# Robust JPEG Image Steganography Based on SVD and QIM in Stationary Wavelet Domain

Zhiguo Wang[1(✉)], Zhiyuan Li[2], Xiaofeng Song[1], and Yi Zhang[3]

[1] National University of Defense Technology, Xi'an 710106, China
[2] Geely University, Chengdu 641423, China
[3] Special Police College, Beijing 102211, China

**Abstract.** Robust image steganography technology is important for covert communication under lossy network environment where the images are often compressed. To resist the lossy image compression, the robust embedding domain should be constructed firstly and then the secret messages are embedded by special steganography code. In this paper, by taking the advantages of stationary wavelet transform, SVD and QIM, a robust JPEG image steganography algorithm is proposed based on SVD and QIM in stationary wavelet domain. First, the framework of the proposed robust JPEG steganography algorithm is given. Then, the embedding distortion of cover element is defined. Finally, the message embedding and extraction procedure are described in the details. The experimental results show that the proposed robust steganography algorithm has competitive robustness and detection resistance.

**Keywords:** JPEG · Steganography · Robustness · Wavelet · QIM · SVD

## 1 Introduction

Digital steganography is a kind of covert communication technology in which secret messages are hidden in public digital carriers and transmitted through open channels [1]. For the behavior of covert communication is concealed, steganography is very deceptive and often used for the important message transmission in unsafe public network channel. Due to the extensive use of digital images, image is one of the most widely used carrier. Researchers have proposed many image steganography algorithms with high anti-detection ability [2, 3], which greatly improves the security of covert communication. In recent years, WeChat, microblog and other social media are rising rapidly. These social platforms transmit and share a large amount of image data every day, which provides a huge amount of cover images for covert communication by image steganography, which greatly increases the difficulty of communication behavior detection. However, in order to save bandwidth and processing costs, and speed up image loading speed, most social network channels will compress and scale image data, which makes the current image steganography algorithm for lossless processing difficult to apply. The design of image steganography algorithm with lossy processing resistance and anti-detection ability has become the research hotspot in the field of information hiding.


X. Sun et al. (Eds.): ICAIS 2021, CCIS 1424, pp. 551–560, 2021.
https://doi.org/10.1007/978-3-030-78621-2_46

Image steganography for lossy network channel requires steganography to be robust to lossy processing such as compression, cutting, scaling and so on, and at the same time, the anti-detection ability should be considered. Compared with adaptive steganography with high anti-detection ability, robust steganography has attracted less attention in the previous years. However, in the recent years, a series of robust image steganography algorithms have been proposed. In [4], a robust JPEG steganography algorithm is proposed based on DCT coefficient correlation. In [5], a robust image steganography algorithm is proposed based on dither modulation. In [6], a robust image steganography algorithm is proposed based on texture synthesis. In [7], Zhao et al. proposed a robust and adaptive JPEG image steganography algorithm based on transmission channel matching. In [8], Tao et al. proposed a robust JPEG steganography by generating the 'intermediate image' that is just the stego image after JPEG compression with special quality factor. In [9], Yu et al. proposed a robust image steganography algorithm based on generalized dither modulation and embedding domain expansion. In [10], Zhang et al. proposed an adaptive steganography algorithm with multiple robustness enhancements, which uses the difference of inter-block DCT coefficients to embed the secret messages. Although these algorithms can improve the extraction accuracy of the embedded secret messages to a certain extent. However, they are generally weak against detection, and how to improve the detection resistance of image robust steganography needs to be studied.

The wavelet transform has good time-frequency analysis characteristics and has a wide range of applications in image analysis, information hiding and other fields. In image steganography, wavelet transform is widely used, for example, in the design of adaptive steganography algorithms J-UNIWARD [2], the embedding distortion is defined according to the ratio between the amount of change of image wavelet coefficients and the image wavelet coefficients, which can limit the embedding change to the complex texture area of the image, and achieve good anti-detection ability. In terms of robust image watermarking, wavelet domain watermarking algorithm is usually more robust than spatial domain watermarking algorithm [11]. At the same time, the singular value of image has good characteristics in describing the distribution characteristics of image pixel matrix, which can better represent the important basic structure of image data. The singular value of image pixel matrix represents the relationship between pixels rather than visual features [12]. The change of singular value will not cause large image distortion. Moreover, the singular value of the matrix has good stability, and will not fluctuate with the disturbance of the matrix. Therefore, it has been widely used in robust image watermarking.

