A Robust Image Steganography on Resisting JPEG Compression with No Side Information

Z. Bao, X. Luo, Y. Zhang, C. Yang and F. Liu

State Key Laboratory of Mathematical Engineering and Advanced Computing, China and Zhengzhou Science and Technology Institute, Zhengzhou 450001, People's Republic of China

ABSTRACT
Robust JPEG steganographic algorithms are proposed to transmit covert message against JPEG compression. The existing robust JPEG steganographic algorithms are working with the side information about JPEG compression quality factor of a lossy channel. However, massive recent experimental results reveal that the performance of the present robust JPEG steganographic algorithms is poor if the side information is unknown. Thus, this paper proposes a new robust JPEG steganographic algorithm to satisfy the requirement. First, the error diffusion of steganographic embedding encoder is analyzed. Then, a new robust JPEG steganographic algorithm is proposed based on the analysis result. A series of experiments are conducted on 10,000 images from BOSSbase 1.01 image library. The results show that the proposed method can resist JPEG compression efficiently with acceptable resistance to steganalysis statistical detection.

KEYWORDS
Detection resistant; JPEG compression resistant; Lossy channel analysis; No side information; Robust steganography; Steganographic embedding

1. INTRODUCTION
Steganography is an art of covert communication [1–5]. It can transmit secret message through public communication channels without causing attention of watcher, especially in a controlled communicating situation (such as prisoner-communication in the prison under the monitoring of guard). In recent years, with the development of mobile communication technology, many social medias such as FaceBook, WeChat, and Instagram transmit enormous images through intelligent mobile terminal [6]. JPEG compression is always applied on the images of social medias after considering the bandwidth, tariff, traffic and other restrictions of intelligent mobile terminal. This kind of lossy operation often destroys the message hidden by traditional steganographies [7]. Therefore, robust steganography on resisting JPEG compression is proposed to protect the message against the lossy compression with acceptable resistance to steganalysis statistical detection, and then it is the focus of this manuscript.

When it comes to the words “robust steganography”, it is natural to think of “robust watermark”. The robust watermarking technology has been researched for more than two decades, and some kinds of robust watermarking methods (such as spread spectrum modulation [8], feature-based algorithm [9], and scale invariant feature transformation [10]) are proposed to reduce the effect of various lossy operations on cover image object. In general speaking, the priority purpose of robust watermarking is to guarantee the existence of embedded information against the various attacks (such as JPEG compression, rotation, cropping, down-sampling, and so on), and the completeness of the embedded information is on the second stage [11]. Meanwhile, the designs of most robust watermarking ignore the ability of resisting steganalysis detection for there is no related requirement [12]. Thus, the robust watermarking algorithm cannot be simply used as a steganography to transfer secret message on security consideration.

In recent years, the adaptive steganography becomes a hotspot in the research of information hiding [1,2]. A design is widely used by the recent adaptive steganographies – “embedding cost function + steganographic embedding code” [13]. The cooperation between the function and embedding code (STCs, Syndrome Trellis Codes [14]) can concentrate embedding modifications to the proper areas (hard to detect the change on them) [1,13,15,16]. Because the embedding cost function mainly influence the distribution of modifications on cover image, many embedding cost functions are proposed in the recent proposed adaptive JPEG steganographies, such as New Perturbed Quantization [17] algorithm, Uniform Embedding Distortion [18] (UED) algorithm, Efficient Block-entropy Steganographic scheme [19] algorithm and JPEG UNiversal
These adaptive steganographic algorithms work in the lossless communication channel and receive high performance on resisting steganalysis statistical detection methods [21–24].

Nevertheless, the above adaptive steganographic algorithms suffer setbacks in the lossy channel, and robust steganographic algorithm is proposed to protect the embedded message. In the previous work, Zhang et al. proposed robust steganographic algorithms DCT Coefficient Relationship-based Adaptive Steganography (DCRAS [7]) and Feature Region-based Adaptive Steganography (FRAS [25]), and they can resist JPEG compression efficiently with acceptable detection resistance. However, these robust algorithms need to know the quality factor of the JPEG compression used in the lossy channel (side information), and they can hardly protect the embedded message if the lossy channel compresses the stego object in a different quality factor.

