



Research Paper

Robust steganography resisting JPEG compression by improving selection of cover element

Tong Qiao^{a,b}, Shuai Wang^a, Xiangyang Luo^{b,*}, Zhiqiang Zhu^a^a School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China^b State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, Zhengzhou, Henan, China

ARTICLE INFO

Article history:

Received 24 November 2020

Revised 29 January 2021

Accepted 18 February 2021

Available online 20 February 2021

Keywords:

Robust steganography

Social network platform

JPEG compression

Sign of DCT coefficients

ABSTRACT

Through minimizing embedding cost, modern adaptive steganography has gained unprecedented success in terms of its undetectability. However, due to Joint Photographic Experts Group (JPEG) compression, the secret bits hidden in the image transmitted over social network platform fail to be perfectly extracted, that remarkably limits its wide application in the real world. In this paper, by improving selection of cover element, we propose to design an enhanced robust steganographic algorithm to resist against JPEG compression. First, since that before and after JPEG compression the sign of Discrete Cosine Transform (DCT) coefficient is not easy to change, we devise cover element based on the sign of DCT coefficient. Furthermore, the selection of cover element is successfully improved with the help of post-processing operation analysis. Second, the embedding cost for each candidate DCT coefficient is calculated. Finally, dependent of both error correction algorithm and syndrome-trellis codes, a compression-resistant stego image is generated with minimum distortion. Numerical results verify that the robustness of our proposed steganographic algorithm is superior to that of current arts; meanwhile, the effectiveness of the algorithm is also verified over social network platform.

© 2021 Elsevier B.V. All rights reserved.

1. Introduction

Steganography is a science and art of transmitting secret bits in a covert channel while concealing the behavior of secret communication for avoiding detection from steganalysis. Till now, steganography has unprecedentedly advanced. Various modern steganographic algorithms [1–5] with strong undetectable power have been proposed to resist against steganalysis [6–12]. However, the problem of moving steganography from the laboratory to the real-world scenario is rarely addressed. In the practical scenario, when the social network platform serves as a transmission channel instead of simulated environment, modern steganography probably fails due to JPEG compression operation. Thus, in this context, let us devise an effective steganographic scheme with resisting against JPEG compression.

Currently, one of the most successful adaptive models rather treats the message embedding as a source coding problem with a fidelity constraint [2]. In this framework of minimizing the cost, the design of the distortion function becomes fundamentally important for the steganographer who prefers hiding information into cover source. Due to its superior undetectability, adaptive

steganography has been well-designed, such as spatial domain-based Highly Undetectable steGo (HUGO) [1], Wavelet Obtained Weights (WOW) [13], Spatial UNiversal WAvelet Relative Distortion (S-UNIWARD) [2], High-pass, Low-pass, and Low-pass (HILL) [4], and in JPEG domain JPEG Universal WAvelet Relative Distortion (J-UNIWARD) [2], Uniform Embedding Distortion (UED) [3] and Uniform Embedding Revisited Distortion (UERD) [5]. Alternatively, mainly relying on the model of non-additive cost, Clustering Modification Directions (CMD) [14], Synch [15], Dejoin [16], and the recently-proposed Gaussian Markov Random Field (GMRF) [17] are well-designed for dealing with the problem of covert communication.

However, most of them have unsatisfactory performance of resisting JPEG compression in the real transmission channel. Thus, the general framework of devising robust steganographic algorithm is recently proposed to address that challenge (see [18] for instance), in which the authors categorize the transmission channel into clean and dirty one. Specifically, in the ideal scenario, an image cannot be attacked by the channel, namely “in the clean channel”; in the practical scenario, an image is probably attacked by the channel, namely “in the dirty channel”. More importantly, four principles of designing robust algorithm, referring to as *imperceptibility*, *capacity*, *undetectability*, and *robustness* should be strictly required.

* Corresponding author.

E-mail address: xiangyangluo@126.com (X. Luo).

To study the problem of designing a robust steganographic algorithm resisting JPEG compression is what this paper mainly focuses on. Currently, a few effective embedding schemes have been devised, among which some combine the strength of modern adaptive steganography and robust watermarking [19–24] while some put focus on investigating the stego image impacted by the transmission channel [25,26]. Accordingly, let us divide them into two categories: *channel-independent* scheme and *channel-dependent* scheme, that will be discussed in details.

- In the first category, the designed algorithm embeds the secret bits into the image without knowing the used channel. In 2015, [19] first proposed an effective robust algorithm named DCRAS (DCT Coefficients Relationship based Adaptive Steganography), where the relationship of DCT coefficients from each block is used for establishing the embedding domain. Meanwhile, by comparing the magnitudes between the DCT coefficient in the target block and the mean of three coefficients from the adjacent blocks, the cover elements are successfully devised. Subsequently, in virtue of the embedding domain of DCRAS, [20] proposed FRAS (Feature Regions based Adaptive Steganography), in which the Harris-Laplacian features are used for constructing the embedding regions, leading to that both JPEG compression resistance and undetectability can be guaranteed. Next, In DMAS (Dither Modulation based Adaptive Steganography) [21], by characterizing the features of quantization operation, the authors utilize the dither modulation strategy to construct the embedding domain, in which most of middle-frequency DCT coefficients are used for embedding. Based on the Poisson distribution, [22] established a burst error model to reduce the fault tolerance performance of the aforementioned three methods. Additionally, to further improve robustness and undetectability of DMAS, the GMAS (General Modulation based Adaptive Steganography) is proposed [24]. Recently, dependent of concatenated error correction encoder, [23] improved the accuracy of secret bit extraction while guaranteeing the security. In addition, the steganographic algorithm proposed by [27] has the ability of resisting multi-attacks. In general, the scheme in this category has low computation complexity due to its relative independence of transmission channel. However, the limitation is that the capacity of embedding is relevantly small, compared with the second category, referring to as channel-dependent scheme.
- The schemes in this category mainly investigate the characteristics of procedures operated by the transmission channel. In other words, before generating stego image, a steganographer has previously known the used channel. To address the problem of low capacity for robust steganography, [25] repeatedly compressed the image in order to reduce the impact caused by the transmission channel, that was named as transmission channel matching method. In addition, by capturing the similarity between stego image generation and JPEG compression of transmission channel, [26] proposed to first transform a cover image to an intermediate image, directly resulting in that the JPEG compression operation from transmission channel helps the intermediate image change to an ideal stego image. Although both methods can bring larger capacity than those in the first category, they [25,26] have to previously know the compression characteristic of transmission channel, which to some degree limits its wide application over social media platforms. What's more, when generating a stego image, the method proposed in [25] needs to repeatedly upload and download images, where the abnormal behavior unavoidably increases risk of being detected by steganalyzer. Additionally, inspired by the aforementioned prior-arts, [28,29] perform very well when resisting at-

tacks by JPEG compression while ensuring a high accuracy of correctly extracting secret information.

Within the proposed principles, the algorithms dependent of transmission channel can ensure the embedding capacity while is incapable of completing robust steganography across different channels due to its procedure of learning features from the targeted channel (see [25,26] for instance). By contrast, mainly relying on the invariable property of sign of DCT coefficient during JPEG compression, the sign steganographic algorithm independent of transmission channel can achieve the requirement of robustness across various channels while its capacity cannot be guaranteed (see [18] for details). For improving the overall performance of the robust steganographic algorithm, let us study the design of enhanced robust steganographic scheme resisting JPEG compression. The contributions of this paper are as follows:

1. We specifically analyze the characteristics of post-processing operation from practical transmission channel, referring to as social network platform.
2. We improve the selection of cover element from sign of DCT coefficient with the help of post-processing operation analysis.
3. By designing a cost function, we guarantee the minimum distortion caused by embedding.
4. Relying on the rule of syndrome-trellis codes (STCs), together with the strategy of error correction, we finally establish an enhanced robust steganography.

