$. Let $\mathbf{B}_i$ denotes the i-th 8×8 block generated by dividing the subband $\mathbf{A}_0$ into nonoverlapping blocks, and N is the number of blocks. Then, 2D DCT is performed for each 8×8 block and the corresponding DCT coefficient matrix can be got as shown in Fig. 2. For the low and middle frequency DCT coefficients have better stability, we construct a 6×6 matrix $\mathbf{M}_i$ using the DCT coefficients with numbers 1 to 36.

Then, SVD is performed for each matrix $\mathbf{M}_i$ by (5) as follow:

$$\mathbf{M}_i = \sum_{j=1}^{r} \lambda_{i,j} \mathbf{U}_{i,j} \mathbf{V}_{i,j}^T, \tag{5}$$

where $\lambda_{i,j}$ denotes the j-th singular value in descending order.

For the maximum singular value $\lambda_{i,1}$ of $\mathbf{M}_i$ has good robustness against lossy JPEG compression. Therefore, we extract the maximum singular value from each 6×6 matrix, then the sequence $\lambda_{1,1}, \lambda_{2,1}, \ldots, \lambda_{N,1}$ is the robust element set which also forms the robust embedding domain.

After the robust elements are extracted, based on QIM, the message bit b can be embedded by (6) as follow:

$$\lambda'_{i,1} = \left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + b \right\rfloor, 2 \right) \right) \times q, \tag{6}$$

where $\lambda_{i,1}$ denotes the maximum singular value and q denotes the quantization step.

Correspondingly, the embedded message bit b can be extracted by (7) as follow:

$$b = \mathrm{mod}\left(round\left(\frac{\lambda'_{i,1}}{q} \right), 2 \right). \tag{7}$$

To verify the effectiveness of the message embedding method using the robust element set, the Barbara image with 512×512 and quality factor (QF) 85 is used for message embedding. According to the above extraction method of robust elements, the number of robust elements is 4096. First, the 4096 bits are embedding according to (6) and the stego image is generated. Then, the JPEG compression is performed for the stego image with QF 65, 75, 85, 95 respectively. Finally, the message bits are extracted according to (7). In Fig. 3, the message extraction error rates are shown.

From the extraction error rates shown in Fig. 3, it can be seen that the extraction error rates reduce rapidly with the increment of the quantization step q. Moreover, when the QF of JPEG compression is low, such as QF 65 and 75, the corresponding quantization step q should be larger to extract the correct message bits.

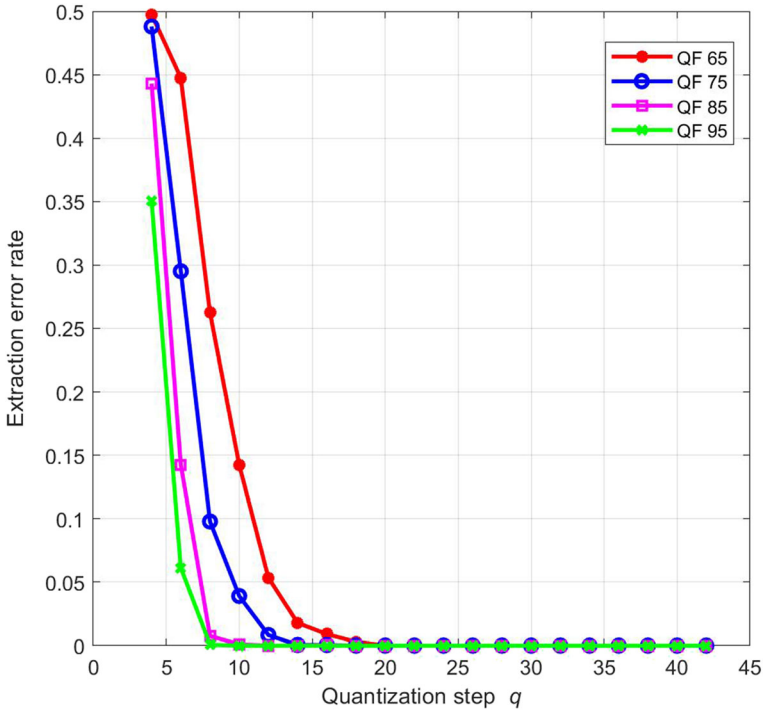

Fig. 3 Message extraction error rates when JPEG compression is performed for the stego Barbara image with QF 65, 75, 85 and 95 respectively

3 Proposed robust JPEG steganography algorithm

In this section, the framework of the proposed robust JPEG steganography algorithm is firstly introduced, and then the implement details of message embedding procedure and extraction procedure are described.

3.1 Framework of proposed steganography algorithm

In Fig. 4, the whole framework of the proposed robust JPEG steganography algorithm is shown, which includes the message embedding procedure and message extracting procedure. This framework employs NSST, DCT and SVD to extract robust elements and then use minimal distortion steganography principle to embed secret message. Moreover, the cover element extraction and the stego element embedding is based on QIM.