Considering the characteristics of image wavelet transform and SVD, the robust embedding domain is constructed by using SVD in image wavelet domain. Because the discrete orthogonal wavelet transform will be sampled after image filtering, and it does not have translation invariance. Here, the image is decomposed by using the translation invariant stationary wavelet transform. The size of the low frequency and high frequency subband is the same as the original image after the stationary wavelet transform. Because the lossy network channel is mainly used to change the high frequency information of the image when compressing the image, the low frequency subband after the image stationary wavelet transform is used to embed the message.

The procedure of the proposed robust JPEG steganography algorithm can be described briefly as follows. First, the image is transformed by stationary wavelet transform to get a low frequency subband and three high-frequency subbands. Since the lossy processing has a great influence on the high frequency subband, the low-frequency subband is divided into non overlapping $8 \times 8$ blocks, and the corresponding singular values are obtained by performing SVD for each block. Then, taking advantage of the good stability of the maximum singular value, the corresponding message embedding and extraction method are proposed. Second, the embedding distortion function is defined according to the texture complexity of blocks, and the secret message embedding is realized by STCs coding [13] and the stego elements are got. Finally, the QIM(quantization index modulation) method is used to embed the stego elements to obtain the final stego image.

## 2 Proposed Robust JPEG Steganography Algorithm

### 2.1 Overall Framework

The framework of the proposed robust JPEG steganography algorithm is shown in Fig. 1. According to Fig. 1, it can be seen that the proposed algorithm includes robust message embedding procedure and the corresponding message extraction procedure.

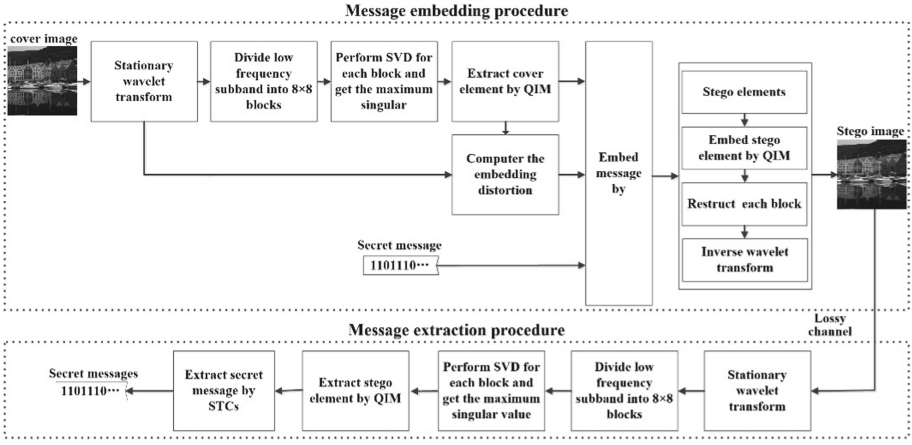



**Fig. 1.** Framework of the proposed steganography algorithm.

For secret message embedding, first, one-level stationary wavelet transform is performed for the cover image and the low-pass subband is used for embedding domain construction, and then the low-pass subband is divided into $8 \times 8$ blocks and the maximum singular value of each block is generated; secondly, the cover elements are extracted by performing QIM for the maximum singular values and the embedding distortion of each cover element is measured according to the embedding changes and texture complexity of block; thirdly, the secret messages are embedded by STCs and the correspond

stego elements are obtained; finally, the stego elements are embedded by performing QIM for the maximum singular values of the $8 \times 8$ blocks, and then each block is reconstructed using the modified maximum singular values and the inverse stationary wavelet transform is performed to get the stego image.

For secret message extraction, firstly, the one-level stationary wavelet transform is also performed for the received stego image and the low-pass subband is divided into $8 \times 8$ blocks; secondly, the maximum singular values of all blocks are generated and the stego elements are extracted by performing QIM for the maximum singular values; finally, the secret messages are extracted by STCs.