In recent study, it is proposed to make full use of unchangeable sign of DCT coefficients for designing robust steganographic scheme. However, the randomly-selected cover elements cannot bring the optimal results, and meanwhile the effectiveness of covert communication without error bits cannot be always guaranteed. Thus, in this context, relying on analysis of post-processing operation by transmission channel, it is proposed to improve the selection of cover elements to further enhance the performance of sign steganography. It is assumed that since the sign of DCT coefficient basically remains unchanged before and after JPEG compression, the proposed robust steganographic method based on that invariable property is named sign steganography. In the following sections, let us first review the main procedure concerning the prior work sign steganography.

The rest of the paper is organized as follows. In Section 2, it is proposed to describe the main steps of our prior scheme. In Section 3, we present the main improvement of performance by improving the selection of cover elements, in which the characteristics of post-processing procedure by transmission channel are detailedly analyzed. Subsequently, the numerical experimental results are provided to proof the better performance of our proposed enhanced robust steganography than prior arts in Section 4. Finally, we conclude this paper in Section 5.

2. Preliminaries and prior work

In this section, we first introduce some definitions, and specifically revisit our prior work involving fundamental procedures. For clarity, it is proposed to summarize the main notations used in this paper in Table 1.

The technique of robust watermarking mainly focuses on security of the protected carrier, in which the digital watermark has to be detectable and verifiable. Different from watermarking, steganography is an application of secret bits embedded in a carrier, where the behavior of covert communication is carefully concealed. In such context, robust steganography establishes an effective bridge connecting two techniques while overcoming the limitation of steganographic algorithm application in the practical channel. Motivated by the aforementioned fundamental,

Table 1
Notations.

c	Cover element
s	Stego element
R	Payload
d	DCT coefficient of cover image
d^s	DCT coefficient of stego image
ρ	Embedding cost of sign steganography
γ	Exponent parameter
m	Original secret bits
m^{ECA}	Secret bits after error correction

the design of robust steganography basically follows the general framework “Robust domain + Secure embedding scheme + Efficient coding with correction functionality”, RSE for abbreviation, which has verified its effectiveness and reliability in the current arts (see [19,27] for instance), also in our experiments (see details in Section 4). Specifically, the in-depth analysis is presented as follows:

- “Robust domain” guarantees that the robust stego image can resist against unknown attacks such as JPEG compression from the lossy channel. In the robust domain, cover element is required to be successfully extracted with the ability of resisting against JPEG compression attack. In fact, cover element in the robust domain serves as the realistic carrier for hiding secret bits. Moreover, it makes sense that the improvement of cover element can further improve the robustness of stego image, which this paper mainly focuses on.
- “Secure embedding scheme” ensures that the robust stego image is capable of detection-resistance to steganalysis. In modern steganography, the steganographic methods are generally established with minimizing the total embedding cost for security, where the embedding scheme is rather treated as a source coding with a fidelity constraint [2].
- “Efficient encoding with correction functionality” helps the data hider realize the embedding procedure, and restore the hidden bits with fault tolerance. After calculating the embedding cost from a cover image, the efficient steganographic encoding, such as STCs, has been widely applied to generate stego element, which is also used for establishing a stego image in this context. Furthermore, it is worth noting that prior to steganographic encoding, the hidden bits is encoded with error correction algorithm such as Reed-Solomon (RS) to realize correction functionality.

Cover element comes from the DCT coefficient in JPEG domain or pixel intensity in spatial domain before embedding; stego element for DCT coefficient or pixel intensity after embedding. Generally, in spatial or JPEG domain, most of cost functions are designed for constantly boosting the undetectability performance of steganography while few methods focus on the robust performance of steganography. Supposing that some stego elements are attacked by JPEG compression, it hardly holds true that the secret hidden bits can be perfectly extracted. Therefore, in this context, based on the RSE framework of designing robust steganography, the cover/stego element can be constructed, that is immune to JPEG compression.

In the prior work, the sign of DCT coefficient is firstly proposed to generate the *Cover Element* (see Subsection 2.1) in order to ensure the robustness of its corresponding stego element after JPEG compression. Secondly, the function of *Embedding Cost* (see Subsection 2.2) has to be re-designed. First of all, let us briefly review the following main stages of the original sign steganography.

2.1. Cover element

For establishing the cover elements, we first select non-zero DCT coefficients of a JPEG cover image with quality factor $QF^{(1)}$, which should perform robustly to JPEG compression. When the JPEG cover image is re-compressed again by the given $QF^{(2)}$, the non-zero candidate DCT coefficient can be used for generating cover element, which is formulated as:

$$c_l = \begin{cases} 1, & d_l > 0 \\ 0, & d_l < 0 \end{cases} \quad (1)$$

where $\mathbf{c} = \{c_l\}, l \in \{1, \dots, L\}$ represents cover element with the length L , and the candidate DCT coefficients $\mathbf{d} = \{d_l\}, l \in \{1, \dots, L\}$. Besides, the location information of cover elements has to be shared as a key. In sign steganography, the selection of cover elements is actually to improve the candidate DCT coefficients \mathbf{d} . If the quantization step increases, L unavoidably becomes small, that directly impacts the capacity of embedding. Moreover, the $QF^{(2)}$ to some extent also impacts the performance of sign steganography, which is not mainly addressed in the prior work while in Section 3 we specifically analyze that issue.

2.2. Embedding cost

To our knowledge, the most successful approach for image steganography is content adaptive, meaning that the embedding strategy is designed based on the framework of minimizing distortion between the cover and the its stego version. In sign steganography, the value of cover element is determined by sign of DCT coefficient. It makes sense that the small absolute value of the DCT coefficient brings low cost distortion. Besides, the cost of the texture region is smaller than that of the smooth region. Accordingly, the DCT coefficient of the texture region with small absolute value is the optimal choice for embedding.

It is proposed to define the pre-cost ρ^{pre} , that can be calculated by referring to J-UNIWARD [2]. Actually, in sign steganography, the cost function also can be extended to the other effective ones, such as UED [3] or UERD [5]. Then, the embedding cost of sign steganography can be defined by:

$$\rho_l = \begin{cases} |d_l|^\gamma, & \rho^{\text{pre}}(d_l) < \tau \\ \rho^{\text{pre}}(d_l), & \rho^{\text{pre}}(d_l) \geq \tau, \end{cases} \quad (2)$$

where τ serves as the threshold. It can adaptively adjust the embedding cost by comparing with the pre-cost ρ^{pre} . Meanwhile, the exponent parameter γ , not smaller than one, is adopted to adaptively magnify the embedding cost when the large absolute value of DCT coefficient appears. In such manner, the size of the preferential embedding DCT coefficients can be effectively controlled, and the selection of cover elements is improved.

Next, the error correction algorithm (ECA) is used for encoding the secret bits for further enhancing the ability of self-correction. Finally, as modern steganography, the STCs helps the cover elements transform to stego elements with the secret bits. It is worth noting that the stego elements need to be inversely mapped to DCT coefficients for obtaining a stego image. Without loss of generality, the extraction of secret bits can be smoothly realized according to the inverse procedure.