For message embedding, the maximum singular value of each constructed DCT coefficient matrix is firstly got based on NSST, DCT and SVD, and then the quantization step q is determined and the corresponding binary cover element is extracted according to QIM; next, the embedding cost of each cover element is computed using the embedding changes and the texture complexity measure, and the messages are encoded by RS code to reduce the extraction errors; then, the encoded messages are embedded by STCs to get the stego elements and QIM is performed for the maximum singular values of all the constructed DCT coefficient matrices

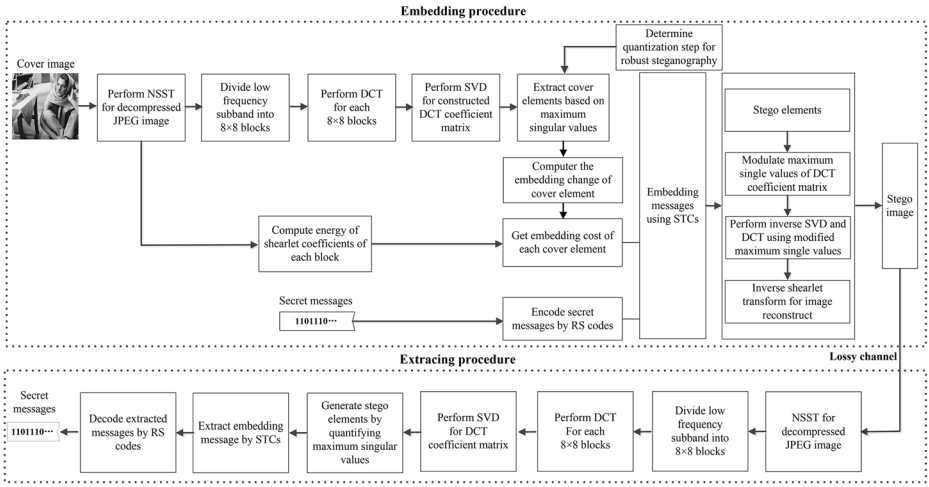

Fig. 4 Framework of proposed robust JPEG steganography algorithm

to embed the stego elements; finally, all the 8 × 8 blocks are reconstructed using the modulated maximum singular values, and then inverse NSST is performed to get the stego image.

For message extraction, the stego image is firstly decompressed to the spatial domain, and then the decompressed JPEG image is decomposed by single scale NSST to obtain a low frequency subband and several high frequency directional subbands; next, the low frequency subband is divided into nonoverlapping 8 × 8 blocks and DCT is performed for each block; then, the 6 × 6 DCT coefficient matrices are constructed from the 8 × 8 DCT blocks and the corresponding maximum singular values are generated to get the stego elements using QIM; finally, the embedded messages are extracted by STCs and RS decoder is used to get the original secret message.

3.2 Message embedding procedure

3.2.1 Extract cover elements

According to the section 2.3, the cover JPEG image is decomposed by NSST and the low frequency subband is divided into 8 × 8 nonoverlapping blocks, and then the robust element $\lambda_{i,1}$ is extracted from each block $\mathbf{B}_i$. To employ the minimal distortion steganography principle to embed the secret message, the binary cover element x_i is generated by (8) as follow:

$$x_i = \mathrm{mod}\left(round\left(\frac{\lambda_{i,1}}{q}\right), 2\right). \tag{8}$$

According to (8), we can find that the generation of cover element is same with the extraction of message bit shown in (7). Then, for each block, we can generate a cover element and N cover elements $\mathbf{x} = (x_1, x_2, \cdots, x_N)$ are generated in total. These cover elements construct the cover object which is a binary sequence.

3.2.2 Define embedding cost

As we know, the embedding cost of each cover element x_i must be defined when the message embedding is performed by STCs which is the widely used for minimal distortion steganography. Here, the texture complexity of the 8 × 8 block $\mathbf{B}_i$ and the embedding change of robust element $\lambda_{i,1}$ are considered at the same time.

As the cover element x_i is extracted from the 8 × 8 block $\mathbf{B}_i$ and the corresponding shearlet coefficients of the high-pass subbands $\mathbf{D}_{k,l}$ reflect the texture complexity of image block. Therefore, the texture complexity measure can be defined by (9) as follow:

$$t_i = \frac{1}{\sum_{l=1}^{D}\sum_{m=1}^{8}\sum_{n=1}^{8}|f_l(i,m,n)|}, \tag{9}$$

where $f_l(i, m, n)$ denotes the (m, n)-th shearlet coefficient of the corresponding blocks in high-pass subband at direction l, and D denotes the number of high-pass subbands. In (9), the t_i is energy of the corresponding shearlet coefficients of the block $\mathbf{B}_i$. The large energy value means the more complex texture structure difficult to model.

Furthermore, as we know, the robust element $\lambda_{i,1}$ should be modulated when the cover element x_i need to be changed for message embedding. The embedding change of robust element $\lambda_{i,1}$ is defined by (10) as follow:

$$e_i = \left|\left(\left\lfloor\frac{\lambda_{i,1}}{q}\right\rfloor + mod\left(\left\lfloor\frac{\lambda_{i,1}}{q} + (1-x_i)\right\rfloor, 2\right)\right) \times q - \lambda_{i,1}\right|. \tag{10}$$

Finally, the embedding cost d_i of the cover element x_i is defined by (11) as follow:

$$d_i = \frac{|t_i - t_{min}|}{|t_{max} - t_{min}|} + \frac{|e_i - e_{min}|}{|e_{max} - e_{min}|}, \tag{11}$$

where t_{max} and t_{min} denote respectively the maximum value and minimal value of the texture complexity measure of all the blocks, e_{max} and e_{min} denote the maximum value and minimal value of embedding changes.