To solve the problem above, a new robust JPEG steganography with no side information is proposed in this manuscript. A series of experiments are conducted on 10,000 images from BOSSBase 1.01 image library, and the results reflect that the proposed robust JPEG steganographic algorithm can resist JPEG compression in a quality factor range (65,85) with acceptable resistance to steganalysis statistical detection. The main works of this manuscript are as follows:

1. The error diffusion of steganographic embedding code STCs is analyzed. The relationship between the parameters of STC and the error probability of extracted message in the lossy channel is pointed out: the height and width of sub-matrix of STCs have a positive correlation with the error probability of extracted message.
2. A new robust JPEG steganographic algorithm with no side information is proposed. It is based on the error diffusion analysis result and the relationship between DCT coefficients. The method of reduction error diffusion in the lossy channel can apply to another robust JPEG steganography.

The rest of this manuscript is organized as follows. Section 2 introduces the related researches of adaptive JPEG steganography and robust JPEG steganography. Then, the analysis of error diffusion of STCs in the lossy channel and the proposed robust JPEG steganographic algorithm are described in Sections 3 and 4, respectively. In Section 5, the results of comparative experiments on resisting JPEG compression and steganalysis detection are presented. Section 6 summarizes the full manuscript.

2. RELATED WORKS

2.1 Adaptive JPEG Steganography

A JPEG image is obtained from an original spatial image through several processes, such as color space conversion, down-sampling, $8 \times 8$ blocking, applying block DCT transformation independently, quantizing the resulting DCT coefficients by quality factor (QF) to integer numbers, and encoding the coefficients for the storage operation. The embedding modification of JPEG adaptive steganography algorithm is usually applied on the rounded DCT coefficients after quantizing.

Many adaptive JPEG steganographic algorithms are composed of embedding cost function and steganographic embedding code. This framework [13] is originated from the minimal distortion model proposed by Fridrich et al. [26]. It achieves good performance on resisting detection for the embedding modifications are hidden in the DCT coefficients with higher resistance to detection. On the research of how to define proper embedding cost function, Holub et al. proposed an adaptive steganographic algorithm J-UNIWARD on JPEG image in the article [20]. Wavelet decomposition coefficients are used to describe the suitability of an element on resisting statistical detection. The embedding cost function $DF(X, Y)$ on cover and stego DCT coefficient sequences $X$ and $Y$ is defined as follows:

$$DF(X, Y) = DF(J^{-1}(X), J^{-1}(Y))$$

$$= \sum_{r, u, v} \frac{|W_{uv}^{(r)}(J^{-1}(X)) - W_{uv}^{(r)}(J^{-1}(Y))|}{\varepsilon + |W_{uv}^{(r)}(J^{-1}(X))|},$$

where $J^{-1}(\cdot)$ is the inverse function that transforms the DCT coefficients to spatial domain, $W_{uv}^{(r)}$ denotes the $uv$th coefficient of $r$th ($r = 1, 2, 3$) wavelet decomposition, and $\varepsilon > 0$ is used to prevent the molecule from zero (in current, $\varepsilon = 10^{-5}$).

2.2 Robust JPEG Steganography

In [7], we proposed a framework for designing a robust steganographic algorithm. The framework combines the robust measure of robust watermarking with the design of adaptive steganographic algorithm, in order to resist both JPEG compression and steganalysis detection.
In the framework, for the sender, the embedding domain is determined first; then, design the message embedding modification method with strong robustness to JPEG compression; then, the embedding cost function is defined to elevate the resistance to steganalysis detection; in the next, the error correction coding is applied to further improve the robustness of embedded message. Finally, use the steganographic embedding code to embed the message into the cover object through the designed modification method above. For the receiver, the STCs is first decoded to obtain the interfered information flow, and then the error correction code is used to reduce the bit error rate, and finally get the original embedded message.

Based on the robust JPEG steganographic framework above, DCRAS and FRAS algorithms are also proposed in articles [7,25]. DCRAS and FRAS algorithm owns much better JPEG compression resisting performance than typical adaptive JPEG steganographic algorithm, such as J-UNIWARD, UED, and so on. But they need the side information about the quality factor of the attacking JPEG compression. If the stego object is suffered by a JPEG compression with a different quality factor. These algorithms can no longer protect the embedded message any more. That is because the quality factor is used to generate the robust cover object against JPEG compression, and the generated object is strong related to the quality factor in these algorithms. How to generate a robust cover object without the knowledge of quality factor is needed for robust JPEG steganography. On this problem, this paper will propose a new robust JPEG steganographic algorithm.