Due to that the sign of DCT coefficient plays an important role in robust steganography, we name the algorithm as sign steganography. In fact, by adopting sign steganography, not all “effective” cover elements are used for embedding. Intuitively, by improving the selection of cover element, we can further design the scheme of enhanced sign steganography, that will be elaborated in Section 3.

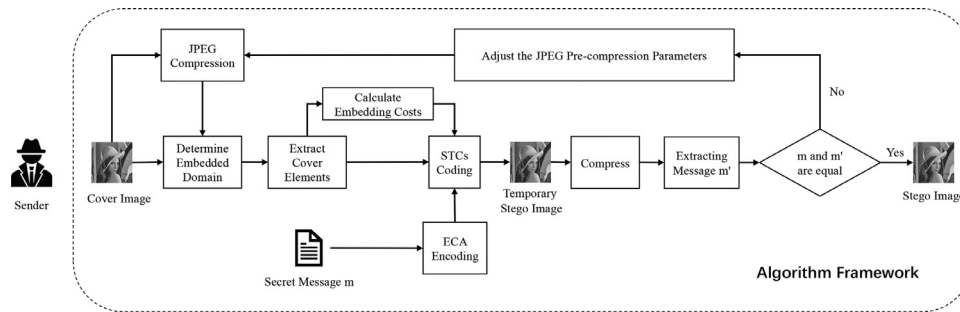


Fig. 1. Illustration of our proposed robust steganographic framework.

3. Proposed work

3.1. Problem statement

In this paper, we mainly focus on improving the selection of cover elements based on side information provided by transmission channel. In general, the social network platforms possibly adopt different techniques to post-process the upload images by users. For instance, JPEG compression is usually applied to the uploaded images. On the one hand, compression operation helps the server save the capacity of storage; on the other hand, it can actively defend some latent malicious attacks, such as steganography. In our prior study (see Section 2), we have designed well-performed algorithm of robust steganography, namely sign steganography, that can be applied to dirty channel without knowing compression characteristic. Thus, the algorithm can be widely-extended independent of transmission channel.

However, unlike the robust steganographic algorithm relying on transmission channel, [25,26] for instance, that learn the channel characteristic prior to embedding, the limitation of the prior algorithm is that it cannot perfectly restore the hidden bits, that is to say extraction errors appear when unknown JPEG quality factor is used. To address that challenge, we propose to consider the compression characteristic of social network platform as side information, and further improve the overall performance of sign steganography. The primary step of sign steganography is to select the effective candidate cover elements with given quality factor. Because the quality factor directly determines which cover element is feasible for embedding.

In the original design, it makes sense that a candidate image with small quality factor should have less cover elements for sign steganography, QF 60 for instance. In fact, some social network platforms always strike the balance between image quality and storage capacity, resulting in that too small QF is impossible applied. Let us take Facebook for example, where QF 71 is used for compression by its server¹. In this context, the cover elements acquired by using the mismatched QF 60 hardly leads to the satisfying results. Inspired by some algorithms relying on the transmission channel [25,26], we propose to enhance the performance of sign steganography. Through predicting the quality factor of JPEG compression used by social network platform, it is proposed to improve the selection of cover elements, instead of heuristically choosing quality factor. That indeed helps us improve the robustness and meanwhile decrease the extraction error of sign steganography.

For simplicity and clarity, let us briefly demonstrate the flow chart of the proposed algorithm in Fig. 1.

- Step #1: *Target Transmission Channel*. Prior to embedding, we first select the latent social network platform, that is widely-used and easy to upload/download images. More importantly, the platform carries out the few post-processing operations, that serves as side information for embedding.
- Step #2: *Analyze Post-processing Operation*. In this paper, we only investigate JPEG compression operation used by social network platform. If the platform publishes its source codes, we can directly acquire its compression characteristic. Otherwise, the reverse engineering is required, referring to as learning the compression characteristic by once uploading and downloading cover images. In fact, the platform possibly changes its compression strategy from time to time. Nevertheless, prior to practical data hiding, the compression characteristic has to be re-confirmed.
- Step #3: *Select Ready-to-embed Cover Image*. Based on the predicted compression quality factor, it is proposed to select the suitable cover image. Moreover, the candidate cover elements from DCT coefficients, are selected for embedding.
- Step #4: *Embed Secret Bits into Cover Image*. The specific embedding procedure involves calculation of embedding cost and acquisition of stego elements. Besides, the parameters of the proposed algorithm is empirically predicted.
- Step #5: *Generate Robust Stego Image*. Based on the stego elements, together with the design of embedding rule, DCT coefficients containing secret bits are completely obtained, leading to generation of a stego image capable of resisting against JPEG compression.

In Step #1, it is not difficult to determine the transmission channel since that many fashionable social network platforms can be utilized for covert communication nowadays, such as Facebook, Twitter, and WeChat. Thus, in the following sections, we mainly focus on Steps #2, #3, #4, and #5.

3.2. Analysis of post-processing operation

Without loss of generality, we first have to target which practical channel is available for transmitting stego images, that exactly corresponds to Step #1. Then let us study the transmission characteristic of the selected social network platform in detail, that just corresponds to Step #2. To specifically study the impact caused by post-processing operation, let us first illustrate a comparison example for addressing the impact of QF⁽²⁾ (see details in Section 2.1) used for selecting cover elements. As Fig. 2 reports, for the same cover image, it is proposed to adopt two different QF⁽²⁾s (small and large) for selecting cover elements. It is worth noting that low cost brings better undetectability of stego image. Obviously, it can hardly hold true that too small or large quality factor is our choice. The small QF⁽²⁾ possibly misses some candidate cover elements (return to zero caused by QF⁽²⁾); the large QF⁽²⁾ reserves some candidate cover elements with low cost, leading to the improve-

¹ In the early stage (before 2019), QF 71 is the common strategy which was changed after 2019.

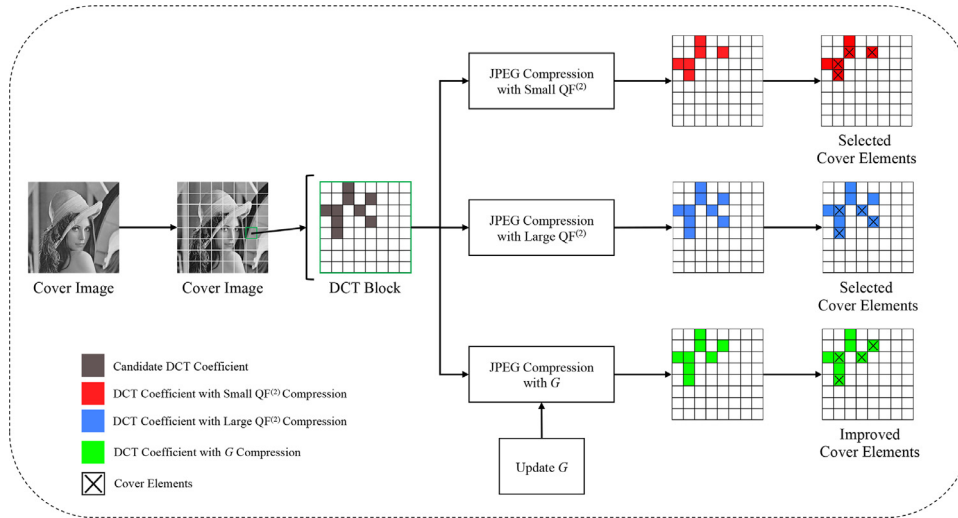


Fig. 2. Illustration of impact on cover elements caused by JPEG compression with different $QF^{(2)}$ s.

