Copyright © 2019 Tech Science Press CMC, vol.59, no.1, pp.199-214, 2019

Anti-JPEG Compression Steganography Based on the High Tense Region Locating Method

Yang Wu[1], Weiping Shang[2, *] and Jiahao Chen[3]

Abstract: Robust data hiding techniques attempt to construct covert communication in a lossy public channel. Nowadays, the existing robust JPEG steganographic algorithms cannot overcome the side-information missing situation. Thus, this paper proposes a new robust JPEG steganographic algorithm based on the high tense region location method which needs no side-information of lossy channel. First, a tense region locating method is proposed based on the Harris-Laplacian feature point. Then, robust cover object generating processes are described. Last, the advanced embedding cost function is proposed. A series of experiments are conducted on various JPEG image sets and the results show that the proposed steganographic algorithm can resist JPEG compression efficiently with acceptable performance against steganalysis statistical detection libraries GFR (Gabor Filters Rich model) and DCTR (Discrete Cosine Transform Residual).

Keywords: Robust data hiding, steganography, JPEG compression resistant, Harris-Laplacian feature.

1 Introduction

Steganography is now a fairly standard concept in computer science [Ker, Bas, Böhme et al. (2013)]. It focuses on establishing a stable and effective covert channel by using the public channel [Fridrich (2009)]. Thus, the secret information can be transmitted through public carrier with a supervising monitor by steganographic (stego) technology (especially in an enemy-controlled environment). At present, social and blog-like networks are gradually entering the daily life of human beings, and the images (most images are JPEG format in social networks) transmitted therein are of mass amount and spread widely. Thus, it is easy to cover up the stego images and the identities of covert communication users when the covert channel is established on such networks. However, such networks tend to use lossy compression algorithms to save computing power and network bandwidth in the transmitting process [Zhang, Luo, Yang et al. (2016)]. How to reduce the influence of such lossy operations on the embedded information is an essential problem of applying steganography in social networks.

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, 450002, China.

[2] School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China.

[3] Zhuhai Campus of Beijing Normal University, Zhuhai, 519000, China.

[*] Corresponding Author: Weiping Shang. Email: 18538567977@163.com.

CMC. doi:10.32604/cmc.2019.05194 www.techscience.com/cmc

On this problem, Zhang et al. [Zhang, Luo, Yang et al. (2016)] first proposed the a steganography algorithm DCRAS (Discrete Cosine Relationship Adaptive Steangography) which is based on the relative relationship between DCT coefficients of adjacent 8×8 blocks in the same in-block position of JPEG images; Then, FRAS (Feature Region based Adaptive Steganography) algorithm [Zhang, Luo, Yang et al. (2017)] is proposed based on the invariant-feature-point region where the modified elements are concentrated in the hard-to-detect area to reach higher resisting performance against steganographic statistical detections [Pevný and Fridrich (2007); Kodovský, Pevný and Fridrich (2010); Holub and Fridrich (2015); Denemark, Boroumand and Fridrich (2016); Ma, Luo, Li et al. (2018)]. In the JPEG compression channel, DCRAS and FRAS algorithms can extract the embedded information correctly with much higher probability than the traditional adaptive JPEG steganographic algorithms, such as NPQ (New Perturbed Quantization) [Huang, Luo, Huang et al. (2012)], UED (Uniform Embedding Distortion) [Guo, Ni and Shi (2012)], J-UNIWARD (JPEG image UNIversal WAvelet Relative Distortion) [Holub, Fridrich and Denemark (2014)] and so on. It is worth noting that, as stated in the literature [Zhang, Luo, Yang et al. (2016); Zhang, Luo, Yang et al. (2017)], a necessary condition of the DCRAS and FRAS algorithms is that the sender needs to know the quality factor value of JPEG compression used in the lossy channel (named as side information). Furthermore, the generated stego image can only resist the JPEG compression whose quality factor value is same to the side information. When the side information is missing, the DCRAS and FRAS algorithms can hardly work properly in many compression situations [Zhang, Qin, Zhang et al. (2018); Bao, Luo, Zhang et al. (2018)].

To improve the resistance against JPEG compression of steganography without the side information, an anti-JPEG compression steganography algorithm is designed in this manuscript. First, the region with strong anti-JPEG compression is proposed based on Harris-Laplacian transform. Second, the anti-JPEG cover generation method for borderless information and the corresponding embedding distortion function are given. Last, the concatenated error correction code is combined to elevate the extraction accuracy. The effectiveness of the proposed algorithm is verified by a series of comparative experiments on the standard steganalysis image library BOSSbase 1.01 against existing JPEG adaptive steganography, robust watermarking, DCRAS algorithm and FRAS algorithm for anti-JPEG compression and anti-statistical detection. The results imply that the proposed method can effectively resist JPEG compression under the condition of missing quality factor information with acceptable resistance performance to statistical detection.

The paper has a simple structure. The knowledge of adaptive JPEG steganography and matrix embedding coding are introduced in Section 2 first. Then, Section 3 describes the details of proposed method. Last, the experimental results and conclusions are presented in Section 4 and Section 5 respectively.

2 Related works

In this section, the adaptive JPEG steganography and matrix embedding coding methods are briefly introduced in the following subsections.

2.1 Adaptive JPEG steganography

JPEG format is popular in the social networks for the high image quality and compression performance. Usually, most JPEG steganographic algorithms such as NPQ, UED and J-UNIWARD embed the secret message into the cover JPEG image by modifying the DCT (Discrete Cosine Transform) coefficients of it.