3. ERROR DIFFUSION OF STCS

3.1 Construction of STCs Embedding Matrix

The main purpose of the steganographic embedding code is to minimize the cost value caused by embedding the secret message in the steganographic algorithm. The most popular embedding form is matrix embedding [1], and it can be described as

$$\arg \min_{y} \{D(x, y) | \text{msg} = y \cdot H^t\},$$

(2)

where $x = \{x_1, x_2, \ldots, x_n\}$, $y = \{y_1, y_2, \ldots, y_n\}$ denote the cover object and stego object of $n$ length, respectively. And $\text{msg} = \{\text{msg}_1, \text{msg}_2, \ldots, \text{msg}_m\}$ denotes the secret message with $m$ bits. $H$ denotes the embedding matrix, and $D(x, y)$ is the embedding cost function describing the distortion caused by changing cover element. How to find a $y$ that satisfies Equation (2) is the main purpose of steganographic embedding coding.

At present, most algorithms of the adaptive steganography and robust steganography use STCs [14] to embed a secret message into the cover object. STCs embedding code is based on the idea of the Viterbi decoding algorithm and find suitable solution of $y$ by limited exhaustive, pruning, and traceable operations. A brief example of STCs is presented in Figure 1. From the example, we can see that the STCs algorithm can work efficiently because of the special construction of the embedding matrix $H$, and the detail of $H$ is shown in Figure 2.

From the figure we can see that, $H$ is composed by $m$ sub-matrices $\hat{H}$ lined in diagonal. Notice that some rows of the last $h - 1$ sub-matrices are deleted to guarantee the size of $H$ is $m \times n$. This special construction makes the

\[ H = \left( \begin{array}{cccc} \hat{H} & \hat{H} & \hat{H} & \hat{H} \end{array} \right) \quad \hat{h} = \begin{pmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix} \]

Figure 2: Construction of embedding matrix used in the STCs

Figure 1: Example of STCs embedding code
The sender can find a stego nearly satisfies Equation (2) by the exhaustive process, and the computational complexity is acceptable on a personal computer. Embedding experiments in the article [14] show that the performance of STCs is gradually near to the theoretical bound with the height of $\tilde{H}$ grows.

### 3.2 Analysis of Error Diffusion

In the lossy channel of JPEG compression, the DCT coefficients are changed and caused error bits in the steganographic extraction process. Article [6] points out that the occurrence of error bits in robust stego object of DCRAS after JPEG compression is random.

We suppose the error probability of the robust stego object $y_{1\times n}$ after JPEG compression is $p_{err}$. $y$ is generated by STCs with $H_{m\times n}$, and the embedding matrix is composed by $m$ sub-matrices $\tilde{H}_{b\times w}$. According to Equation (2) of matrix embedding, the embedded $m$ bits message $msg_{1\times m}$ is extracted on the binary field by

$$msg = y \cdot H^t. \quad (3)$$

The construction of $H$ indicates that an element $y_a$ of $y$ effects $h$ elements in the extracted message. It is because the other elements of the corresponding column of $y_a$ are definitely 0. On the other hand, for the same reason, an element $m_b$ of $msg$ is influenced by $hw$ continuous elements of $y$. Thus, the error bits number expectation $E(H_{err}(m_b))$ on the row of $H$ corresponding to $m_b$ is

$$E(H_{err}(m_b)) = hw \times p_{err} \times p_1, \quad (4)$$

where the symbol $p_1$ denotes the probability of “1” elements in sub-matrix $\tilde{H}$. As described in [11], the elements of $\tilde{H}$ are suggested to be chosen randomly chosen from set $\{0, 1\}$, $p_1$ can be regarded as 1/2. Thus, the error probability of the elements in $\tilde{H}$ is $p_{err}/2$. Notice that the computation of Equation (3) is on the binary field, and $1 \oplus 1 = 0$ on this field. It means that if the number of errors is even, the extracted message is correct. Because the extracted message $m_b$ is computed by $hw$ elements from $\tilde{H}$, the error probability $p_{mb}$ of $m_b$ can be expressed as

$$p_{mb} = \sum_{1 \leq i \leq hw, \text{mod}(i) = 1} C_i^h \frac{p_{err}}{2} \cdot \left(1 - \frac{p_{err}}{2}\right)^{hw-i}. \quad (5)$$

Because the value of $p_{err}$ is less than 0.1 in many situations based on the experiments in [4], $p_{mb}$ can be estimated by

\[
p_{mb} \approx hw\left(\frac{p_{err}}{2}\right)(1 - \frac{p_{err}}{2})^{hw-1} + \frac{hw(hw-1)(hw-2)}{6} \left(\frac{p_{err}}{2}\right)^3(1 - \frac{p_{err}}{2})^{hw-3}.
\]

From Equation (6), we can get that, the larger values of height and width of $\tilde{H}$ cause higher error probability of extracted message in the lossy channel.