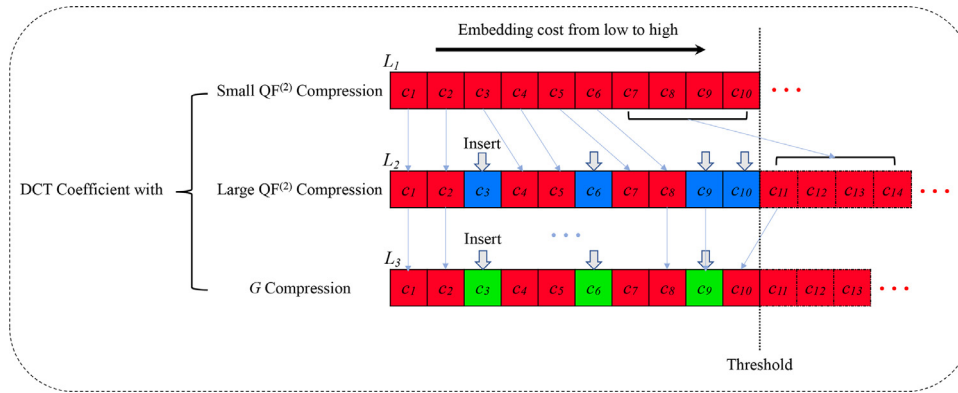


Fig. 3. Illustration of cover element selection with the fixed payload.

ment of undetectability. However, with the $QF^{(2)}$ gradually increasing, the finding of cover elements with the robust characteristic becomes more and more difficult. Therefore, when the large $QF^{(2)}$ is adopted, the DCT coefficients with weak robustness and strong undetectability are probably selected; when the small $QF^{(2)}$ is used for JPEG compression, the DCT coefficients with strong robustness and weak undetectability are probably selected.

To further demonstrate the importance of quality factor, we give an example of cover element selection with the fixed payload, 10 cover elements selected for instance (see Fig. 3). In our illustration, $\{c_i\}$ denotes the cover elements, whose embedding cost is sorted in ascending order; the threshold determines the number of selected elements. Moreover, three different compression schemes are adopted. As small $QF^{(2)}$ compression, 10 cover elements with the lowest cost are selected for embedding, denoting L_1 . As large $QF^{(2)}$ compression, 10 updated cover elements with the lowest cost are selected, denoting L_2 . It should be noted that the four new elements with lower cost in L_2 are inserted in place of the original elements with high cost in L_1 . However, in L_2 , we cannot guarantee that all the elements are robust to compression. Thus, we propose to further improve the selection of cover element by adopting the updated G , for better robustness and undetectability. For instance, more robust c_{11} in L_2 replaces c_{10} in L_3 .

3.3. Improvement of selecting cover element

Based on our empirical results, when $QF^{(2)}$ used for selecting cover elements is very close to $QF^{(1)}$ from the original JPEG cover

image, the stego image cannot perform its robustness to JPEG compression as the ones generated by the other QFs. That is because the two similar QFs applied to the images nearly cannot impact the characteristic of DCT coefficient. Thus, we are intuitively prone to compress cover image with low QF, that can help us search for more robust coefficients while reserving less cover elements at the cost, leading to a large scale of zero coefficients not used for embedding. In such case, the capacity is also further curtailed while cannot guarantee the low error bits. On the contrary, the large QFs hardly brings out enough candidate cover elements for embedding, where the DCT coefficients robust to compression cannot be accurately located.

Therefore, it is proposed to devise an effective scheme for dealing with the aforementioned trade-off problem, to further improve the performance of robust steganography. Specifically, by considering the impact of transmission channel, $QF^{(2)}$ needs to be well-designed for various images while not remains the same. Immediately, let us formulate compression factor $QF^{(2)}$ as parameter G :

$$G = P - \alpha \quad (3)$$

where P denotes the value of QF from the transmission channel, serving as side information inspired by two baseline methods [25,26]. $\alpha \in \mathbb{N}$ represents an adaptive factor (see details in Table 3), used for selecting the G leading to the improvement of c (see Eq. (1)), which can be updated by iteration (see details in Algorithm 1). It should be noted that when G is fixed for images over the transmission channel, the acquired stego image is the

Table 2
Experimental statistic.

Image source	BOSSbase 1.01 dataset [30]
Image color	Grayscale
Image size	512 × 512
Image format	JPEG
Quality factor	75
Compression attack	QF = {71, 75, 85}
Number of original images	10000
Payload	0.01 ~ 0.1 bpnzac
Compared algorithms	ESS (Ours), SS [18], TRI [26], TCM [25], MREAS-Pj [27], DCRAS [19], RIS [23], J-UNIWARD [2], UERD [5].

same as the one as our prior algorithm. Relying on the parameter G , the performance of the original robust steganography is remarkably improved, especially on robustness and undetectability.

As we have mentioned before, the quality factor $QF^{(2)}$ indeed plays an important role in our proposed method, which directly determines the selection of cover elements (see Fig. 2 for illustration). In our designed rule of selection, based on the embedding cost, the selected cover elements from the candidate DCT coefficients with robustness are used for embedding. Thus, “sufficient”, “robust”, and “undetectable” candidate DCT coefficients is the first priority. In our design, G should be close to P the value of QF from the transmission channel, which guarantees the “sufficient” candidate DCT coefficients. That is because the transmission channel actively compresses the image without using too small quality factor, generally in the premise of image quality. Besides, G should be slightly smaller than P , parameterized by α , that to some extent guarantees the “robust” candidate DCT coefficients. Last but not least, due to that we select cover elements in virtue of the embedding cost, the “undetectable” DCT coefficients can be used for embedding. Next, let us complete the remaining procedures, referring to as Steps #4 and #5.

3.4. Description of embedding

Let us define the secret bits $\mathbf{m} = \{m_n\}, n \in \{1, \dots, N\}$. Then the error correction algorithm (ECA), such as RS, is adopted to encode \mathbf{m} . Immediately, $\mathbf{m}^{ECA} = \{m_k^{ECA}\}, k \in \{1, \dots, K\}$ is obtained. Next, with the help of STCs, the stego elements $\mathbf{s} = \{s_l\}, l \in \{1, \dots, L\}$ can be formulated by:

$$s_l = F_{STCs}(c_l, \rho_l, m_k^{ECA}) \quad (4)$$

where $F_{STCs}(\cdot)$ denotes a function of STCs encoding. For ensuring that the secret bits are successfully embedded, K is not larger than L . It should be noted that the ECA plays an important role during embedding. When the stego image is attacked by JPEG compression, the DCT sign of the stego image generated by sign steganography basically remains unchanged. Meanwhile, the ECA can correct error bits in case that a small portion of the DCT coefficients (with the large quantization step) becomes zero. In practice, to ensure the security of transmitted data, the secret bits \mathbf{m} are usually

encrypted, in which the design of encryption algorithm is not our consideration of this paper.