In general, the original spatial image needs to perform color space conversion (from RGB domain to YUV domain) and down-sampling operation first. Then the three independent YUV sub-images are divided into continuous non-overlapping 8×8 blocks respectively, and then independently perform discrete cosine transformation operation. The ready to stored DCT coefficients are gained after quantization and rounding processes. Because the inter-relationship between elements of U sub-image and V sub-image is sensitive, it is suggested to apply embedding process on Y sub-image to increase the security. Meanwhile, the Y sub-image store the luminance information, and researchers try to brief the JPEG image. Thus, the experiments of existing researches on JPEG steganography are focused on grayscale images which can ignore the effects of color space conversion and down-sampling processes. The experiments of this manuscript will also follow this setting and focus on grayscale images.

At present, most popular JPEG adaptive steganographic algorithms consist of embedding cost function and steganographic embedding encoder. This framework is based on the minimum distortion model introduced by Fridrich et al. [Fridrich and Filler (2007)]. This architecture can concentrate the modifications caused by embedding on the DCT coefficients of smaller “cost value” in the embedding cost function. The anti-statistical detection capability of the algorithm is increased if the embedding cost function is well defined. Therefore, the anti-statistical detection capability of the JPEG steganographic algorithm under the framework is closely related to the embedding cost function. On this research, Holub et al. [Holub, Fridrich and Denemark (2014)] proposed the JPEG adaptive steganography algorithm J-UNIWARD, which is defined by The embedded distortion function is composed of decomposition coefficients of a plurality of two-dimensional wavelets (two of which are perpendicular to each other), which can finely describe the smoothness of pixels in multiple directions, so that the embedded modification can be more concentrated to be difficult to detect. On the element, the embedded distortion function can be defined as:

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

The symbols $\mathbf{X}$ and $\mathbf{Y}$ represent cover object and stego object respectively, the symbol $J^{-1}(\square)$ represents the inverse DCT from the frequency domain to the spatial domain, and the symbol $W_{uv}^{(r)}$ represents the *uv*-th decomposition coefficient of the *r*-th (*r*=1, 2, 3) wavelet (*u* and *v* represent the position of the two sub-wavelet respectively), $\varepsilon > 0$ is a constant value which is used to prevent the divisor from appearing 0, it is usually set to a small value, such as $\varepsilon = 10^{-5}$.

2.2 Robust steganography

Zhang et al. [Zhang, Luo, Yang et al. (2016)] proposed a framework for designing robust steganography algorithm. This framework combines the traditional JPEG adaptive steganography algorithm with a famous robust watermarking algorithm, and tries to reach the goal of resisting the statistical detection and JPEG compression.

Under this framework, on the sender:

1 Determining the domain in which the robust steganographic embedding modification is performed.

2 Determining the specific modification measurement on the domain in Step 1 to make the embedded information can effectively resist the lossy JPEG compression operation.

3 Defining the embedding cost function according to the embedded modification measurement to reduce the influence on statistical aspect.

4 Encoding the embedded secret information by using the error correction code to improve the robustness.

5 Embedding secret information by STCs embedding algorithm and packaging the stego object to JPEG format.

For the receiver, after receiving the JPEG image transmitted over the lossy channel:

1 Reading the JPEG format image and the corresponding stego object in the domain.

2 Extracting the information using the STCs extraction algorithm.

3 Correcting the errors in the extracted information by the error correcting code, and finally obtaining the original embedded information.

Under the framework above, the DCRAS and FRAS algorithms are proposed [Zhang, Luo, Yang et al. (2016); Zhang, Luo, Yang et al. (2017)], they can protect the embedded information against JPEG compression and statistical detection well. Nevertheless, the QF (quality factor) of JPEG compression used by the lossy channel should be known in advance (regard as side information) nor leading to significant decline in resisting JPEG compression, and the generated stego object can only resist the specific JPEG compression whose QF value is same to the pre-known QF.

2.3 Harris-Laplacian feature

At present, in the research of robust watermarking algorithms, the information embedding method for information protection through local image feature points has become one of its hot spots. The robust watermarking algorithm calculates the invariant feature points of the watermark carrier image, and then uses the feature point as a center point to generate a watermark embedded region and hides the information. The literature [Lu, Lu and Chung (2010)] uses filtering residuals to calculate and locate the feature points of the carrier image, and gives a normalization method for the regions delimited by the feature points, which can better guarantee the robustness of the embedded information. Using the idea of invariant feature points, a robust watermarking algorithm based on image Harris-Laplacian feature points are proposed in Tsai et al. [Tsai, Huang and Kuo (2011)]. It performs Harris-Laplacian transformation of the image and calculates its corresponding feature points, and selects feature regions to resist specific ones. Lossy operation improves the ability of the watermark information to resist multiple types of lossy attacks. At the same time, the literature [Tsai, Huang, Kuo et al. (2012)] demonstrates the effectiveness of such Harris-Laplacian transform image features in robust watermarking, and proposes a more robust and secure one based on the literature [Lu, Lu and Chung (2010)].

3 Proposed method

On the problem of eliminating QF side information in robust steganography and resisting JPEG compression with multiple QF values, a new anti-JPEG steganography based on a region location method is proposed in this section. Frist, the proposed region location method is proposed. Then, the improved cover generation method is described. Last, the proposed embedding cost function and the error correction method setting is briefly introduced.

Notice that the proposed anti-JPEG steganography is under the framework in Section 2.2, and the diagram is shown in Fig. 1.