### 4. PROPOSED ROBUST STEGANOGRAPHIC ALGORITHM

In this section, the robust steganographic algorithm without side information of quality factor is proposed. The basic flow chart of the proposed algorithm is shown in Figure 3, which mainly includes generating robust virtual cover object, defining embedding cost function, coding the secret message by error correction encoder, reducing the error diffusion of STCs, embedding coded message through STCs and the corresponding extracting algorithms. This section will introduce how to generate the robust virtual cover object, define the embedding cost function and reduce the error diffusion.

#### 4.1 Construction of Robust Virtual Cover Object

Based on the relative relationship between DCT coefficients, a robust against JPEG compression virtual cover object is generated:

1. Decoding the JPEG image $I$ to achieve a set of nonoverlapping $8 \times 8$ DCT coefficients blocks $D_k = \{D_k(i), i = 1, 2, \ldots, 64\}$, $k = 1, 2, \ldots, B$. $B$ is the number of the blocks, and $D_k(i)$ is the $i$th coefficient in the $k$th block.

2. Generating robust virtual cover object $X = \{x_1, x_2, \ldots, x_n\}$ based on the relationship between coefficient $D_k(i)$ and $M_{ki}$. The symbol $M_{ki}$ is the rounded mean value of three DCT coefficients $D_{ki1}(i), D_{ki2}(i), D_{ki3}(i)$ at the same in-block position of three neighboring blocks. The element $x_j$ of the generated cover object $X$ satisfying:

\[
x_j = \begin{cases} 
0, & \text{if } D_k(i) \leq M_{ki}, \\
1, & \text{if } D_k(i) > M_{ki},
\end{cases}, \quad 1 \leq j \leq n, \quad (7)
\]

Then, robust virtual stego object $Y = \{y_1, y_2, \ldots, y_n\}$ is obtained after embedding message into the virtual cover object $X$. A corresponding mapping rule from the robust
virtual stego object $Y$ to the DCT coefficients $\{D_k\}_{1 \leq k \leq B}$ is presented:

$$D^Y_k(i) = \begin{cases} 
M_{ki} + \sigma_{ki}, & \text{if } y_j = 1 \& D_k(i) < M_{ki} + \sigma_{ki}, \\
M_{ki} - \sigma_{ki}, & \text{if } y_j = 0 \& D_k(i) > M_{ki} - \sigma_{ki}, \\
D_k(i), & \text{else. }
\end{cases}$$

(8)

Last, for the receiver, the extracted stego object after compression is denoted as $\hat{Y}$, and the extracting rule is

$$\hat{y}_j = \begin{cases} 
0, & \hat{D}_k(i) \leq \hat{M}_{ki}, \\
1, & \hat{D}_k(i) > \hat{M}_{ki},
\end{cases}$$

(9)

where the symbols $\hat{D}$, $\hat{D}_k = \{\hat{D}_k(i), i = 1, 2, \ldots, 64\}$ and $\{\hat{M}_{ki}\}_{k,i}$, respectively, denote the sets of DCT coefficients, $8 \times 8$ blocks and neighboring mean values after JPEG compression. (3) To determine the value of $\sigma_{ki}$ in formula (8) of step II is presented as follows:

$$\sigma_{ki} = \begin{cases} 
1, & \text{if } D^\text{max}_k(i) - D^\text{min}_k(i) \leq T, \\
2, & \text{if } T_1 \leq D^\text{max}_k(i) - D^\text{min}_k(i) \leq T_2, \\
3, & \text{if } D^\text{max}_k(i) - D^\text{min}_k(i) > T_2,
\end{cases}$$

(10)

where $D^\text{max}_k(i) = \max\{D_k(i), D_{k_1}(i), D_{k_2}(i), D_{k_3}(i)\}$ is the maximum value among the four coefficients, $D^\text{min}_k(i) = \min\{D_k(i), D_{k_1}(i), D_{k_2}(i), D_{k_3}(i)\}$ is the minimum value, $T_1, T_2 (T_1 < T_2)$ are the threshold values determined by user, a suggested value of $(T_1, T_2)$ is $(15, 30)$ according to the experiments in [24].