3.2.3 Embed secret message

As shown in Fig. 4, to reduce the extraction error rate, the secret message **m** is encoded by RS code and then the encoded message is embedded using STCs. For the cover elements are binary bits, the binary embedding operation [7] is performed by (12) and (13) as follows:

$$\mathbf{y} = \mathrm{Emb}(\mathbf{x}, \mathbf{m}) = \arg \min_{y \in C(\boldsymbol{m})} D(\mathbf{x}, \mathbf{y}) \tag{12}$$

$$\mathbf{m} = \mathrm{Ext}(\mathbf{y}) = \mathbf{H}\mathbf{y} \tag{13}$$

where $D(\mathbf{x}, \mathbf{y})$ is embedding distortion function, $\mathbf{H} \in \{0, 1\}^{m \times n}$ is a parity-check matrix of the code C, $C(\mathbf{m}) = \{\mathbf{z} \in \{0, 1\}^n | \mathbf{Hz} = \mathbf{m}\}$ is the coset corresponding to syndrome **m**, $D(\mathrm{x}, \mathrm{y}) = \sum_{i=1}^{n} \rho_i |x_i - y_i|$ is embedding distort function, and all operations are in binary arithmetic.

In other words, binary STCs [7] is used for secret message embedding. After messages embedding by binary STCs, we can get the binary stego element set $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$.

3.2.4 Embed stego element based on QIM

As shown in Fig. 4, the binary stego element y_i should be embedded by modulating the robust element $\lambda_{i,1}$ according to (14) as follow:

$$\lambda'_{i,1} = \left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + y_i \right\rfloor, 2 \right) \right) \times q, \tag{14}$$

where the $\lambda'_{i,1}$ denotes the maximum singular value after modulation.

3.2.5 Generate stego image

Based on the maximum singular value $\lambda'_{i,1}$, we firstly reconstructed the $\mathbf{M}_i$ according to (5), and then then inverse DCT is performed on each 8 × 8 block. Finally, inverse NSST is performed and the stego image is generated.

That is to say, the robust element $\lambda'_{i,1}$ carries the stego element. For the robust elements can resist lossy JPEG compression, it is more likely to get the correct maximum singular values after the stego image is compressed. Then, the corresponding correct stego elements can be got and the correct secret message will be extracted using STCs.

3.2.6 Determine quantization step q

For the above procedure for message embedding, the quantization step q is an important parameter. In (14), the stego element y_i is embedded by modulating the maximum singular

value $\lambda_{i,1}$, and the quantization step q determines the steganography robustness. The large quantization step q means the good robustness, however, the corresponding embedding change is also large and the anti-detection capability will be weakened. Therefore, it is necessary to determine an appropriate quantization step to achieve the balance between steganography robustness and detection resistance.

For a cover image, the determination of quantization step q is shown in Fig. 5. First, the threshold of error rate T_{ER} is given according to the robustness requirements for steganography. Then, an initial value of quantization step q is set and the stego image is generated. Finally, the embedded messages are extracted from the stego image which has been compressed, and the error rate ER is counted. If $ER < T_{ER}$, then the current q is the final quantization step, otherwise the q is increased and the above process continues until $ER < T_{ER}$ is satisfied. Similar to Fig. 3, the message extraction error rate will reduce rapidly with the increment of quantization step q.

According to the Fig. 5, it can be seen that the quantization step q is determined through an iterative process. In other words, for a cover image, the appropriate quantization step q can be determined by performing secret message embedding and extracting iteratively and increasing the q with a fixed step size until the error rate of the extracted secret message equal to zero or satisfactory. Therefore, this process is relatively time-consuming. In addition, it should be noticed that the appropriate quantization step q is changeable with cover image.

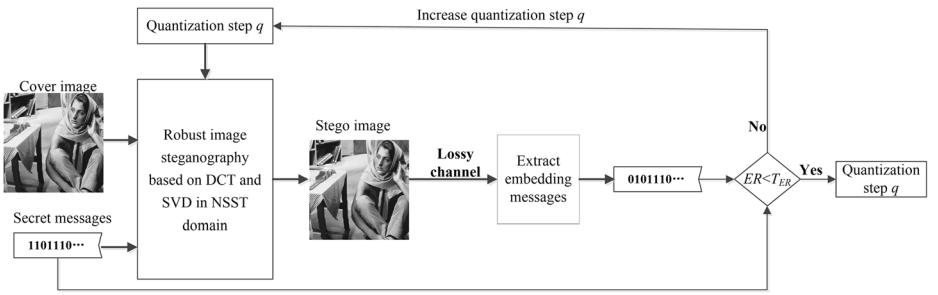

Fig. 5 procedure for determining quantization step q

All above, the embedding process of the secret message is described in Algorithm 1 in details.

Algorithm 1: Embedding algorithm	
Input:	Cover image $\mathbf{I}_c$, message $\mathbf{m}$, initial quantization step q_0, threshold T_{ER}, direction number D of NSST, the upper bound q_{max} of quantization step.
Output:	Stego image $\mathbf{I}_s$.
Step. 1:	The JPEG image is decompressed to spatial domain.
Step. 2:	The decompressed JPEG image is decomposed by NSST with single scale and D directions.
Step. 3:	The low frequency subband is divided into nonoverlapping 8×8 blocks.
Step. 4:	DCT is performed on each 8×8 block and the 6×6 matrix is constructed using the DCT coefficients in low and middle frequency domain.
Step. 5:	SVD is performed for each 6×6 matrix and the maximum singular values are got.
Step. 6:	The quantization step q is determined according to Fig. 5.
Step. 7:	The cover elements $\mathbf{x} = (x_1, x_2, \cdots, x_N)$ are extracted according to (8).
Step. 8:	The embedding cost of the cover element is computed according to (9), (10) and (11).
Step. 9:	The secret message is encoded by RS code.
Step. 10:	According to the number of the encoded secret message, the same number of cover elements are selected randomly from $\mathbf{x}$. Then, the stego elements are generated by embedding the encoded secret message based on STCs.
Step. 11:	The stego elements are embedded according to (14).
Step. 12:	All the 8×8 blocks are reconstructed by performing inverse SVD and DCT based on the modulated maximum singular values.
Step. 13:	The stego image is got by inverse NSST transform.
Step. 14:	**Return** stego image $\mathbf{I}_s$**.**