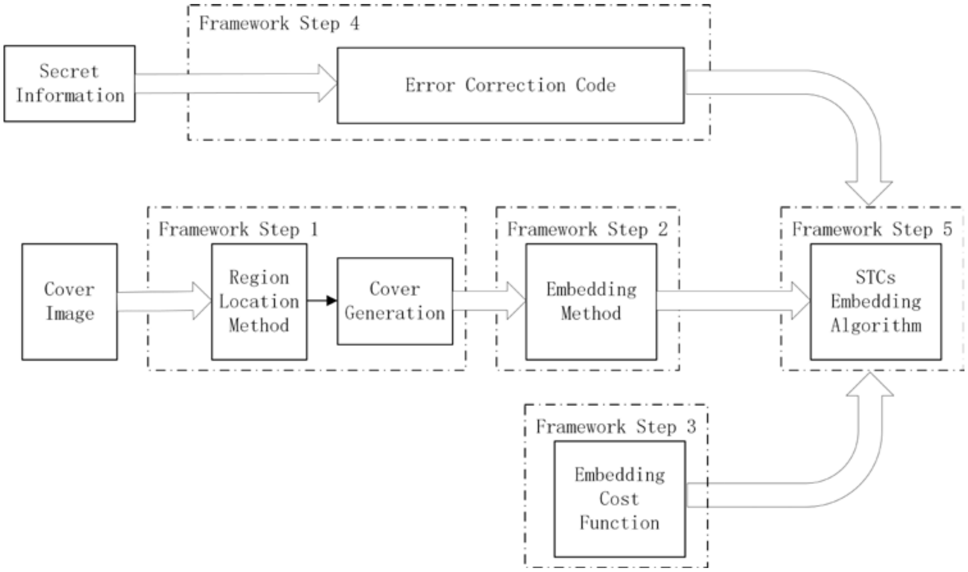


Figure 1: Diagram of the proposed algorithm

3.1 High tense region locating method based on Harris-Laplacian feature point

A natural thought is that the complex-area of image will lose more information than the plain-area after processing JPEG compression. It is reasonable because the discrete cosine transform will concentrate the “energy” of image to the low frequency area, and the quantization and rounding processes cut the details of image to reach the goal of compression.

However, in literature Lu et al. [Lu, Lu and Chung (2010)], a new idea is pointed that the edges of object in image owns strong robustness because they contains much more information about the corresponding object. Furthermore, the pixels of object edges in image are more suitable to be modified than the plain area pixels in most adaptive steganographic algorithms. Thus, this sub-section proposes a high tense region locating method based on the Harris-Laplacian feature point that can be rebuilt the embedding region after the stego image is compressed and the modified elements are concentrated in the complex-area.4

The processes of the method are presented as follows:

Step 1. Functions that convert image I into scale space L are defined as:

$$\begin{aligned} &L\left(\mathbf{a},\sigma_D\right)=G\left(\mathbf{a},\sigma_D\right)*I\left(\mathbf{a}\right),\\ &G\left(\mathbf{a},\sigma_D\right)=\frac{1}{2\pi\sigma_D^2}e^{-(i^2+j^2)/2\sigma_D}, \end{aligned} \tag{2}$$

where symbol $\mathbf{a}=(i,j)$ denotes the spatial coordinates of a certain pixel of the image, function G denotes a standard Gaussian kernel function, σ_D denotes a scale parameter of the kernel function, and “$*$” denotes a convolution calculation operation.

Step 2. In order to characterize the local structure of the image in the scale space, the autocorrelation matrix is defined in the scale space obtained in Step 1:

$$\mu(\mathbf{a},\sigma_I,\sigma_D)=\sigma_D^2G(\mathbf{a},\sigma_I)*\begin{bmatrix} L_x^2(\mathbf{a},\sigma_D) & L_xL_y(\mathbf{a},\sigma_D)\\ L_xL_y(\mathbf{a},\sigma_D) & L_x^2(\mathbf{a},\sigma_D)\end{bmatrix} \tag{3}$$

where σ_I is the integral scale and L_x and L_y represent the first-order derivative function of the *x*-axis and *y*-axis directions, respectively, in the scale space.

Step 3. An angle response function $c(\mathbf{a},\sigma_I,\sigma_D)$ is designed based on $\mu(\mathbf{a},\sigma_I,\sigma_D)$ to quantify the local curvature amplitude of the image (i,j) position pixel:

$$c\left(\mathbf{a},\sigma_I,\sigma_D\right)=\det\left(\mu(\mathbf{a},\sigma_I,\sigma_D)\right)-0.04tr\left(\mu(\mathbf{a},\sigma_I,\sigma_D)\right) \tag{4}$$

where “det” represents matrix determinant, and symbol *tr* represents the trace of the matrix. The larger the value of the angle response function is, the greater the probability that the corresponding image pixel can be repositioned after being subjected to a lossy attack.