### 4.2 Design of Embedding Cost Function

After the robust virtual cover object is created, the popular minimal distortion model [13,26] is used to concentrate the embedding modifications on the elements in the less distortion region to increase the performance on resisting detection. First, embedding cost function is defined to describe the distortion value caused by embedding message on cover object $X$. The cost function is designed based on the combination of the J-UNIWARD embedding cost function $DF(D, \hat{D})$ [18] of formula (1) and the robust virtual cover object. It is shown as follows:

$$DF(x_j, y_j) = \begin{cases} 
0, & x_j = y_j, \\
\rho^{(1)}_{ki}, & \{x_j = 0 \& M_{ki} + \sigma_{ki} - D_k(i) = 1\}, \\
\rho^{(2)}_{ki}, & \{x_j = 0 \& M_{ki} + \sigma_{ki} - D_k(i) = 2\}, \\
wet\_cost, & \text{else,}
\end{cases}$$

(11)

where $\rho^{(1)}_{ki}$ and $\rho^{(2)}_{ki}$, respectively, denote the cost values $DF(D_k(i), \hat{D}_k(i))$ of modification magnitude 1 and 2 in the J-UNIWARD embedding cost function, and wet\_cost denote the cost value that not advanced to be modified in the STCs embedding process (usually be set to a quite large value such as $10^8$). Then, the robust virtual stego object $Y$ is obtained after embedding secret message into $X$ by STCs code, and the modification is mapped into image DCT coefficients $D_k$ by formula (8) to obtain the DCT coefficients stego object.
4.3 Reduction of Error Diffusion

Based on the analysis result Section 3.2, the error probability can be reduced by shrinking the $hw$ of sub-matrix $\tilde{H}$. Because the height $h$ of $\tilde{H}$ effects, the performance of steganographic embedding and computational complexity a lot, the value of $h$ is often in the range $h \in 8, 9, 10, 11, 12$ on embedding efficiency and complexity consideration. Another way to reduce the error diffusion of STCs in Section 3.1, the value of $\alpha$ considered.

Thus, we can increase the embedding rate of STCs by following steps:

I. Sort the elements of robust virtual cover object $X$ computed from the same in-block position $(i, j), i, j \in \{1, 2, \ldots, 8\}$ of $8 \times 8$ DCT coefficients in a row sort($X(i, j)), i, j \in 1, 2, \ldots, 8$.

II. Compute the required length $n_{rd}$ of virtual cover object based on the reduced embedding rate $\alpha$.

III. Select $n_{rd}$ elements from the set $\{\text{sort}(X(i, j)), i, j \in \{1, 2, \ldots, 8\}\}$ in an order shared by the sender and receiver.

The sort of the $X$ is to make the elements in the same in-block position adjoined in the selected $n_{rd}$ elements virtual cover object. This process is to increase the ability of resisting detection of the proposed method. As shown in Figure 4, it tells that the embedding modifications of J-UNIWARD are related to the in-block position, and concentrate to the low-frequency positions. Thus, we suggest the first 10 sort($X(i,j)$) in a permutation as

$$(s(X(1, 3)), s(X(1, 2)), s(X(1, 1)), s(X(2, 1)), s(X(3, 1))$$

$s(X(2, 2)), s(X(3, 2)), s(X(2, 3)), s(X(4, 1)), s(X(1, 4)))$.  

(12)

Then, error correction encoder RS [27] with parameter $(6,15)$ is applied on the secret message, and the robust virtual stego object is obtained after embedding the encoded secret message into the selected $n_{rd}$-element virtual cover object by STCs code. The modifications are mapped into image DCT coefficients $D_k$ by formula (8) to obtain the DCT coefficients stego object.

5. EXPERIMENTS

5.1 Experimental Setups

The experimental results were carried out by the Matlab R2010a, and the spatial image database used in the experiments was BOSSbase v1.01 (proposed by Patrick Bas, Tomas Filler, Tomas Pevny at ICASSP 2013, containing 10,000 images of size 512 × 512, download: http://agents.fel.cvut.cz/stegodata/), the image database contains natural scenery, artificial facilities, and human portraits pictures, at the same time, the photos are shot from eight cameras of different companies to ensure the diversity.

In the resisting JPEG compression experiments, the measure of resisting JPEG compression of the steganographic algorithm is the extraction error rate $R_{\text{error}}$, which is defined as the ratio of the bit-length num$_{\text{error}}$ of the errors in the extracted message after the stego object is JPEG compressed to the bit-length $m$ of the original embedded secret message, that is, $R_{\text{error}} = \frac{\text{num}_{\text{error}}}{m}$. The closer value to 0 indicates the higher performance on resisting JPEG compression.