According to the above embedding process, it can be seen that the time consumption of the Algorithm 1 mainly includes cover image decomposition using NSST, the DCT on the low frequency subbands, SVD on the 6 × 6 matrices, the message embedding by STCs and the operations for image reconstruction to get the stego image. Therefore, the time consumption is relatively larger than the algorithm in [26].

3.3 Message extracting procedure

As shown in Fig. 4, for message extraction, the stego object $\mathbf{y} = (y_1, y_2, \cdots, y_N)$ should be extracted firstly and then the embedded messages can be extracted by STCs and RS decoder. According to (14), the following laws can be found,

if $\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor$ $\left\lfloor \frac{\lambda_{k,1}}{q} \right\rfloor$ is odd number and $y_i = 0$, then $\left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + 0 \right\rfloor, 2 \right) \right)$ is even number;

if $\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor$ is odd number and $y_i = 1$, then $\left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + 1 \right\rfloor, 2 \right) \right)$ is odd number;

if $\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor$ is even number and $y_i = 0$, then $\left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + 0 \right\rfloor, 2 \right) \right)$ is even number;

if $\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor$ is even number and $y_i = 1$, then $\left(\left\lfloor \frac{\lambda_{i,1}}{q} \right\rfloor + mod\left(\left\lfloor \frac{\lambda_{i,1}}{q} + 1 \right\rfloor, 2 \right) \right)$ is odd number.

In other words, the maximum singular value $\lambda_{i,1}$ is an even number when the embedded message bit is 0 while $\lambda'_{i,1}$ is an old number when the embedded message bit is 1. Therefore, the stego elements can be extracted by (15) as follow:

$$y_i = mod\left(round\left(\lambda'_{i,1}/q \right), 2 \right). \tag{15}$$

where the $\lambda''_{i,1}$ is the maximum singular value extracted from the compressed JPEG stego image and the value of quantization step q is same to (14).

The detailed extraction process of secret message is described in Algorithm 2.

Algorithm 2: Extracting algorithm	
Input:	Stego image $\mathbf{I}_s$, quantization step $\boldsymbol{q}$, direction number D of NSST.
Output:	message $\mathbf{m}$.
Step. 1:	The stego JPEG image is decompressed to spatial domain.
Step. 2:	The decompressed JPEG image is decomposed by NSST with single-scale and D directions.
Step. 3:	The low-pass subband is divided into nonoverlapping 8×8 blocks.
Step. 4:	For each block, the 6×6 matrix is constructed using the DCT coefficients in low and middle frequency domain.
Step. 5:	SVD is performed on each 6×6 matrix and the corresponding maximum singular values are got.
Step. 6:	The stego elements are extracted according to (15).
Step. 7:	The encoded secret message is extracted using STCs.
Step. 8:	The secret message is got by RS decoder.
Step. 9:	**Return** secret message $\mathbf{m}$.

4 Experimental results and analysis

4.1 Experimental settings

In the experiments, 10,000 grayscale images from BOSSbase1.01 [2] were used to evaluate the robustness and anti-detection capability of the proposed JPEG steganography algorithm. The image size is 512 × 512 and image format is PGM. First, the robustness of the proposed steganography algorithm against JPEG compression attack is compared with the other robust image steganography algorithms [26]. Second, the anti-detection capability of the proposed steganography algorithm is evaluated by two typical steganalysis features [10, 15] and ensemble classifier [13]. Finally, the robustness of the proposed steganography algorithm against WeChat compression is presented. The parameter of RS code is (31, 19).

4.2 Robustness against JPEG compression

In this experiment, the 10,000 grayscale images with PGM format are performed JPEG compression with QF 85 to generate the cover images. Then, the corresponding stego images are generated by the proposed steganography algorithm, MREAS-P_S and MREAS-P_J [26] respectively. The single scale NSST is performed for each cover image and the number of directions is 16. The quantization step q of the proposed steganography algorithm is determined according to Fig. 5 where the extraction error rate threshold T_{ER} is set to 0, q_{max} = 80 and the lossy channel is JPEG compression with QF 65. For size of cover image is 512 × 512, the maximum embedding payload is 4096 bits. Moreover, for robust steganography, the anti-detection capability is more important than embedding payload. Therefore, the payload is set to 0.001, 0.002, 0.003, 0.004, 0.005, 0.006, 0.007, 0.008, 0.009 and 0.01 bpnzAC (bit per non-zero AC DCT coefficient) respectively. Then, for each robust steganography algorithm, we have one group of cover images and ten groups of stego images. Next, the stego images with different payloads are performed JPEG compression with QF 65, 75, 85 and 95 respectively. The embedding message is extracted from the compressed JPEG stego image according to