Step 4. Laplacian-of-Gaussian operation $LoG(\mathbf{a},\sigma_n)$ and combining the angle response function $c(\mathbf{a},\sigma_I,\sigma_D)$ are used to find the robust edge pixels of the object in multiple dimensions in the image. Selecting the pixels with the largest 1% value of the angle response function $c(\mathbf{a},\sigma_I,\sigma_D)$ in the image to be candidate points first. Then, the extreme point of the absolute value of the Gaussian-Laplacian $LoG(\mathbf{a},\sigma_n)$ on $\sigma_n\in\{(1.1)^i\times1.5\,|\,i=1,2,...,n\}$ is selected. The measure of determining the extreme points is: suppose $\sigma_D=0.7$, *n*=15 when f satisfies:

$$\begin{aligned}&\left|LoG(\mathbf{a},(1.1)^{i}\times 1.5)\right|>\left|LoG(\mathbf{a},(1.1)^{i-1}\times 1.5)\right|\\&\left|LoG(\mathbf{a},(1.1)^{i}\times 1.5)\right|>\left|LoG(\mathbf{a},(1.1)^{i+1}\times 1.5)\right|\\&\left|LoG(\mathbf{a},(1.1)^{i}\times 1.5)\right|>10.\end{aligned}\tag{5}$$

The pixels selected by the above algorithm is named as "feature pixel with scale value $\sigma_c=(1.1)^i\times 1.5$", and form a sequence set $\mathbf{C}=\{\mathbf{a}_1,\mathbf{a}_2,...,\mathbf{a}_k\}$ in order from left to right in the image from top to bottom.

Step 5. The radius value *r* of several same-radius circles whose centers are the elements of $\mathbf{C}=\{\mathbf{a}_1,\mathbf{a}_2,...,\mathbf{a}_k\}$ are determined, and the embedding area are within the circles. The method of determining *r* iteratively is given by setting the initial value of *r* to 1 (the unit is the minimal distance between two pixels), and the *t*-th iteration steps are:

(1) Counting the number n_t of pixels within the circles whose centers are located by the feature pixels of the set $\mathbf{C}$ and the radius is the *r* of this literation.

(2) If the length *m* of information to be embedded satisfies $m\geq n_t/3$, then *r*=*r*+1 and enters the *t*+1 iteration.

(3) If the length *m* of information to be embedded satisfies $m<n_t/3$, stop iterating and output the current value of *r*.

This ensures that there are enough embedded points in the selected area.

3.2 Generating cover object and modifying method

To against the JPEG compression operation, a cover generating (Step 1 and Step 2) and the corresponding modifying method (Step 3 to Step 5) without side information is described as follows:

Step 1. A set of non-overlapping 8×8 DCT coefficient-blocks is obtained from the JPEG cover image. Symbol $\mathbf{D}_k=\{\mathrm{D_k(i),i=1,2,...,64}\}$, $k=1,2,...,m$ is used to denote the set where *m* is the number of DCT blocks, and scalars *i* and *k* denote the *i*-th coefficient in the *k*-th block (in order from left to right, up to bottom).

Step 2. A *n*-element robust cover object $\mathbf{X}=\{\mathrm{x_1,x_2,...,x_n}\}$ is generated by:

$$x_j=\begin{cases}0, if\ D_k(i)\leq M_{ki}\\1, if\ D_k(i)>M_{ki}\end{cases},1\leq j\leq n,\tag{6}$$

where M_{ki} is the rounded mean value of three neighbor-blocked DCT coefficients $D_{k_1}(i),D_{k_2}(i),D_{k_3}(i)$.

Step 3. The robust virtual stego object $\mathbf{Y}$ obtained by modifying element values of cover object $\mathbf{X}$, and the mapping rule of applying the modifications to $\{\mathbf{D}_k\}_{1\leq k\leq B}$ is expressed by:

$$D_k^y(i)=\begin{cases} M_{ki}+\sigma_{ki}, if\ \ y_j=1\ \&\ D_k(i)<M_{ki}+\sigma_{ki} \\ M_{ki}-\sigma_{ki}, if\ \ y_j=0\ \&\ D_k(i)>M_{ki}\text{ - }\sigma_{ki} \\ D_k(i), else \end{cases}. \tag{7}$$

Step 4. The stego object after suffering JPEG compression operation is denoted by symbol $\tilde{\mathbf{Y}}$ whose element $\tilde{y}_j,(1\le j\le n)$ is:

$$\tilde{y}_j=\begin{cases} 0, \tilde{D}_k(i)\le\tilde{M}_{ki} \\ 1, \tilde{D}_k(i)>\tilde{M}_{ki} \end{cases}. \tag{8}$$

where the symbols $\tilde{\mathbf{D}}$, $\tilde{\mathbf{D}}_k=\{\tilde{\text{D}}_\text{k}(\text{i}),\text{i}=1,2,...,64\}$ and $\{\tilde{M}_{ki}\}_{k,i}$ respectively denote the sets of DCT coefficients, 8×8 blocks and neighboring mean values after JPEG compression.

Step 5. The value of σ_{ki} is obtained on:

$$\sigma_{ki}=\begin{cases} 1, if\ \ D_k^{\max}(i)\text{ - }D_k^{\min}(i)\le T \\ 2, if\ \ T_1\le D_k^{\max}(i)\text{ - }D_k^{\min}(i)\le T_2 \\ 3, if\ \ D_k^{\max}(i)\text{ - }D_k^{\min}(i)>T_2 \end{cases}. \tag{9}$$

In formula (9), symbols $D_k^{\max}(i)$ and $D_k^{\min}(i)$ are respectively the maximum value and minimum value among the four coefficients $D_k(i), D_{k_1}(i), D_{k_2}(i), D_{k_3}(i)$, and (T_1,T_2) ($T_1<T_2$) are the threshold values, and a suggested setting is $(15,30)$.

3.3 Design of embedding cost function and error correction method setting

After the cover object is generated by Section 3.2, the embedding process and error correction method are applied to concentrate the modifications on the hard-to-detect area and increase the robustness.