3.5. Generation of stego image

Finally, the DCT coefficients \mathbf{d} from a cover image are modified based on the stego elements \mathbf{s} , and a compression-resistant stego image can be accordingly constructed. Immediately, the modified coefficients $\mathbf{d}^s = \{d_l^s\}$ carrying secret bits can be formulated as:

$$d_l^s = \begin{cases} d_l, & c_l = s_l \\ -d_l, & c_l \neq s_l \end{cases} \quad (5)$$

where c_l represents a cover element; s_l represents a stego element. For clarity, when $c_l = s_l$, $d_l^s = d_l$, where the DCT coefficient remains unchanged; when $c_l \neq s_l$, $d_l^s = -d_l$, where the sign of DCT coefficient is flipped. Finally, a stego image can be acquired relying on the modified DCT coefficients.

To facilitate the reproduction of our proposed robust steganography, it is proposed to give the pseudo-codes in the following (see Algorithm 1 for details). It is worth noting that we conduct the procedure of improvement through rational iteration. In fact, the strategy of iteration and re-compression for designing robust steganography was proposed by TCM in [25]. However, unlike the method in [25], where the same quality factor is used for re-compression, we adopt the updated quality factor for re-compression in order to select the suitable cover elements. In such manner, we improve the selection of cover element. In the premise of the robustness and undetectability, the requirement of improvement can be smoothly met.

4. Numerical experiments

4.1. Setups

To verify the sharpness of our proposed algorithm, let us comprehensively evaluate the performance of it by adopting the benchmark dataset BOSSbase 1.01 [30]. Specifically, 10,000 original images are used to generate the stego images using the payload from 0.01 to 0.1 bpnzac (bits per non-zero AC coefficient) with QF 75. Furthermore, it is proposed to compare our algorithm with the recent baseline algorithms, such as TCM (Transport Channel Matching) [25], TRI (Towards Robust Image) [26], MREAS-Pj (Multiple Robustness Enhancements for image Adaptive Steganography) [27], DCRAS (DCT Coefficients Relationship based Adaptive Steganography) [19], RIS (Robust Image Steganography) [23], and SS (Sign Steganography) [18]. It should be noted that the algorithm proposed in this paper, equipped with RS (31, 15), is the enhanced version of SS, namely ESS. For clarity, Table 2 illustrates the detailed settings. Without loss of generality, the evaluation will be extended based on the following principles: *imperceptibility*, *capacity*, *undetectability*, and *robustness*.

First of all, let us discuss the parameter settings of our proposed algorithm. As our aforementioned discussion, the param-

Table 3
Ratio (%) allocation of images with successful bits extraction under various α .

Payload α	1	2	3	4	5	6	7	8	9	10
0.01	99.71	0.19	0.03	0.02	0	0	0.01	0	0.01	0.01
0.02	99.18	0.56	0.11	0.02	0.03	0	0.02	0	0.01	0
0.03	98.46	0.85	0.24	0.05	0.04	0.06	0.03	0.06	0.02	0.01
0.05	96.81	1.63	0.38	0.28	0.13	0.15	0.06	0.01	0.04	0.05
0.06	96.24	1.90	0.47	0.27	0.13	0.08	0.05	0.06	0.09	0.07
0.07	95.02	2.34	0.63	0.46	0.24	0.18	0.07	0.07	0.07	0.08
0.08	95.61	2.38	0.74	0.51	0.29	0.21	0.07	0.06	0.08	0.06
0.09	93.75	2.78	0.84	0.61	0.23	0.21	0.15	0.05	0.06	0.07
0.10	93.11	2.87	0.96	0.62	0.30	0.22	0.22	0.08	0.07	0.07

Table 4
PSNR comparison.

Test image Method	ESS (Ours)	SS	TCM	TRI
Barbara	42.42	42.43	56.85	52.07
Goldhill	43.98	43.93	54.90	54.88
Lena	45.86	46.86	56.32	56.16
Peppers	46.94	46.84	56.18	56.21

Table 5
SSIM comparison.

Test image Method	ESS (Ours)	SS	TCM	TRI
Barbara	0.9977	0.9974	0.9997	0.9997
Goldhill	0.9975	0.9974	0.9997	0.9997
Lena	0.9977	0.9977	0.9998	0.9998
Peppers	0.9976	0.9975	0.9998	0.9998

ter G plays an important role for selecting cover elements, which is controlled by transmission channel parameter P and adaptive factor α . In fact, P can be accurately predicted by uploading and downloading an image, which is also adopted by the other algorithms [25,26]. Thus, to achieve the improved performance of our proposed robust steganography, it is proposed to conduct our analysis based on empirical results, referring to as modifying α .

10 payloads are applied to generate robust stego images via 10,000 cover images from BOSSbase. As Table 3 reports, when α equals to 1, the optimal results can be achieved. Let us recall the analysis in the last section, where we have addressed that too large or too small G is not satisfying. While if the characteristic of the transmission channel is considered, the selection of G is more sound and effective. The results of Table 3 empirically verify our assumption, that is, G behaves very closely to P while not equal to P . In such manner, the robust stego images by using our proposed algorithm can perform very well. Besides, even though the setting of α is confirmed, the results are probably impacted by the length of secret bits. When less bits are embedded with payload 0.01 for instance, 9971 images among 10,000 images complete covert communication with zero-error extraction.

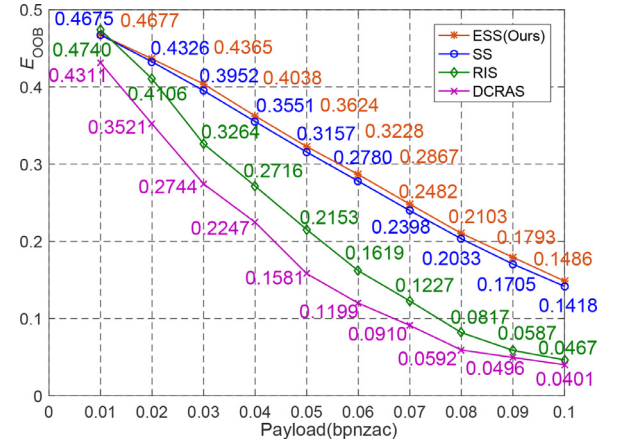
4.2. Evaluation of imperceptibility

The stego image should remain perceptual distortion as small as possible, referring to imperceptibility. For simplicity, we randomly select four standard test image, referring to *Barbara*, *Goldhill*, *Lena*, and *Peppers*. PSNR (Peak Signal to Noise Ratio) and SSIM (Structural SIMilarity index) serve as the evaluation metric.

We select payload 0.1 to generate robust stego image. As Tables 4 and 5 display, TCM and TRI can achieve better results than ESS (Ours) and SS. That is because TCM and TRI generate robust stego image very close to (or nearly same as) the stego one by J-UNIWARD [2], where the structure of cover image can be perfectly reserved under the framework of STCs. On the contrary, ESS and SS possibly modify the sign of DCT coefficients, leading to that the change of coefficients caused by embedding is larger than that of TCM and TRI. Nevertheless, the PSNR and SSIM of stego image generated by our robust steganography are still acceptable, whose imperceptibility performance are also relevant. In such manner, to some degree, it is required to slightly lose the visual quality of the stego image, in order to ensure the robustness of the stego image. Thus, by using our proposed method, we cannot guarantee both robustness and imperceptibility are enhanced together, that is kind of negative correlation. Additionally, we also evaluate the imperceptibility of 10,000 images from BOSSbase. The PSNR of stego images by TCM and TRI are larger than 50, and meanwhile better than that of ESS and SS.

Table 6
Average capacity comparison.