According to the above descriptions, it can be seen that the definition of the embedding distortion function, the message embedding method and the message extraction method are crucial for the proposed robust image steganography algorithms. Therefore, they are introduced in details as follows.

### 2.2 Embedding Distortion Function

According to the framework shown in Fig. 1, it can be seen that one cover element can be extracted from one $8 \times 8$ block. And the embedding distortion of the cover element should be related with the anti-detection ability of stego image. As we know, the embedding changes occur in the complex texture region are difficult to be detected. Therefore, the embedding distortion of cover element extracted from the $8 \times 8$ block with complex texture should be small and the embedding distortion of cover element extracted from smooth block should be large. Because the energy value of image wavelet coefficients can reflect the texture complexity of the image blocks. Therefore, the embedding cost of $d_i$ can be is defined according to Eq. (1),

$$d_k = \frac{1}{\sum_{l=1}^{3} \sum_{i=1}^{8} \sum_{j=1}^{8} |f_l(k, i, j)|} \tag{1}$$

where $f_l(k, i, j)$ denotes the $(i, j)$-th wavelet coefficient of the corresponding blocks in $l$-th high-pass subband.

### 2.3 Message Embedding Procedure

Suppose the image size of the cover image $\mathbf{I}$ is $m \times n$, therefore, after stationary wavelet transform for the cover image, the size of the low-pass subband is also $m \times n$. The detailed message embedding procedure can be described as follows:

(1) The stationary wavelet transform is performed for the cover image $\mathbf{I}$ and the low-pass subband $\mathbf{L}$ is got.
(2) The low-pass subband $\mathbf{L}$ is divided into $8 \times 8$ blocks $\mathbf{B_{i,j}}$, $1 \le k \le u_B$, $1 \le l \le v_B$, $u_B = \lfloor m/8 \rfloor$, $v_B = \lfloor n/8 \rfloor$, $\lfloor \bullet \rfloor$ indicates the floor integer of $\bullet$.
(3) SVD is performed for each block $\mathbf{B_{i,j}}$ and the corresponding maximum singular value set $\mathbf{S} = \{s_i | 1 \le i \le u_B \times v_B\}$ are obtained.

(4) Suppose the secrete message sequence $\mathbf{m} = \{m_i | 1 \leq i \leq u_B \times v_B\}$, the quantization step is $T$, then the cover element set $\mathbf{X} = \{x_i | 1 \leq i \leq u_B \times v_B\}$ can be extracted according to Eq. (2),

$$x_i = mod(\lfloor s_i / T \rfloor, 2) \tag{2}$$

(5) The embedding distortion of each cover element $x_i$ is computed according to Eq. (1).
(6) The secrete message sequence $\mathbf{m}$ is embedded using STCs and the corresponding stego element set $\mathbf{Y} = \{y_i | 1 \leq i \leq u_B \times v_B\}$ can be obtained.
(7) Each stego element $y_i$ is embedded by perform QIM for maximum singular value $s_i$ according to the Eq. (3),

$$s_i^{'} = \begin{cases} \left(\left\lfloor \frac{s_i}{T} \right\rfloor + \frac{3}{2}\right) \times T, & if \ mod\left(\left(\left\lfloor \frac{s_i}{T} \right\rfloor + y_i\right), 2\right) = 1 \\ \left(\left\lfloor \frac{s_i}{T} \right\rfloor + \frac{1}{2}\right) \times T, & else \quad otherwise \end{cases} \tag{3}$$

(8) Each block is reconstructed by performing inverse SVD based on the maximum singular value $s_i^{'}$.
(9) Inverse stationary wavelet transform is performed based on the modified low-pass and the original three high-pass subbands, and then the stego image is generated.

### 2.4 Message Extracting

The receiver can get the stego image which may be applied the lossy operation by the public network channel. To extract the embedding secret messages, the following steps should be performed.

(1) Stationary wavelet transform is performed for the stego image and the low-pass subband is obtained.
(2) The low-pass subband is divided into $8 \times 8$ blocks and the SVD is performed for each block.
(3) According to Eq. (4), the stego elements are extracted by performing the QIM for all the maximum singular values extracted from the $8 \times 8$ blocks.

$$y_i^{'} = mod(\left\lfloor s_i^{'} / T \right\rfloor, 2) \tag{4}$$

where $s_i^{'}$ denotes the maximum singular value of $i$-th $8 \times 8$ block of the received stego image, and $y_i^{'}$ denotes the corresponding stego element.