According to the typical steganographic scheme, the design of embedding cost function effects the detection resisting performance a lot because the embedding encoder STCs nearly reach the bound. The construction of embedding cost function used in Bao et al. [Bao, Luo, Zhang et al. (2018)] achieves good performance and it is expressed as:

$$DF(x_j,y_j)=\begin{cases} 0, \qquad x_j=y_j \\ \rho_{ki}^{(1)}, \{x_j=0\ \&\ M_{ki}+\sigma_{ki}-D_k(i)=1\} \\ \qquad or\ \{x_j=1\ \&\ D_k(i)-M_{ki}+\sigma_{ki}=1\} \\ \rho_{ki}^{(2)}, \{x_j=0\ \&\ M_{ki}+\sigma_{ki}-D_k(i)=2\} \\ \qquad or\ \{x_j=1\ \&\ D_k(i)-M_{ki}+\sigma_{ki}=2\} \\ wet\_cost, \quad else \end{cases}. \tag{10}$$

The symbols $\rho_{ki}^{(1)}$ and $\rho_{ki}^{(2)}$ in formula (10) denote the function-values of amplitude “1” and “2” by formula (1). However, the function in formula (10) cannot describe some situations well:

Even though $x_j = y_j$, the function value calculated by formula (10) is not "0" when $x_j = y_j = 1\,\&\, D_k(i) < M_{ki} + \sigma_{ki}$ and $x_j = y_j = 0\,\&\, D_k(i) > M_{ki} - \sigma_{ki}$.

Because the STCs embedding encoder tries to concentrate the modifications on low-function-value elements, thus the element in the situations above cannot be fully used. Thus, a new embedding cost function $DF_{pro}(x_j, y_j)$ is proposed as follows:

$$DF_{pro}(x_j, y_j) = \begin{cases} 0, & x_j = y_j \\ \rho_{ki}^{(1)}, & \{x_j = y_j = 0\,\&\, D_k(i) > M_{ki} - \sigma_{ki}\,\&\, D_k(i) - M_{ki} + \sigma_{ki} = 1\} \\ & or\ \{x_j = y_j = 1\,\&\, D_k(i) < M_{ki} + \sigma_{ki}\,\&\, M_{ki} + \sigma_{ki} - D_k(i) = 1\} \\ \rho_{ki}^{(2)}, & \{x_j = y_j = 0\,\&\, D_k(i) > M_{ki} - \sigma_{ki}\,\&\, D_k(i) - M_{ki} + \sigma_{ki} = 2\} \\ & or\ \{x_j = y_j = 1\,\&\, D_k(i) < M_{ki} + \sigma_{ki}\,\&\, M_{ki} + \sigma_{ki} - D_k(i) = 2\} \\ \rho_{ki}^{(1)}, & \{x_j = 0\,\&\, M_{ki} + \sigma_{ki} - D_k(i) = 1\} \\ & or\ \{x_j = 1\,\&\, D_k(i) - M_{ki} + \sigma_{ki} = 1\} \\ \rho_{ki}^{(2)}, & \{x_j = 0\,\&\, M_{ki} + \sigma_{ki} - D_k(i) = 2\} \\ & or\ \{x_j = 1\,\&\, D_k(i) - M_{ki} + \sigma_{ki} = 2\} \\ wet\_\cos t, & else \end{cases}, \quad (11)$$

$$1 < j < n,\ j \in Z.$$

Then, error correction encoder RS (Reed and Solomon) is applied on secret information before using STCs algorithm. RS is set to parameter (40, 90) which means 40 input elements encoded to 90 output elements, and error diffusion method proposed in Bao et al. [Bao, Luo, Zhang et al. (2018)] are also used in this process to increase the robustness of cover object to against JPEG compression.

4 Experiments

In order to verify the effectiveness of the proposed method, experiments were conducted based on BOSSbase image library. First, the experimental setups and the used image database are introduced. Then, the anti-JPEG compression performance and anti-statistical detection performance of the proposed method are compared with the JPEG adaptive steganography algorithm J-UNIWARD [Holub, Fridrich and Denemark (2014)], robust watermarking algorithm [Chen, Ouhyoung and Wu (2000)], robust steganography algorithm DCRAS [Zhang, Luo, Yang et al. (2016)] and FRAS [Zhang, Luo, Yang et al. (2017)].

4.1 Setups

All the experiments presented in this section were performed on a personal computer equipped with Intel Core i7-8700 CPU (3.2 GHz) and Windows 10 system. The software used in the experiment is MATLAB R2017a, and the spatial image library used is BOSSbase 1.01 (proposed by Patrick Bas, Tomas Filler, Tomas Pevny on ICASSP 2013, the download address is: http://agents.fel.cvut.cz/stegodata/).