Table 1 Average extraction error rates of three robust steganography algorithms for all images in BOSSbase1.01. (**×10⁻³**)

QF	Algorithm	Payload (bpnzAC)									
		0.001	0.002	0.003	0.004	0.005	0.006	0.007	0.008	0.009	0.01
65	**Proposed**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	MREAS-P_S	185	186	186	187	188	188	189	190	191	191
	MREAS-P_J	180	180	181	181	181	181	180	181	181	181
75	**Proposed**	4.3	4.5	5.1	5.6	6.3	6.2	7.6	7.9	8.5	9.3
	MREAS-P_S	8.5	9.0	9.1	8.9	8.6	8.9	9.1	9.2	9.4	9.6
	MREAS-P_J	**0.48**	**0.49**	**0.49**	**0.56**	**0.55**	**0.51**	**0.55**	**0.53**	**0.57**	**0.56**
85	**Proposed**	**0.01**	**0.04**	**0.07**	**0.10**	**0.11**	**0.11**	**0.13**	**0.13**	**0.14**	**0.14**
	MREAS-P_S	0.40	0.38	0.37	0.42	0.37	0.43	0.42	0.47	0.48	0.46
	MREAS-P_J	0.05	0.06	0.10	0.12	0.11	0.12	0.15	0.15	0.14	0.14
95	**Proposed**	**0**	**0**	**0.02**	**0.05**	**0.07**	**0.08**	**0.10**	**0.10**	**0.11**	**0.11**
	MREAS-P_S	0.29	0.25	0.26	0.30	0.27	0.30	0.32	0.38	0.35	0.34
	MREAS-P_J	0.06	0.06	0.07	0.11	0.10	0.10	0.10	0.13	0.11	0.11

The bold entries denote the good results

Algorithm 2. The average extraction error rates of the different robust steganography algorithms are shown in Table 1.

According to the average extraction error rates shown in Table 1, it can be seen that the proposed steganography algorithm has achieve the competitive robustness. As shown in Table 1, for MREAS-P_S and MREAS-P_J, the average extraction error rates are low when the QFs of JPEG recompression are 85 and 95. However, the extraction error rates become high when the QF of JPEG recompression is 65 which means strong attack. In addition, in this experiment, the QFs of JPEG compression attack are 65, 75, 85 and 95 respectively and the QF 65 means the strongest compression attack. Then, the quantization step q for each image is also determined when the QF of compression attack is assumed to be 65. In other words, we do not choose the quantization step q for QFs 75, 85 and 95. We want to know the changes of the extraction error rates when the real QF of JPEG compression attack is not consistent with the assumed value. From the experimental results in Table 1, it can be seen that the extraction error rate is lowest when QF is 65. This is because the real QF of JPEG compression attack is consistent with the assumed value. For other QFs, we can find that the extraction error rates will decrease with the increasement of QFs and this is because that the higher QF means weaker compression attack.

As we know, the complex images often have strong resistance to the detection. Therefore, we should select some images with complex texture structure as the cover images. Here, we will evaluate the steganography robustness of the complex images. First, the images are decomposed by NNST with single scale and 16 directions and the most complex 2000 images are selected according to the energy values of shearlet coefficients from all the high frequency subbands. Then, the 2000 image are used as cover images and the corresponding stego images are generated. Finally, the stego images are attacked by JPEG recompression and the average extraction error rates are shown in Table 2.

According to the extraction errors shown in Table 2, we can find that the proposed steganography algorithm also can achieve the competitive robustness for the complex images. Moreover, compared with results in Table 1, the extraction error rates increased slightly. This is because that the JPEG recompression has larger impact for the complex images.

Table 2 Average extraction error rates of three robust steganography algorithms for complex images in BOSSbase1.01. ($\times\mathbf{10^{-3}}$)

QF	Algorithm	Payload (bpnzAC)									
		0.001	0.002	0.003	0.004	0.005	0.006	0.007	0.008	0.009	0.01
65	**Proposed**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	MREAS-P_S	248	249	251	253	255	257	257	258	259	259
	MREAS-P_J	245	248	247	250	249	250	249	250	251	251
75	**Proposed**	8.5	8.4	9.1	9.0	10.4	11.2	11.6	12.3	12.7	13.3
	MREAS-P_S	12.3	12.5	13.1	13.3	13.0	13.0	13.1	14.0	14.4	14.4
	MREAS-P_J	**0.92**	**1.00**	**1.20**	**1.50**	**1.50**	**1.40**	**1.30**	**1.30**	**1.40**	**1.40**
85	**Proposed**	**0.06**	**0.08**	**0.18**	**0.23**	**0.29**	**0.35**	**0.41**	**0.41**	**0.43**	**0.45**
	MREAS-P_S	0.88	1.00	1.10	1.30	1.30	1.40	1.30	1.50	1.50	1.50
	MREAS-P_J	0.13	0.12	0.28	0.36	0.44	0.43	0.50	0.45	0.49	0.49
95	**Proposed**	**0.07**	**0.10**	**0.15**	**0.26**	**0.29**	**0.33**	**0.32**	**0.35**	**0.37**	**0.37**
	MREAS-P_S	0.60	0.56	0.75	0.91	0.88	0.99	0.92	1.10	0.98	0.98
	MREAS-P_J	0.13	0.12	0.25	0.42	0.47	0.40	0.39	0.47	0.39	0.39

The bold entries denote the good results

4.3 Detection resistance against steganalysis

In this experiment, the anti-detection capability of the proposed robust steganography algorithm is compared with the MREAS-P$_S$ and MREAS-P$_J$ [26]. The steganalysis features are CC-PEV [15] with 548 dimensions and DCTR [10] with 8000 dimensions. The ensemble classifier [13] is trained by the steganalysis feature and used as the detector. The ratio of training images 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 P_E is averaged over ten random image database splits.