(4) The secret messages are extracted by performing STCs for the extracted steg elements.

## 3 Experimental Results and Analysis

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. For the robustness and anti-detection experiments, the 10000 Gy-scale images from BOSSbase1.01 [14] 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).

### 3.1 Robustness Experiment

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 UEDR-P [8], MREAS-$P_S$ [10] and MREAS-$P_J$ [10] and. 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.

After the stego images are generated, the JPEG recompression attack is applied to the steg images. The QF of JPEG recompression is 65, 75, 85 and 95 respectively. The parameter T in Eq. (2), (3) and (4) is set according to requirement for extraction error rate. In other words, the low extraction error rate means large $T$. For UEDR-P, the assumed QF of JPEG compression attack is 85. The other parameters of the robust steganography algorithms used for comparison are all set as the default values. The average extraction error rates of the compressed stego images are shown in Table 1.

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. For UEDR-P, the average extraction error rate is 0 only when the QF of JPEG compression is same to the assumed QF, and the extraction error rates are very high when the QFs are different with the assumed QF.

In Table 2, the average extraction error rates are given for all the 10000 images in BOSSbase1.01. According to the experimental results in Table 1, it can be seen that the extraction error rates decrease in contrast to the 2000 complex images. This is because that the JPEG compression has larger impact for complex images than for simple images. However, we should notice that the detect resistance of the simple images is often weak.

### 3.2 Detection Resistance Experiment

The detection resistance is important for robust image steganography. Although the UEDR-P has the strongest an-detection ability, it is robust only when the QF of JPEG

**Table 1.** Average extraction error rates of three robust steganography algorithms for the 2000 complex images in BOSSbase1.01. ($\times 10^{-3}$)

| QF | Algorithm | Payload (bpnzAC) | | | | |
|---|---|---|---|---|---|---|
| | | 0.001 | 0.002 | 0.003 | 0.004 | 0.005 |
| 65 | Proposed | **0.25** | **0.26** | **0.41** | **0.75** | **0.93** |
| | MREAS-P$_S$ | 248 | 249 | 251 | 253 | 255 |
| | MREAS-P$_J$ | 245 | 248 | 247 | 250 | 249 |
| | UEDR-P | 499 | 500 | 500 | 500 | 500 |
| 75 | Proposed | **0.74** | **0.77** | **0.89** | **1.45** | **1.30** |
| | 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 |
| | UEDR-P | 500 | 499 | 499 | 499 | 500 |
| 85 | Proposed | 0.09 | 0.09 | 0.22 | 0.35 | 0.63 |
| | 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** |
| | UEDR-P | **0** | **0** | **0** | **0** | **0** |
| 95 | Proposed | **0.09** | **0.09** | **0.15** | **0.32** | **0.45** |
| | 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 |
| | UEDR-P | 499 | 500 | 500 | 499 | 499 |

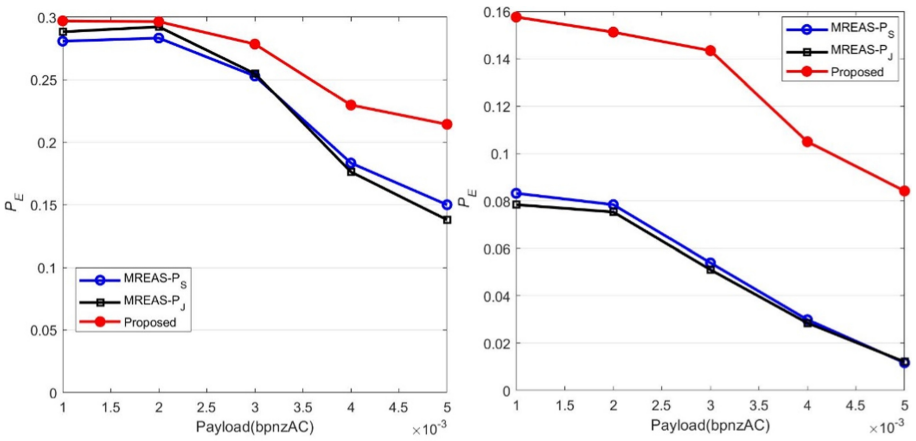
compression attack is known. Therefore, the proposed steganography algorithm is compared with MREAS-P$_s$ and MREAS-P$_J$ using CC-PEV [15] and DCTR [16] which are the typical steganalysis features.