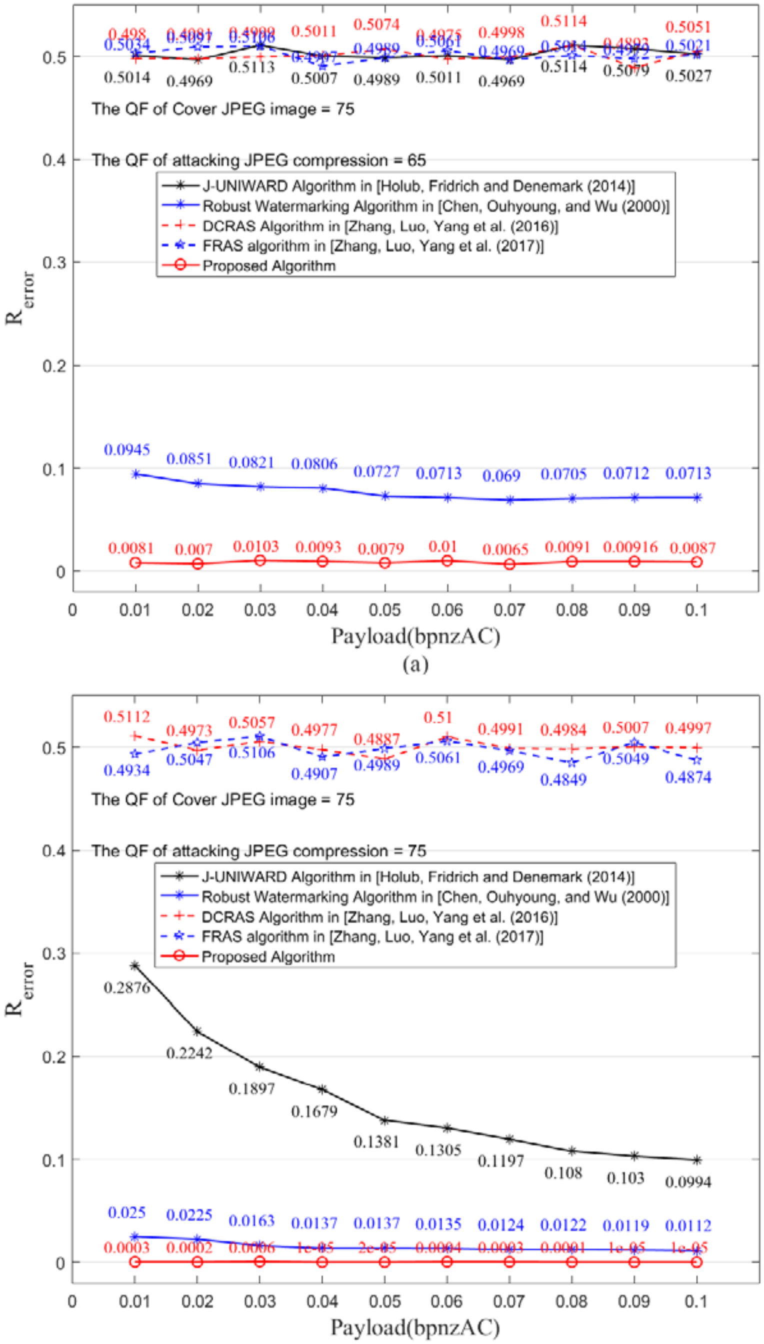
In the experiment of anti-JPEG compression, the embedded information in the stego image is extracted after lossy compression of JPEG. The error rate of information extraction is used to measure the resistance of robust steganographic algorithm to JPEG compression. It is defined as the rate of error bits number in extracting information to the total bits number of embedded information.

In the anti-detection performance experiment, two famous JPEG image statistical detection feature libraries GFR (Gabor Filters Rich model [Song, Liu, Yang et al. (2015)]) and DCTR (Discrete Cosine Transform Residual [Holub and Fridrich (2015)]) are used with ensemble classifier [Kodovský, Fridrich and Holub (2012)]. Last, the test error of the ensemble classifier is used to measure the anti-detection performance of the steganography algorithm. The closer value to 50% means the stronger anti-detection performance.

4.2 Anti-JPEG compression experiments

In this section, the 10,000 JPEG images compressed with QF=75 is generated from BOSSbase 1.01 image database. The steganographic information is embedded by J-UNIWARD [Holub, Fridrich and Denemark (2014)], robust watermarking algorithm [Chen, Ouhyoung and Wu (2000)], robust steganography algorithm DCRAS [Zhang, Luo, Yang et al. (2016)], FRAS [Zhang, Luo, Yang et al. (2017)] and the proposed method in this manuscript. The embedding rate is varied from 0.01 bpnzAC (bits per non-zero Alternating Current coefficient) to 0.10 bpnzAC with 0.01 interval on the BOSSbase library with the 5 different algorithms mentioned above. Each setting generates 10,000 stego images and they are JPEG compressed by quality factors of 65, 75 and 85. Then, the embedded information is extracted to count the error rate. It is worth noting that in order to simulate the lossy transmission of unbounded information, the side information used by the carrier generated by DCRAS algorithm in the experiment is QF=90. The error extraction rate counting results of JPEG compression attacks with QF=75, 85 and 95 are shown in Fig. 2.