In the resisting detection experiment, the popular detection features (such as ccPEV [28] and DCTR [23] detection feature libraries with 548 and 8000 dimensions, respectively) are extracted from the cover image set and stego image set. Then half of the features are used to train the classifier and use the trained classifier to classify the remaining images to test the detection resisting performance of steganographic algorithm. The measurement is “out of bag estimate of the testing error”, and denoted as $E_{\text{Oob}}$, which is an unbiased value and indicates the test error rate of the classifier. The higher the value, the better performance of the steganographic algorithm owns.
5.2 Experiments of Resisting JPEG Compression

In this section, we randomly select 1000 spatial images from the BOSSbase v1.01 image database to, respectively, generate 1000 cover images when quality factor is 75, and then use J-UNIWARD [20], robust watermarking algorithm [29], DCRAS [7] and the improved method in this paper to transmit secret message. The embedding rate varies from 0.01 bpnzAC (bits per non-zero Alternating Current coefficient) to 0.1 bpnzAC with 0.01 interval and 1000 stego images are generated on each embedding rate with each embedding algorithm. To simulate the no side information of quality factor of JPEG lossy channel, the stego images generated by DCRAS algorithm are obtained to resist 80 quality factor JPEG compression. Then, the JPEG compression attacks with the quality factor of 65, 75, and 85 are applied to the stego images. Then, the corresponding message extraction algorithms are run after the lossy compression, and the extracted message is compared with the original message by bit. Last, the extraction error rates $R_{error}$ of the tested methods are calculated, and the results are shown in Figures 5–7.

It can be seen from the figures that the secret carriers obtained by J-UNIWARD algorithm and DCRAS algorithm are unable to resist the lossy compression. At the same time, the extraction error rate of the robust watermarking algorithm in the [29] is between 3% and 10%. It owns better JPEG compression resisting performance than typical adaptive JPEG steganographic algorithm but the error rate is still high. The correctness rate of the extraction error rate of the proposed algorithm about 0.3–3%, and it means that the proposed algorithm can resist JPEG compression efficiently.

5.3 Experiments of Resisting Statistical Detection

In this section, we construct the cover image set with QF = 75 from all 10,000 spatial images in the BOSSbase v1.01 image database, and test the resisting performance of detection on the proposed algorithm, the robust watermarking algorithm [29], and DCRAS [7] algorithm. The embedding rate varied from 0.01 to 0.1 bpnzAC, 10,000 stego images are generated on each embedding rate with different testing algorithms. Then, the detection features of the cover set and the stego set are extracted by the detection feature library, and then the ensemble integration classifier [30] is trained by the extracted features (from 5000 cover-stego pairs). In the next, the trained classifier is used to classify the remaining 10,000 images (5000 cover images and 5000 stego images are random distributed). The results of $E_{coob}$ are shown in
Figure 8: Results of resisting detection on cover object of quality factor 75

Figure 8, where Figure 8(a) presents the results on detection library ccPEV [28] (a typical library of 548 features), and Figure 8(b) shows the results of the DCTR detection algorithm (DCTR is one of the most effective detection library for JPEG steganography, and it contains 8000 features [23]). It can be seen from Figure 8 that the detection error rate $E_{\text{oob}}$ of robust watermarking algorithm is low, the possible reason is that the anti-detectability is not considered in the design of robust watermarking algorithm, resulting in the embedded image is easy to be detected. At the same time, the $E_{\text{oob}}$ of the proposed algorithm is less than the $E_{\text{oob}}$ of DCRAS algorithm at most 7%. This is because the STC used in the proposed method only to find the solution of Equation (2) in a part of the whole cover object, and better solution can be found if considering the whole cover object. Thus, the ability of the proposed method is reduced when compared to DCRAS algorithm.

6. CONCLUSIONS

In view of the problem that the JPEG compression quality factor is unknown in some lossy channels. This paper proposed a new robust JPEG steganographic algorithm to satisfy the situation without knowledge of JPEG compression quality factor. It generates a robust virtual cover object based on the relationship between DCT coefficients. A series of experiments are conducted and the results show that the proposed robust algorithm can achieve high extraction accuracy in various JPEG compression situations without knowing the quality factor of compression and can resist steganalysis statistical detection methods.

Without any doubts, better coding performance can be obtained if the steganographic embedding code is combined with the error correction code, it may be the focus of the next work. How to elevate the extraction accuracy to 100% is a curious question. Furthermore, exploiting new method to resist stronger lossy attacks (such as rotation, cropping, down-sampling, etc.) is another interesting topic of robust steganography.