In Fig. 6, the detection error rate P_E are given for all the cover images and the corresponding stego images. According to the detection performances, it can be seen that the proposed steganography has stronger detection resistance than MREAS-P$_S$ and MREAS-P$_J$. On the one hand, this is because that the robust embedding domain is constructed in the low frequency subband and the image high-frequency features such as texture, edge have been preserved. On the other hand, the quantization step q of each cover image is determined according to the threshold of extraction error rate, therefore the corresponding embedding changes caused by the quantization operation is relatively small than the embedding changes when a large quantization step q is fixed for all the cover images.

In Fig. 7, the detect errors are presented for the most complex 2000 images in BOSSbase1.01. The image complexity is also measured using energy value of shearlet coefficients in all the high frequency subbands. According to the experimental results shown in Figs. 6 and 7, it can be seen that the anti-detection capability of the 2000 complex images is obviously stronger than the anti-detection capability of all the images in BOSSbase1.01. Moreover, for complex images, the proposed steganography also has stronger detection resistance than MREAS-P$_S$ and MREAS-P$_J$.

In Fig. 8, the detect errors are presented for the simplest 2000 images from BOSSbase1.01. It can be seen that the anti-detection capability of the simple images is obviously weaker in contrast to the complex images. Therefore, we should select the image with complex texture

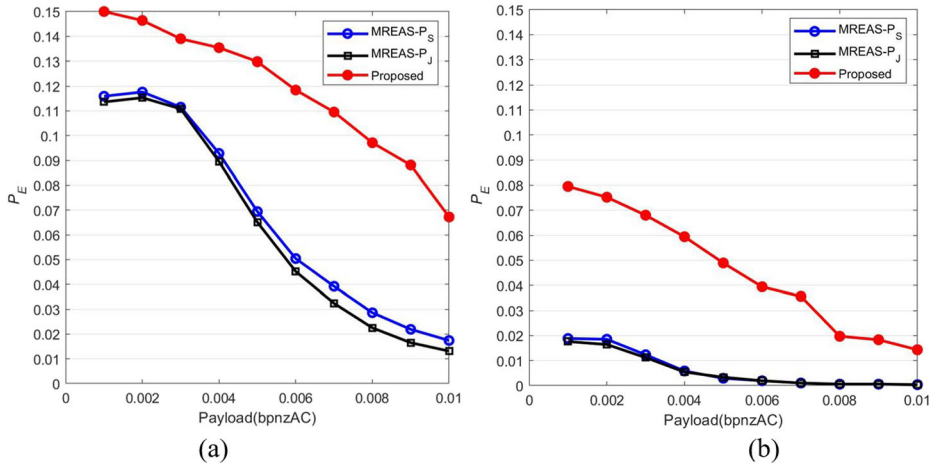

Fig. 6 Comparisons of detection error rates P_E of two steganalysis features for stego images generated from all images in BOSSbase1.01. **a** CC-PEV feature, **b** DCTR feature

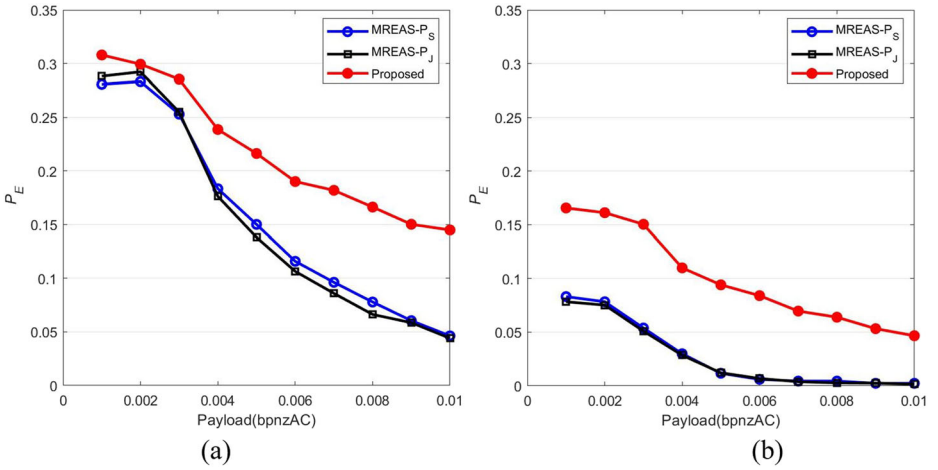

Fig. 7 Comparisons of detection error rates P_E of two steganalysis features for stego image generated from 2000 complex images in BOSSbase1.01. **a** CC-PEV feature, **b** DCTR feature

structure as the cover image for convert communication. Moreover, for simple images, the proposed algorithm also has stronger detection resistance than MREAS-P_S and MREAS-P_J.

4.4 Application in WeChat platform

In this experiment, the robustness of the proposed steganography algorithm against WeChat compression is test. As we know, WeChat is a widely used instant communication tool which allows the users to share their images. However, to reduce transmission and storage costs, the uploaded image will be compressed. In particular, the compression algorithm of WeChat is unknown for users. We select two cover images from BOSSbase1.01 which are converted to JPEG images with QF85 and are shown in Fig. 9.