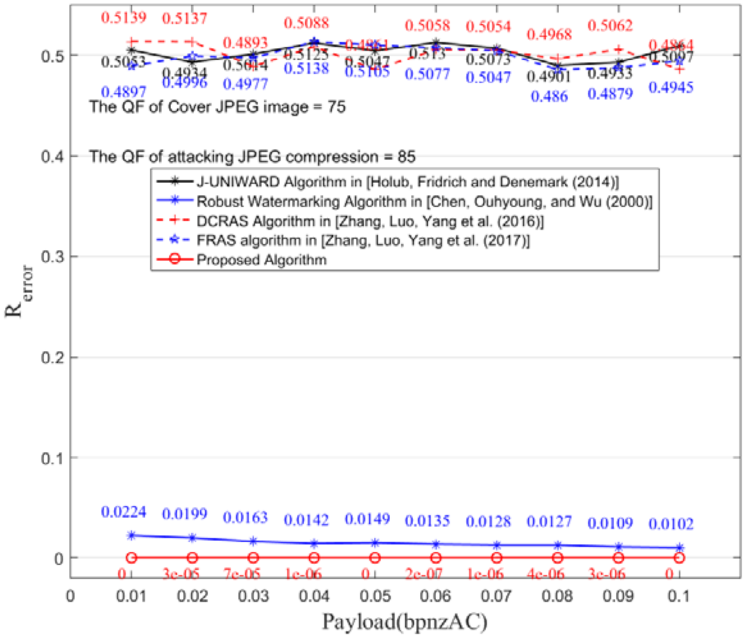
From the Figs. 2(a), 2(b), 2(c), we can see that the error rates of extracted information of J-UNIWARD, DCRAS and FRAS are about 50%. It means that they can hardly resist the damage on embedded information from JPEG compression. The DCRAS and FRAS lost the ability of resisting JPEG compressing when the side-information is missing. The proposed algorithm and the robust watermarking algorithm both have low error rate of information extraction under most JPEG compression conditions. Among different compression settings, the error extraction rates of the proposed algorithm in this manuscript can be reduced by 9.47% at most (JPEG compression attack with QF=65) compared with that of the watermarking algorithm. It is also noted that the error extraction rates decreases with the increase of the quality factor of JPEG compression attacks. In JPEG compression attacks with QF=75 and 85, the proposed algorithm can also guarantee the low error extraction rate. This is because the higher the quality factor of JPEG compression, the less image information lost during compression.


0.498
0.4981
0.4999
0.5011
0.5074
0.4975
0.4998
0.5114
0.4893
0.5051
0.5034
0.5097
0.5106
0.4907
0.4989
0.5061
0.4969
0.5014
0.4972
0.5021
0.5014
0.4969
0.5113
0.5007
0.4989
0.5011
0.4969
0.5114
0.5079
0.5027
The QF of Cover JPEG image = 75
The QF of attacking JPEG compression = 65
J-UNIWARD Algorithm in [Holub, Fridrich and Denemark (2014)]
Robust Watermarking Algorithm in [Chen, Ouhyoung, and Wu (2000)]
DCRAS Algorithm in [Zhang, Luo, Yang et al. (2016)]
FRAS algorithm in [Zhang, Luo, Yang et al. (2017)]
Proposed Algorithm
0.0945
0.0851
0.0821
0.0806
0.0727
0.0713
0.069
0.0705
0.0712
0.0713
0.0081
0.007
0.0103
0.0093
0.0079
0.01
0.0065
0.0091
0.00916
0.0087
R_{error}
0.5
0.4
0.3
0.2
0.1
0
0
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
0.09
0.1
Payload(bpnzAC)

(a)

0.5112
0.4973
0.5057
0.4977
0.4887
0.51
0.4991
0.4984
0.5007
0.4997
0.4934
0.5047
0.5106
0.4907
0.4989
0.5061
0.4969
0.4849
0.5049
0.4874
The QF of Cover JPEG image = 75
The QF of attacking JPEG compression = 75
J-UNIWARD Algorithm in [Holub, Fridrich and Denemark (2014)]
Robust Watermarking Algorithm in [Chen, Ouhyoung, and Wu (2000)]
DCRAS Algorithm in [Zhang, Luo, Yang et al. (2016)]
FRAS algorithm in [Zhang, Luo, Yang et al. (2017)]
Proposed Algorithm
0.2876
0.2242
0.1897
0.1679
0.1381
0.1305
0.1197
0.108
0.103
0.0994
0.025
0.0225
0.0163
0.0137
0.0137
0.0135
0.0124
0.0122
0.0119
0.0112
0.0003
0.0002
0.0006
1e-05
2e-05
0.0004
0.0003
0.0001
1e-05
1e-05
R_{error}
0.5
0.4
0.3
0.2
0.1
0
0
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
0.09
0.1
Payload(bpnzAC)

(b)



(c)

Figure 2: Experimental results of anti-JPEG compression attack on different steganographic and robust watermarking algorithms: (a), (b) and (c) present the results under JPEG compression attack of quality factor=65, 75 and 85 respectively

4.3 Statistical detection experiments

In this section, a set of carrier images with a quality factor of 75 and 85 is generated from all 10,000 spatial images in the BOSSbase 1.01 image database, and then random secret information is embedded using robust watermarking algorithm [Chen, Ouhyoung and Wu (2000)], DCRAS [Zhang, Luo, Yang et al. (2016)], FRAS [Zhang, Luo, Yang et al. (2017)] algorihtmsand and the proposed algorithm. The embedding rate is varied from 0.01 bpnzAC to 0.10 bpnzAC with 0.01 interval, and 10,000 stego images are generated of each different embedding algorithms with different embedding rates. Then, we use two statistical detection features of GFR (contains 17,000 features) and DCTR (contains 8,000 features) to extract the features of the carrier and the carrier image. Then we use the extracted features from 5,000 random chosen cover-stego pairs to train the ensemble linear classifier, and then the trained classifier is applied on the remained 10,000 images (5,000 cover images and 5,000) in the image database. Distribution) is used to classify the ensemble classifier. The test error rates of classifier with GFR and DCTR features are shown in Tab. 1 and Tab. 2 respectively.