FUNDING

This work was supported by National Natural Science Foundation of China: [grant number 61572052, 61772549, U1636219, U1736119, U1736214]; National Key R&D Plan: [grant number 2016QY 01W0105, 2016YFB0801303]; Key Technologies R&D Program of Henan Province: [grant number 162102210032]; and Plan for Scientific Innovation Talent of Henan Province: [grant number 2018J0018].

ORCID

X. Luo □ http://orcid.org/0000-0003-3225-4649

REFERENCES

1. A. D. Ker, P. Bas, R. Bohme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevny, “Moving steganography and steganalysis from the laboratory into the real world,” in Proceedings of ACM Workshop on Information Hiding and Multimedia Security, Montpellier, 2013, pp. 45–58.

2. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge: Cambridge University Press, 2009.

3. C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, “An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism,” IEEE Trans. Circuits Syst. Video Technol., Vol. 23, no. 7, pp. 1109–18, 2013.

4. C. Qin, C. C. Chang, and Y. P. Chiu, “A novel joint data-hiding and compression scheme based on SMVQ and image inpainting,” IEEE Trans. Image Process., Vol. 23, no. 3, pp. 969–78, 2014.
5. C. Qin, C. C. Chang, and T. J. Hsu, “Reversible data hiding scheme based on exploiting modification direction with two steganographic images,” *Multimedia Tools Appl.*, Vol. 74, no. 15, pp. 5861–72, 2015.

6. Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, “On the fault-tolerant performance for a class of robust image steganography”, *Signal Process.*, Vol. 146, pp. 99–111, Feb. 2018.

7. Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, “A framework of adaptive steganography resisting JPEG compression and detection,” *Secur. Commun. Netw.*, Vol. 9, no. 15, pp. 2957–71, Apr. 2016.

8. G. Tiwari, “A review on robust watermarking with its applications and comparative analysis,” *Int. J. Signal Process. Image Process. Pattern Recognit.*, Vol. 8, no. 6, pp. 85–90, Jun. 2015.

9. J. S. Tsai, W. B. Huang, Y. H. Kuo, and M. F. Horng, “Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions,” *Signal Process.*, Vol. 92, no. 6, pp. 1431–45, Jun. 2012.

10. E. D. Tsoungis, G. A. Papakostas, D. E. Koulouriotis, and V. D. Tourassis, “Performance evaluation of moment-based watermarking methods: A review,” *J. Syst Softw.*, Vol. 85, no. 8, pp. 1864–84, Sep. 2012.

11. X. Y. Wang, Y. N. Liu, H. Xu, A. L. Wang, and H. Y. Yang, “Blind optimum detector for robust image watermarking in nonsubsampled shearlet domain,” *Inf. Sci.*, Vol. 372, pp. 634–54, Apr. 2016.

12. C. C. Chang, T. S. Nguyen, and C. C. Lin, “A reversible compression code hiding using soc and smvq indices,” *Inf. Sci.*, Vol. 300, pp. 85–99, Jul. 2015.

13. T. Filler, and J. Fridrich, “Design of adaptive steganographic schemes for digital images,” in *Proc. IS&T/SPIE Electronic Imaging, Media Watermarking, Security, and Forensics XIII*, Vol. 7880, pp. 0F–1–0F–14, Feb. 2011.

14. T. Filler, J. Judas, and J. Fridrich, “Minimizing embedding impact in steganography using trellis-coded quantization,” in *Proc. IS&T/SPIE Electronic Imaging, Media Forensics and Security XII*, Vol. 7541, pp. 05–1–05–14, Mar. 2010.

15. B. Li, S. Tan, M. Wang, and J. Huang, “Investigation on cost assignment in spatial image steganography,” *IEEE Trans. Inf. Forensics Sec.*, Vol. 9, no. 8, 1264–77, Sep. 2014.

16. V. Holub and J. Fridrich, “Designing steganographic distortion using directional filters,” in *Proceedings of IEEE International Workshop on Information Forensics & Security*, Guangzhou, 2013, pp. 234–9.

17. F. Huang, J. Huang, and Y. Shi, “New channel selection rule for JPEG steganography,” *IEEE Trans. Inf. Forensics Sec.*, Vol. 7, no. 4, pp. 1181–91, Apr. 2012.

18. L. Guo, J. Ni, and Y. Shi, “An efficient JPEG steganographic scheme using uniform embedding,” in *Proceedings of the IEEE International Workshop on Information Forensics and Security*, Costa Adeje, Tenerife, 2012, pp. 169–74.