Quality factor Method	ESS (Ours)	SS	TCM	TRI
75	41,587	41,529	33,387	41,592
85	45,400	28,748	33,362	56,206
95	38,397	31,525	33,440	98,065

**Fig. 4.** The undetectability of robust stego images (respectively generated by ESS, SS, RIS, and DCRAS) with payloads from 0.01 to 0.1.

4.3. Evaluation of capacity

The capacity can be evaluated by the maximum number of secret bits embedded into the image. In the DCT domain, the capacity is measured by the number of non-zero AC coefficients used for embedding. In particular, 10,000 images are compressed with QF = {75, 85, 95}, serving as cover source. Four compared algorithms convert cover images into stego ones.

As Table 6 illustrates, TRI has the largest capacity, in which all non-zero AC coefficients can be used to acquire cover elements. To our knowledge, for TRI, the robust domain is actually the same as that of modern steganography, where the high embedding capacity can be effectively conserved. However, TCM, SS, ESS have to select robust DCT coefficients as cover elements. Besides, due to that TCM needs to multiply compress the transmitted images with the same QF for reserving the invariance of DCT coefficients, the similar capacity appears among original cover images with different QFs. By strictly improving the cover elements, the well-performed cover elements guarantee that at the receiver, the secret bits can be correctly extracted, and resist against JPEG compression attack from the lossy channel. In fact, TCM, SS, and ESS sacrifice to some extent capacity for guaranteeing robustness.

4.4. Evaluation of undetectability

In this section, compared with the original SS, we intend to verify the improved undetectability of ESS by using the benchmark steganalytic detector. Meanwhile, RIS and DCRAS serve as the baseline methods for comparison. The benchmark ensemble steganalysis classifier [31], together with the discriminative features CC-PEV [32], is established. Also, 10,000 cover images are converted into stego ones with payloads from 0.01 to 0.1. We randomly select 5000 stego images and 5000 cover images for training; the remaining images are used for testing. It is proposed to denote the ensemble's "out-of-bag" (OOB) error E_{OOB} as classification error rate. It should be noted that the larger E_{OOB} is, the undetectability of the method is stronger.

As Fig. 4 illustrates, if the small payloads (not larger than 0.1) are adopted for evaluation, the undetectability performance of all

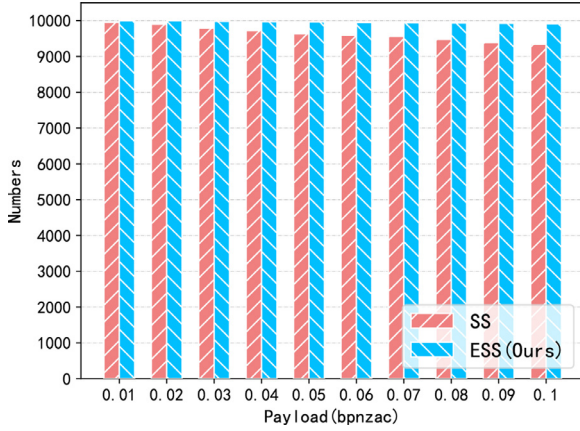


Fig. 5. Illustration of the total number of stego images (respectively generated by SS and ESS), where the secret bits can be correctly extracted, with payloads from 0.01 to 0.1.

the methods is degraded with increasing the payload. It should be noted that on the whole, both RIS and DCRAS perform worse than ESS and SS. More importantly, ESS performs better than its counterpart SS among all payloads, which further verifies the improvement of the selection of cover element. That is because, during the procedure of improvement, the embedding cost of cover element is updated, resulting into that the undetectability of ESS is further enhanced. Besides, when we use the alternative rich model features CC-JRM [31], the similar results can be acquired, where stego images by ESS has superior undetectability.

Additionally, we have to admit that the undetectability of both TCM and TRI (E_{OOB} larger than 0.4) is better than that of both ESS and SS. Moreover, we need address that the undetectability of MREAS-P_j is the worst among all the compared methods, in which the E_{OOB} of it cannot arrive at 0.25 for payload 0.01. Although the undetectability of ESS (weakness point) is not satisfying, we can assign the secret bits (high payload) into multiple images with groups of bits (low payload), leading to that more secure robust steganography in our proposed framework.

4.5. Evaluation of robustness

Last but not least, let us comprehensively evaluate the robustness of our proposed algorithm. Here, it is proposed to evaluate the robustness of stego images from two perspectives. 1) image level: the number of images where the secret bits can be perfectly extracted; 2) bit level: the extraction error rate, which is formulated as:

$$R_{\text{error}} = \frac{n_{\text{error}}}{l_{\text{msg}}}, \quad (6)$$

where n_{error} denotes the number of incorrectly extracted bits, and l_{msg} is the length of secret bits. In such manner, we can comprehensively evaluate the compared algorithms from global (image level) to local (bit level) robustness performance.

Similarly, all the cover images from BOSSbase are used for our following experiments. First of all, ESS and SS respectively help us acquire robust stego images with payloads from 0.01 to 0.1, in order to verify the effectiveness by improving the selection of cover elements. In this case, we propose to simulate JPEG compression attack with QF 71. As Fig. 5 reports, whatever payload is used for embedding, ESS always performs better than SS, since that more images with perfect bits extraction are counted. Furthermore, with increasing payload, ESS basically remains its robustness while SS cannot perform very well. Besides, we also count the number of stego images carrying hidden bits with prior-art J-UNIWARD. Un-

Algorithm 1: Our proposed robust steganography.

Input : Cover image X , QF of transmission channel P , secret message \mathbf{m}

Output: Stego image Y

```

1:  $\mathbf{m}^{\text{ECA}} = F_{\text{ECA}}(\mathbf{m})$  // ECA encoding prior to embedding
2: if  $QF^{(1)} < P$  then
3:    $Y = F_{\text{SS}}(X, \mathbf{m}^{\text{ECA}}, QF^{(2)})$  // Embedding with fixed  $QF^{(2)}$ ,
   that is selected without improvement
4: Return  $Y$ 
5: else
6:    $\alpha = 1$  //Initializing the adaptive factor  $\alpha$ 
7:   while  $\alpha \leq 10$  do
8:      $G = P - \alpha$ 
9:      $Y = F_{\text{ESS}}(X, \mathbf{m}^{\text{ECA}}, G)$  // Embedding with adaptive  $G$ ,
   and the improved cover elements are selected
10:     $Y' = F_{\text{compress}}(Y, P)$  // Compression attack with  $P$ 
11:     $\mathbf{m}_{\text{extract}} = F_{\text{extract}}(Y')$  // Message extraction from  $Y'$ 
12:    if  $\mathbf{m}_{\text{extract}} == \mathbf{m}$  then
13:      Return  $Y$ 
14:    else
15:       $\alpha = \alpha + 1$  // Updating  $\alpha$ 
16:    end if
17:    Return failure // Adaptive  $G$  cannot be acquired
18:  end while
19:  Return failure // Large  $\alpha$  degrades undetectability
20: end if

```

fortunately, none of images completes the task of covert communication under JPEG compression attack.

To further verify the powerful robustness of ESS, it is proposed to compare the other baseline algorithms [18,19,25–27] in the more practical scenario, where the JPEG compression attack is launched with three different QFs. The average R_{error} is used for evaluation. The rich experimental results are illustrated in Table 7.