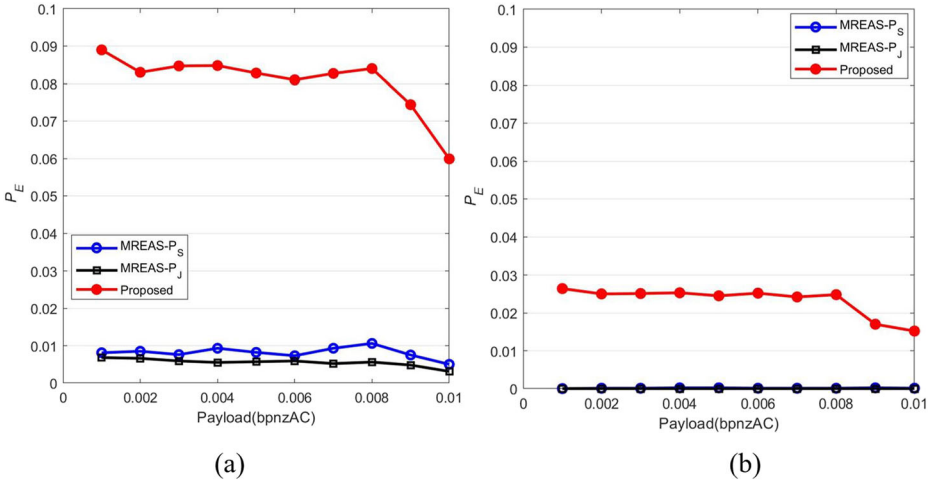

Fig. 8 Comparisons of detection error rates P_E of two steganalysis features for stego image generated from 2000 simple images in BOSSbase1.01. **a** CC-PEV feature, **b** DCTR feature

(a) (b)

Fig. 9 Cover image for covert communication by WeChat. **a** '8.jpg' in BOSSbase1.01 and **b** '4226.jpg'

First, the stego images are generated with different quantization q and the payload is 0.01 bpnzAC. Then, the stego images are posted on WeChat moment. Finally, the stego images are downloaded from the WeChat moment and the embedded messages are extracted from the downloaded stego image. The extraction error rates are shown in Fig. 10.

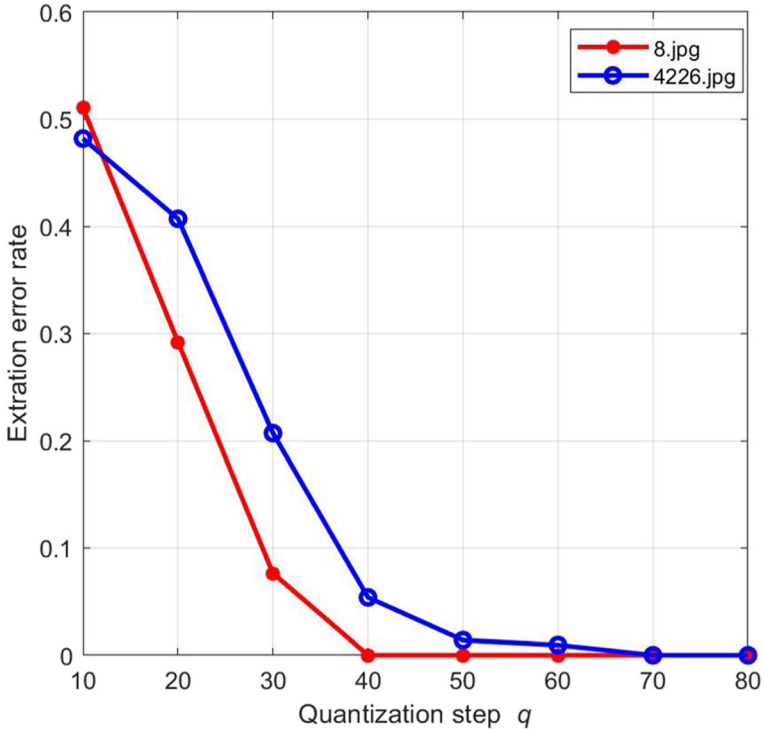

Fig. 10 Extraction error rate of the stego images after WeChat channel compression

In Fig. 10, it can be seen that the steg images can resist WeChat compression channel by selection appropriate quantization step q. It should be noticed that large quantization step means good robustness while the corresponding quantization operations will bring the large embedding changes for cover image. Moreover, for different cover images, the quantization steps for correct message extraction are also different. Therefore, we need to select the appropriate quantization step q for different cover images.

5 Conclusions and future work

Robust image steganography is an important technique for covert communication by lossy public channels. In this paper, a robust JPEG steganography algorithm is proposed based on DCT and SVD in NSST domain. The experimental results show the proposed algorithm can achieve competitive robustness and detection resistance in contrast to the stat-of-the-art techniques. This is because that the maximum singular value has strong stability and QIM can further eliminate some errors. Moreover, embedding changes in low frequency subband can achieve stronger detection resistance because the texture and edge features of stego image can get better maintained. Furthermore, the quantization step is determined for each cover image according to the threshold of extraction error rate, therefore, the stronger anti-detection capability can be achieved in contrast to the fixed quantization step for all the cover images.