First, the most complex 2000 images from BOSSbase1.01 are used to generate stego images. The payloads are from 0.001 to 0.005 bpnzAC. The ensemble classifier [17] 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 $P_E = min_{P_{\text{FA}}}(P_{\text{FA}} + P_{\text{MD}})/2$, where $P_{\text{FA}}$ denotes the false-alarm probabilities and $P_{\text{MD}}$ denotes the missed-detection probabilities. The value of $\overline{P}_E$ is averaged over ten random image database splits.

In Fig. 2, the detection error rate $\overline{P}_E$ of two steganalysis features are respectively shown for the three robust steganography algorithms when the stego images are generated by 2000 complex images from BOSSbase1.01. According to the detection performances, it can be seen that the proposed steganography has stronger detection resistance than MREAS-P$_S$ and MREAS-P$_J$. 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. Therefore, the stego image has stronger detection resistance. In addition, we should notice that the high-dimensional feature DCTR has better detection performances.

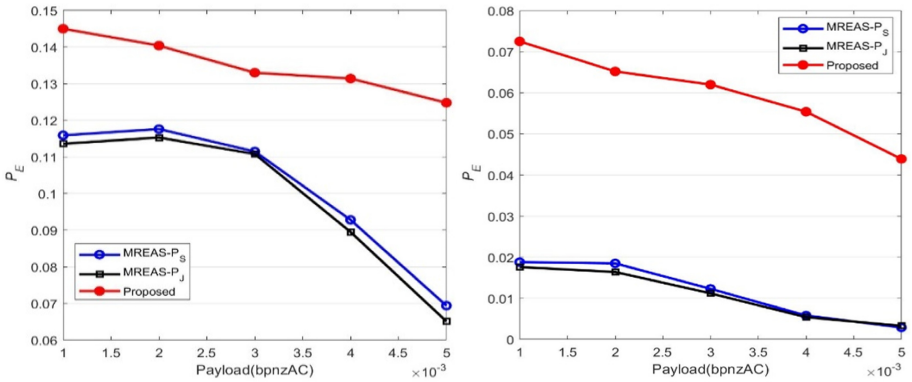
**Table 2.** Average extraction error rates of three robust steganography algorithms for all images in BOSSbase1.01. ($\times 10^{-3}$)

| QF | Algorithm | Payload (bpnzAC) | | | | |
|---|---|---|---|---|---|---|
| | | 0.001 | 0.002 | 0.003 | 0.004 | 0.005 |
| 65 | Proposed | **0.18** | **0.16** | **0.23** | **0.29** | **0.32** |
| | MREAS-P$_S$ | 185 | 186 | 186 | 187 | 188 |
| | MREAS-P$_J$ | 180 | 180 | 181 | 181 | 181 |
| | UEDR-P | 500 | 500 | 499 | 500 | 500 |
| 75 | Proposed | **0.28** | **0.30** | **0.32** | **0.37** | **0.39** |
| | MREAS-P$_S$ | 8.5 | 9.0 | 9.1 | 8.9 | 8.6 |
| | MREAS-P$_J$ | 0.48 | 0.49 | 0.49 | 0.56 | 0.55 |
| | UEDR-P | 500 | 499 | 499 | 500 | 500 |
| 85 | Proposed | 0.04 | 0.04 | 0.07 | 0.10 | 0.16 |
| | MREAS-P$_S$ | 0.40 | 0.38 | 0.37 | 0.42 | 0.37 |
| | MREAS-P$_J$ | 0.05 | 0.06 | 0.10 | 0.12 | **0.11** |
| | UEDR-P | **0** | **0** | **0** | **0** | **0** |
| 95 | Proposed | **0.03** | **0.05** | **0.05** | **0.06** | **0.10** |
| | MREAS-P$_S$ | 0.29 | 0.25 | 0.26 | 0.30 | 0.27 |
| | MREAS-P$_J$ | 0.06 | 0.06 | 0.07 | 0.11 | 0.10 |
| | UEDR-P | 499 | 500 | 500 | 499 | 500 |




(a) CC-PEV feature (b) DCTR feature

**Fig. 2.** Comparisons of detection error rates $\overline{P}_E$ of two steganalysis features for stego image generated from 2000 complex images in BOSSbase1.01.