On the whole, compared with the others, our proposed ESS performs the best average R_{error} (not larger than 0.25×10^{-3}) with different payloads. It should be noted that compared with the original SS, the robustness of our proposed ESS in this paper is remarkably improved. Due to that before and after JPEG compression the sign of DCT coefficient is not easy to change, the cover elements extracted in the robust domain can effectively resist against JPEG compression attack. Furthermore, by improving the selection of cover elements, our proposed ESS is superior to the original SS. Besides, with increasing payload, R_{error} slightly increases while the ESS basically remains its robustness resisting against JPEG compression with various QFs.

In particular, when the robust stego images carrying small payload are attacked by compression with QF 71, most of the compared methods perform very well except DCRAS. In our experiments, for fair comparison, all 10,000 original images from Bossbase are used for evaluation while in [19] for DCRAS only 2000 original images are used for evaluation. Moreover, for MREAS-P_j, due to that the cover images are first selected based on the content complexity, not all the images are used for evaluation in [27]. Thus, the results of DCRAS and MREAS-P_j in Table 7 exist differences from the results as the references provided.




Especially for TRI [26], among all the payloads, the secret bits can be successfully extracted for 10,000 images with QF 71, that are the best results compared with the others. Since that the procedure of compression attack from transmission channel imitates the stage of adaptive embedding, it makes sense that the perfect results can be achieved by TRI. However, when QF changes, TRI fails to complete robust steganography, as well as TCM. In fact, both TRI and TCM heavily rely on the transmission channel, where

Table 7 $R_{\text{error}} (\times 10^{-3})$ of six compared methods under JPEG compression attack with QF = {71, 75, and 85}.

Method	QF	Payload									
		0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
DCRAS [19]	71	443	328	254	206	172	146	125	109	96	85
	75	0.02	0.01	0.01	0.03	0.04	0.09	0.08	0.15	0.18	0.24
	85	506	496	493	488	484	481	477	473	469	464
	AVG	316	275	249	231	219	209	201	194	188	183
MREAS-P _j [27]	71	6.20	7.85	8.87	8.92	8.30	7.76	7.38	7.12	6.88	6.77
	75	0.56	0.72	0.82	0.83	0.89	0.97	1.02	1.09	1.13	1.18
	85	0.66	0.90	1.02	1.04	1.07	1.13	1.19	1.23	1.28	1.34
	AVG	2.47	3.16	3.57	3.60	3.42	3.29	3.20	3.15	3.10	3.10
TCM [25]	71	12.7	13.2	13.6	13.7	13.1	13.5	13.3	13.4	13.2	13.2
	75	501	498	500	499	502	498	499	500	498	502
	85	498	497	500	499	502	501	501	498	499	500
	AVG	337	336	338	337	339	338	338	337	337	338
TRI [26]	71	0	0	0	0	0	0	0	0	0	0
	75	498	499	500	499	503	499	498	499	501	502
	85	501	498	497	499	502	500	498	501	500	499
	AVG	333	332	332	333	335	333	332	333	334	334
SS [18]	71	0.27	0.28	0.41	0.45	0.59	0.62	0.64	0.74	0.77	0.83
	75	0.15	0.15	0.17	0.21	0.28	0.28	0.31	0.38	0.40	0.41
	85	0.00	0.01	0.02	0.03	0.02	0.04	0.04	0.04	0.05	0.05
	AVG	0.14	0.15	0.20	0.23	0.30	0.31	0.33	0.39	0.41	0.43
ESS (Ours)	71	0.03	0.06	0.08	0.12	0.18	0.23	0.31	0.33	0.40	0.42
	75	0.01	0.06	0.07	0.10	0.12	0.18	0.21	0.24	0.28	0.28
	85	0.00	0.01	0.02	0.02	0.02	0.04	0.04	0.04	0.05	0.05
	AVG	0.01	0.04	0.06	0.08	0.11	0.15	0.19	0.20	0.24	0.25

Table 8

A toy example of ESS over social network platform: Facebook, WeChat, and Twitter.

SNP	Facebook	WeChat	Twitter
Stego image			
QF from uploaded stego image	75	90	90
QF from downloaded stego image	71	85	85
R_{error}	0	0	0
Covert communication	success	success	success

both algorithms are designed only for the specific channel with fixed QF JPEG compression, meaning that the generated stego images cannot resist against various QFs. On the contrary, SS is designed completely independent of transmission channel while ESS serves as the enhanced version of SS by considering the side information provided by channel.

4.6. Practical performance over social network platform

In the practical scenario, we will verify the effectiveness of our proposed ESS over Social Network Platform (SNP), such as Facebook, Twitter, and WeChat². Then it is proposed to randomly select an image No. "6494.jpg" in the BOSSbase, and generate robust stego image with QF 75 uploaded to Facebook, with QF 90 respectively uploaded to Wechat and Twitter, where the payload equals to 0.1. When the image is downloaded from SNP, we can test the correctness of the extracted secret bits. As Table 8 illustrates, our proposed robust steganography successfully completes the task of covert communication over SNP.

To further verify the superior robustness of our proposed ESS, we randomly select 50 JPEG images with QF 85, which are used for covert communication on Facebook with the changeable QF. Two metrics are adopted, referring to R_{error} and N_s denoting the num-

Table 9Performance of robustness evaluated by R_{error} and N_s .

MetricMethod	ESS (Ours)	SS	TRI	TCM	J-UNIWARD	UERD
R_{error}	0.0016	0.0043	0.3537	0.5013	0.4593	0.4600
N_s	48	47	0	0	0	0

ber of images in which all the hidden bits can be completely extracted. As Table 9 reports, our proposed ESS with the lowest R_{error} remains the optimal robustness, which is slightly better than SS, and remarkably better than the others. Also, if the stego images are generated by adopting ESS, 48 of 50 images can be perfectly covertly transmitted on Facebook while both traditional steganography (J-UNIWARD, UERD) and robust steganography (TRI, TCM) fail to covertly communicate (see Table 9). That is because both TRI and TCM can only be realized when the JPEG compression attack of transmission channel remains the invariant QF.

5. Concluding remarks

In this paper, by improving the selection of cover element, a novel robust steganographic algorithm is well-devised, which can resist against JPEG compression attack. Relying on the sign invariance of the selected DCT coefficients before and after JPEG compression, we successfully complete the robust steganography, even though the transmission channel starts the compression attack. It

² In this context, we address the "Moment" function of WeChat, in which images can be shared with user's friends on SNP.

is worth noting that we comprehensively evaluate the effectiveness of the proposed algorithm, referring to imperceptibility, capacity, undetectability, and robustness. Compared with the original sign steganography, by addressing the importance of cover element, we indeed further improve the robustness and undetectability of the proposed sign steganography while basically remaining the imperceptibility and capacity. To our knowledge, few literature address the four principles together for evaluating a steganographic scheme in the current study, in which robustness usually cannot attract much attention. In fact, the robust performance of stego image plays an important role in moving steganography from laboratory to the real-world such as SNP.

In comparison with the baseline algorithms, our proposed steganographic algorithm performs superior robustness, both in the simulated transmission channel and practical channel of SNP. While we have to admit that the undetectability of stego image with high payload is the limitation of our robust steganography. Alternatively, we can assign the secret bits (high payload) into multiple images with groups of bits (low payload), in order to reduce the risk of detection by steganalysis. Nevertheless, in the future study, we need to further enhance the robust steganographic algorithm, and strike the balance between undetectability and robustness.

Declaration of Competing Interest

We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled, Robust Steganography Resisting JPEG Compression By Improving Selection of Cover Element.