19. C. Wang and J. Ni, “An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients,” in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, Kyoto, 2012, pp. 1785–8.

20. V. Holub, J. Fridrich, and T. Denemark, “Universal distortion function for steganography in an arbitrary domain,” *EURASIP J. Inf. Sec.*, Vol. 2014, no. 1, 1–13, Jan. 2014.

21. J. Kodovský, and J. Fridrich, “Calibration revisited,” in *Proceedings of the 11th ACM Workshop on Multimedia and Security*, Princeton, NJ, 2009, pp. 63–74.

22. J. Fridrich, and J. Kodovský, “Rich models for steganalysis of digital images,” *IEEE Trans. Inf. Forensics Sec.*, Vol. 7, no. 3, 868–82, Mar. 2012.

23. V. Holub, and J. Fridrich, “Low-complexity features for JPEG steganalysis using undecimated DCT,” *IEEE Trans. Inf. Forensics Sec.*, Vol. 10, no. 2, pp. 219–28, Feb. 2015.

24. Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, “Selection of rich model steganalysis features based on decision rough set-positive region reduction,” *IEEE Trans. Circuits Syst. Video Technol.*, published online, Jun. 2018. doi:10.1109/TCSVT.2018.2799243.

25. Y. Zhang, X. Luo, C. Yang, and F. Liu, “Joint JPEG compression and detection resistant performance enhancement for adaptive steganography using feature regions selection,” *Multimedia Tools Appl.*, Vol. 76, no. 3, pp. 1–20, Mar. 2017.

26. J. Fridrich and T. Filler, “Practical methods for minimizing embedding impact in steganography,” in *Proc. IS&T/SPIE Electronic Imaging*, Photonics West, Vol. 6505, pp. 02–01–02–15, 2007.

27. I. S. Reed, and G. Solomon, “Polynomial codes over certain finite fields,” *J. Soc. Ind. Appl. Math.*, Vol. 8, no. 2, pp. 300–4, Feb. 1960.

28. T. Pevny and J. Fridrich, “Merging Markov and DCT features for multi-class JPEG steganalysis,” in *Proceedings of SPIE – The International Society for Optical Engineering*, Vol. 6505, pp. 650503–650503–13, 2007.

29. D. Y. Chen, M. Ohyoung, and J. L. Wu, “A shift-resistant public watermark system for protecting image processing software,” *IEEE Trans. Consum. Electron.*, Vol. 46, no. 3, 404–14, Mar. 2000.

30. J. Kodovský, J. Fridrich, and V. Holub, “Ensemble classifiers for steganalysis of digital media,” *IEEE Trans. Inf. Forensics Sec.*, Vol. 7, no. 2, pp. 432–44, Feb. 2012.
Authors

Zhenkun Bao received his BS and MS from the Zhengzhou Information Science and Technology Institute, in 2011 and 2014, respectively. Now, he is a doctoral candidate of Computer Applications of Zhengzhou Information Science and Technology Institute. His current research interests include image steganography and steganalysis technique.

Email: bao252547116@sina.com

Xiangyang Luo received his BS, MS and PhD from Zhengzhou Information Science and Technology Institute, in 2001, 2004, and 2010, respectively. He has been with Zhengzhou Information Science and Technology Institute since July 2004. From 2006 to 2007, he was a visiting scholar of the Department of Computer Science and Technology of Tsinghua University. He is the author or co-author of more than 50 refereed international journal and conference papers. His research interest includes image steganography and steganalysis.

Corresponding author. Email: luoxy_ieu@sina.com.

Yi Zhang received his BS and MS from the Zhengzhou Information Science and Technology Institute, in 2014 and 2017, respectively. Now, she is a doctoral candidate of Computer Applications of Zhengzhou Information Science and Technology Institute. Her current research interests include image steganography and steganalysis technique.

Email: 919119543@qq.com

Chunfang Yang received his BS and MS from the Zhengzhou Information Science and Technology Institute, in 2005 and 2008, respectively. Now, he is a doctoral candidate of Computer Applications of Zhengzhou Information Science and Technology Institute. His current research interests include image steganography and steganalysis technique.

Email: chunfangyang@126.com

Fenlin Liu received his BS from Zhengzhou Information Science and Technology Institute in 1986, MS from Harbin Institute of Technology in 1992, and PhD from the Northeast University in 1998. Now, he is a professor of Zhengzhou Information Science and Technology Institute. He is the author or co-author of more than 90 refereed international journal and conference papers. His research interests include information hiding and security theory.

Email: liufenlin@vip.sina.com