In addition, we should notice that the anti-detection capability of the robust image steganography is relatively weak when the detection is performed by the classifier trained by the original cover image and the corresponding stego image. This is because that the embedding changes of robust steganography is larger than the changes of non-robust steganography such as J-UNWARD, UED. In other words, the large embedding changes is used to achieve the robustness. In the future, we will study the construction of robust embedding domain which can led to the stronger robustness and anti-detection capability. Furthermore, the robustness of other steganography method such as Linguistic Steganography [20, 21] and coverless image steganography [4, 14] also need to be studied.

Acknowledgments This work was supported by the National Natural Science Foundation of China (No. 61872448, U1804263) and the Natural Science Basic Research Plan in Shanxi Province of China (No. 2021JQ-379).

References

1. Bao P, Ma X (2005) Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans Circ Syst Video Technol 15(1):96–102
2. Bas P, Filler T, Pevný T (2011) Break Our Steganographic System: The Ins and Outs of Organizing BOSS. In: Proceedings of the 13th International workshop on Information Hiding, Springer, pp 59–70
3. Chen B, Wornell G (2001) Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans Inf Theory 47(4):1423–1443
4. Chen X, Zhang Z, Qiu A, Xia Z, Xiong N (2021) A novel coverless steganography method based on image selection and StarGAN. IEEE Trans Netw Sci Eng 9:219–230. https://doi.org/10.1109/TNSE.2020.3041529

5. Das R, Baykara M, Tuna G (2019) A novel approach to steganography: enhanced least significant bit substitution algorithm integrated with self-determining encryption feature. Comput Syst Sci Eng 34(1):23–32
6. Easley G, Labate D, Lim W (2008) Sparse directional image representations using the discrete shearlet transform. Appl Comput Harmon Anal 25(1):25–46
7. Filler T, Judas J, Fridrich J (2011) Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans Inf Forensic Secur 6(3):920–935
8. Guo L, Ni J, Shi YQ (2014) Uniform embedding for efficient JPEG steganography. IEEE Trans Inf Forensic Secur 9(5):814–825
9. Holub V, Fridrich J (2013) Digital image steganography using universal distortion. In: Proceedings of the first ACM workshop on Information hiding and multimedia security, ACM, pp. 59–68
10. Holub V, Fridrich J (2015) Low-complexity features for JPEG Steganalysis using Undecimated DCT. IEEE Trans Inf Forensic Secur 10(2):219–228
11. Kang X, Zhao F, Lin G, Chen Y (2018) A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimed Tools Appl 77(11):13197–13224
12. Ker A D, Bas P, Böhme R, et al (2013). Moving steganography and Steganalysis from the laboratory into the real world. In: Proceedings of the first ACM workshop on Information hiding and multimedia security, ACM, pp. 45–58.
13. Kodovsky J, Fridrich J, Holub V (2012) Ensemble classifiers for steganalysis of digital media. IEEE Trans Inf Forensic Secur 7(2):432–444
14. Luo Y, Qin J, Xiang X, Tan Y (2021) Coverless image steganography based on multi-object recognition. IEEE Trans Circ Syst Video Technol 31:2779–2791. https://doi.org/10.1109/TCSVT.2020.3033945
15. Pevny T, Fridrich J (2008) Multiclass detector of current steganographic methods for JPEG format. IEEE Tran Inf Forensic Secur 3(4):635–650
16. Qian Z, Zhou H, Zhang W, Zhang X (2016) Robust steganography using texture synthesis. In: Proceedings of 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Springer, pp. 25–33
17. Tao J, Li S, Zhang X, Wang Z (2019) Towards robust image steganography. IEEE Trans Circ Syst Video Technol 29(2):594–600
18. Tian C, Wen R, Zou W, Gong L (2020) Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain. Multimed Tools Appl 79(11):7515–7541
19. Wang X, Liu Y, Xu H, Wang A, Yang H (2016) Blind optimum detector for robust image watermarking in nonsubsampled shearlet domain. Inf Sci 372:634–654
20. Xiang L, Yang S, Liu Y, Li Q, Zhu C (2020) Novel linguistic steganography based on character-level text generation. Mathematics 8(9):1558
21. Yang Z, Zhang S, Hu Y, Hu Z, Huang Y (2021) VAE-Stega: linguistic steganography based on Variational auto-encoder. IEEE Trans Inf Forensic Secur 16:880–895
22. Yi S, Labate D, Easley G, Krim H (2009) A Shearlet approach to edge analysis and detection. IEEE Trans Image Process 18(5):929–941
23. Yu X, Chen K, Wang Y, Li W, Zhang W, Yu N (2020) Robust adaptive steganography based on generalized dither modulation and expanded embedding domain. Signal Process 168:1–12
24. Zhang Y, Luo X, Yang C, Ye D, Liu F. (2015) A JPEG compression resistant adaptive steganography based on relative relationship between DCT coefficients. In: Proceedings of the 10th international conference on availability, Reliability and Security, IEEE, pp. 461–46.
25. Zhang Y, Zhu X, Qin C, Yang C, Luo X (2018) Dither modulation based adaptive steganography resisting JPEG compression and statistic detection. Multimed Tools Appl 77(14):17913–17935
26. Zhang Y, Luo X, Guo Y, Qin C, Liu F (2020) Multiple robustness enhancements for image adaptive steganography in Lossy channels. IEEE Trans Circ Syst Video Technol 30(8):2750–2764
27. Zhao Z, Guan Q, Zhang H, Zhao X (2019) Improving the robustness of adaptive steganographic algorithms based on transport channel matching. IEEE Trans Inf Forensic Secur 14(7):1843–1856