CRedit authorship contribution statement

Tong Qiao: Writing - original draft, Conceptualization, Methodology, Software. **Shuai Wang:** Visualization, Software, Validation. **Xiangyang Luo:** Supervision, Writing - review & editing. **Zhiqiang Zhu:** Writing - review & editing.

Acknowledgements

This work was supported by the Natural Science Foundation of China under grant (No. 61702150, U1804263, U1636219, U1736214), Zhongyuan Science and Technology Innovation Leading Talent Project (No. 214200510019), the Public Research Project of Zhejiang Province under grant No. LGG19F020015, the National Key R&D Program of China (2016YFB0801303 and 2016QY01W0105).

References

- [1] T. Filler, J. Fridrich, Gibbs construction in steganography, *IEEE Trans. Inf. Forensics Secur.* 5 (4) (2010) 705–720.
- [2] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, *EURASIP Journal on Information Security* 2014 (1) (2014) 1.
- [3] L. Guo, J. Ni, Y.-Q. Shi, Uniform embedding for efficient jpeg steganography, *IEEE Trans. Inf. Forensics Secur.* 9 (5) (2014) 814–825.
- [4] B. Li, M. Wang, J. Huang, X. Li, A new cost function for spatial image steganography, in: 2014 IEEE International Conference on Image Processing (ICIP), 2014, pp. 4206–4210.
- [5] L. Guo, J. Ni, W. Su, C. Tang, Y.-Q. Shi, Using statistical image model for jpeg steganography: uniform embedding revisited, *IEEE Trans. Inf. Forensics Secur.* 10 (12) (2015) 2669–2680.
- [6] T. Qiao, C. Zitzmann, R. Cogranne, F. Retraint, Detection of jsteg algorithm using hypothesis testing theory and a statistical model with nuisance parameters, in: *Proceedings of the 2nd ACM workshop on Information Hiding and Multimedia Security (IH & MMSec)*, 2014, pp. 3–13.
- [7] X.-F. Song, F. Liu, C. Yang, X. Luo, Y. Zhang, Steganalysis of adaptive jpeg steganography using 2D gabor filters, in: *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, ACM, 2015, pp. 15–23.
- [8] T. Qiao, F. Retraint, R. Cogranne, C. Zitzmann, Steganalysis of jsteg algorithm using hypothesis testing theory, *EURASIP Journal on Information Security* 2015 (1) (2015) 1–16.
- [9] J. Ye, J. Ni, Y. Yi, Deep learning hierarchical representations for image steganalysis, *Information Forensics and Security, IEEE Transactions on* 12 (11) (2017) 2545–2557.
- [10] M. Boroumand, M. Chen, J. Fridrich, Deep residual network for steganalysis of digital images, *IEEE Trans. Inf. Forensics Secur.* 14 (5) (2018) 1181–1193.
- [11] Y. Ma, X. Luo, X. Li, Z. Bao, Y. Zhang, Selection of rich model steganalysis features based on decision rough set α -positive region reduction, *Circuits and Systems for Video Technology, IEEE Transactions on* 29 (2) (2019) 336–350.
- [12] T. Qiao, X. Luo, T. Wu, M. Xu, Z. Qian, Adaptive steganalysis based on statistical model of quantized dct coefficients for jpeg images, *IEEE Trans Dependable Secure Comput* (2019).
- [13] V. Holub, J. Fridrich, Designing steganographic distortion using directional filters, in: 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, pp. 234–239.
- [14] B. Li, M. Wang, X. Li, S. Tan, J. Huang, A strategy of clustering modification directions in spatial image steganography, *IEEE Trans. Inf. Forensics Secur.* 10 (9) (2015) 1905–1917.
- [15] T. Denemark, J. Fridrich, Improving steganographic security by synchronizing the selection channel, in: *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, 2015, pp. 5–14.
- [16] W. Zhang, Z. Zhang, L. Zhang, H. Li, N. Yu, Decomposing joint distortion for adaptive steganography, *IEEE Trans. Circuits Syst. Video Technol.* 27 (10) (2016) 2274–2280.
- [17] W. Su, J. Ni, X. Hu, J. Fridrich, Image steganography with symmetric embedding using Gaussian Markov random field model, *IEEE Trans. Circuits Syst. Video Technol.* (2020).
- [18] Z. Zhu, N. Zheng, T. Qiao, M. Xu, Robust steganography by modifying sign of dct coefficients, *IEEE Access* 7 (2019) 168613–168628.
- [19] Y. Zhang, X. Luo, C. Yang, D. Ye, F. Liu, A jpeg-compression resistant adaptive steganography based on relative relationship between dct coefficients, in: 2015 10th International Conference on Availability, Reliability and Security (ARES), 2015, pp. 461–466.
- [20] Y. Zhang, X. Luo, C. Yang, F. Liu, Joint jpeg compression and detection resistant performance enhancement for adaptive steganography using feature regions selection, *Multimed Tools Appl* 76 (3) (2017) 3649–3668.
- [21] Y. Zhang, X. Zhu, C. Qin, C. Yang, X. Luo, Dither modulation based adaptive steganography resisting jpeg compression and statistic detection, *Multimed Tools Appl* 77 (14) (2018) 17913–17935.
- [22] Y. Zhang, C. Qin, W. Zhang, F. Liu, X. Luo, On the fault-tolerant performance for a class of robust image steganography, *Signal Processing* 146 (2018) 99–111.
- [23] Z. Bao, Y. Guo, X. Li, Y. Zhang, M. Xu, X. Luo, A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients, *Journal of Ambient Intelligence and Humanized Computing* 11 (5) (2020). 1903–1903
- [24] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, N. Yu, Robust adaptive steganography based on generalized dither modulation and expanded embedding domain, *Signal Processing* 168 (2020) 107343.
- [25] Z. Zhao, Q. Guan, H. Zhang, X. Zhao, Improving the robustness of adaptive steganographic algorithms based on transport channel matching, *IEEE Trans. Inf. Forensics Secur.* 14 (7) (2018) 1843–1856.
- [26] J. Tao, S. Li, X. Zhang, Z. Wang, Towards robust image steganography, *IEEE Trans. Circuits Syst. Video Technol.* 29 (2) (2019) 594–600.
- [27] Y. Zhang, X. Luo, Y. Guo, C. Qin, F. Liu, Multiple robustness enhancements for image adaptive steganography in lossy channels, *IEEE Trans. Circuits Syst. Video Technol.* 30 (8) (2019) 2750–2764.
- [28] F. Li, K. Wu, C. Qin, J. Lei, Anti-compression JPEG steganography over repetitive compression networks, *Signal Processing* (2020) 107454.
- [29] Z. Yin, L. Ke, Robust adaptive steganography based on dither modulation and modification with re-compression, *arXiv preprint arXiv:2007.08301* (2020).
- [30] P. Bas, T. Filler, T. Pevný, “break our steganographic system”: The ins and outs of organizing boss, in: *Proceedings of the 13th International Conference on Information Hiding (IH)*, 2011, pp. 59–70.
- [31] J. Kodovsky, J. Fridrich, V. Holub, Ensemble classifiers for steganalysis of digital media, *IEEE Trans. Inf. Forensics Secur.* 7 (2) (2012) 432–444.
- [32] T. Pevný, J. Fridrich, Merging markov and dct features for multi-class jpeg steganalysis, in: *Security, Steganography, and Watermarking of Multimedia Contents IX*, 6505, 2007, p. 650503.