(a) CC-PEV feature (b) DCTR feature

**Fig. 3.** Comparisons of detection error rates $\overline{P}_E$ of two steganalysis features for stego image generated from all the 10000 images in BOSSbase1.01.

In Fig. 3, the detected cover and stego images are all the 10000 images from BOSSbase1.01. Compared with the detection error rate $\overline{P}_E$ in Fig. 3, the detection error rates in Fig. 3 are relatively low. This is because that the detection for the complex images is more difficult.

## 4 Conclusion

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 SVD and QIM in wavelet domain. The experimental results show the proposed steganography algorithm can achieve competitive robustness and detection resistance in contrast to the stat-of-the-art techniques. This is because that the maximum singular values in wavelet domain have strong robustness. Moreover, QIM and embedding changes in low-pass subband can achieve stronger detection resistance because the texture and edge features of stego image can get better maintained.

In addition, we should notice that the detection resistance 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 non-robust steganography such as J-UNWARD. 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 ability.

**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, UK (2009)
2. Holub, V., Fridrich, J.: Digital image steganography using universal distortion. In: Proceedings of 1st ACM Information Hiding and Multimedia Security Workshop, pp. 59–68. ACM (2013)
3. Guo, L.J., Ni, J.Q., Shi, Y.Q.: Uniform embedding for efficient JPEG steganography. IEEE Trans. Inf. Forensics Secur. **9**(5), 814–825 (2014)
4. Zhang, Y., Luo, X.Y., Yang, C.F., et al.: A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients. In: Proceeding of the 17th International Conference on Availability, Reliability and Security, pp. 461–466 (2015)
5. Zhang, Y., Zhu, X.D., Qin, C., et al.: Dither modulation based adaptive steganography resisting JPEG compression and statistic detection. Multimedia Tools Appl. **77**(14), 17913–17935 (2018)
6. Qian, Z.X., Zhou, H., Zhang, W.M., et al.: Robust steganography using texture synthesis. In: Proceeding of the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 25–33 (2016)
7. Zhao, Z.Z., Guan, Q.X., Zhang, H., Zhao, X.F.: 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.Y., Li, S., Zhang, X.P., Wang, Z.C.: Towards robust image steganography. IEEE Trans. Circuits Syst. Video Technol. **29**(2), 594–600 (2019)
9. Yu, X.Z., Chen, K.J., Yao, Y.F., et al.: Robust adaptive steganography based on generalized dither modulation and expanded embedding domain, 168, 107343 (2020)
10. Zhang, Y., Luo, X.Y., Guo, Y.Q., et al.: Multiple robustness enhancements for image adaptive steganography in lossy channels. IEEE Trans. Circuits Syst. Video Technol. **33**(8), 2750–2764 (2020)
11. Bao, P., Ma, X.H.: Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans. Circuits Syst. Video Technol. **15**(1), 96–102 (2005)
12. Kang, X.-B., Zhao, F., Lin, G.-F., Chen, Y.-J.: A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimedia Tools Appl. **77**(11), 13197–13224 (2017). https://doi.org/10.1007/s11042-017-4941-1
13. 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)
14. Bas, P., Filler, T., Pevný, T.: Break Our steganographic system: the ins and outs of organizing BOSS. In: Proceeding of the 13th International Workshop on Information Hiding, pp. 59–70 (2011)
15. Pevny, T., Fridrich, J.: Multiclass detector of current steganographic methods for JPEG format. IEEE Trans. Inf. Forensics Secur. **3**(4), 635–650 (2008)
16. Holub, V., Fridrich, J.: Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Trans. Inf. Forensics Secur. **10**(2), 219–228 (2015)
17. Kodovský, J., Fridrich, J., Holub, V.: Ensemble classifiers for steganalysis of digital media. IEEE Trans. Inf. Forensics Secur. **7**(2), 432–444 (2012)