Table 1: Experimental results of statistical detection under GFR feature library against different steganographic and robust watermarking algorithms (The QF of cover JPEG image=75 and 85, and the bolt numbers denotes the results under QF=85)

Methods	Embedding Rate (bpdzAC)									
	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
Robust Watermarking Algorithm [Chen, Ouhyoung and Wu (2000)]	0.0013 **0.0018**	0.0009 **0.0016**	0.0005 **0.0014**	0.0004 **0.0009**	0.0001 **0.0001**	0.0016 **0.0016**	0.0013 **0.0014**	0.0011 **0.0013**	0.0010 **0.0001**	0.0010 **0.001**
DCRAS [Zhang, Luo, Yang et al. (2016)]	0.3802 **0.4089**	0.3185 **0.3331**	0.2304 **0.2456**	0.1637 **0.1703**	0.1399 **0.1477**	0.1070 **0.1048**	0.0673 **0.0702**	0.0393 **0.0411**	0.0342 **0.0373**	0.0294 **0.0300**
FRAS [Zhang, Luo, Yang et al. (2017)]	0.4002 **0.4228**	0.3207 **0.3343**	0.250 **0.2621**	0.1703 **0.1755**	0.1499 **0.1533**	0.1150 **0.1227**	0.0827 **0.0886**	0.0509 **0.0574**	0.0465 **0.0518**	0.0392 **0.0417**
Proposed Algorithm	0.3915 **0.4128**	0.3126 **0.3104**	0.2320 **0.2477**	0.1651 **0.1695**	0.1445 **0.1481**	0.0793 **0.0863**	0.0529 **0.0603**	0.0313 **0.0376**	0.0224 **0.0208**	0.0115 **0.0109**

Table 2: Experimental results of statistical detection under DCTR feature library against different steganographic and robust watermarking algorithms (The QF of cover JPEG image=75 and 85, and the bolt numbers denotes the results under QF=85)

Methods	Embedding Rate (bpdzAC)				
	0.01	0.02	0.03	0.04	0.05
Robust Watermarking Algorithm [Chen, Ouhyoung and Wu (2000)]	0.0103 **0.0118**	0.0031 **0.0046**	0.0025 **0.0034**	0.0022 **0.0029**	0.0017 **0.0021**
DCRAS [Zhang, Luo, Yang et al. (2016)]	0.4102 **0.4289**	0.3285 **0.3431**	0.2604 **0.2756**	0.2037 **0.2143**	0.1699 **0.1777**

FRAS [Zhang, Luo, Yang et al. (2017)]	0.4189	0.3355	0.2738	0.2096	0.1749
	0.4328	**0.3543**	**0.2821**	**0.2245**	**0.1803**
Proposed Algorithm	0.3914	0.2926	0.2020	0.1619	0.1645
	0.4108	**0.3104**	**0.2177**	**0.1765**	**0.1539**
Methods	Embedding Rate (bpdzAC)				
	0.06	0.07	0.08	0.09	0.1
Robust Watermarking Algorithm [Chen, Ouhyoung and Wu (2000)]	0.0016	0.0013	0.0011	0.001	0.001
	0.0016	**0.0014**	**0.0013**	**0.0001**	**0.001**
DCRAS [Zhang, Luo, Yang et al. (2016)]	0.1370	0.1127	0.0909	0.0694	0.0517
	0.1448	**0.1202**	**0.1001**	**0.0721**	**0.0529**
FRAS [Zhang, Luo, Yang et al. (2017)]	0.1413	0.1175	0.0992	0.0741	0.0574
	0.1487	**0.1259**	**0.1051**	**0.0793**	**0.0627**
Proposed Algorithm	0.1101	0.0829	0.0613	0.0424	0.0115
	0.1143	**0.0903**	**0.0676**	**0.0471**	**0.0109**

From the results of Tab. 1 and Tab. 2, it can be seen that the detection error rate of robust watermarking algorithm is very low. It is due to the primal design of watermarking is to make the embedded message can be detected even after suffering JPEG compression operation. Therefore, the stego image generated by the robust watermarking algorithm can be easily detected by statistical detection method. Compared with the side informed robust steganography algorithms DCRAS and FRAS, the proposed robust steganography algorithm loss little detection resistance at low embedding rate, while a sharp decline in detection resistance occurs at embedding rate higher than 0.05 bpnzAC. This phenomenon may be caused by the embedding regions selected by proposed method in 3.1 are nearly to the full image. It means that the region select strategy becomes useless in this case. Thus, to ensure security, the proposed robust steganography is suggested to work at a low embedding rate which owns strong anti-statistical detection ability.

5 Conclusions

In order to design robust steganography against JPEG compression without side information, this manuscript proposed a robust watermarking algorithm based on the high tense region method. The region locating method combines the LoG operator and robust steganography and cover generating method without side information is described. New embedding cost function is proposed on overcoming the defects of the existing function. Comparative experimental results show that the proposed algorithm can reach a high compression resistance on sacrifice a small part of the anti-statistical detection ability. How to overcome the resistance decline problem in high embedding rates and more kinds of lossy operation are our further researching interests.

Acknowledgement: This work was supported by the National Key Research and Development Program (2016YFB0801601) and the Pilot Technology Transfer Innovation Reform of Xidian University (No. 90904180001).

References

Bao, Z.; Luo, X.; Zhang, Y.; Yang, C.; Liu, F. (2018): A robust image steganography on resisting JPEG compression with no side information. *IETE Technical Review*, vol. 2, no. 6, pp. 1-10.

Chen, D. Y.; Ouhyoung, M.; Wu, J. L. (2000): A shift-resisting public watermark system for protecting image processing software. *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 404-414.

Denemark, T. D.; Boroumand, M.; Fridrich, J. (2016): Steganalysis features for content-adaptive JPEG steganography. *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1736-1746.

Filler, T.; Fridrich, J. (2011): Design of adaptive steganographic schemes for digital images. *Proceedings of the IS&T/SPIE Electronic Imaging, Media Water-marking, Security, and Forensics*, vol. 7880, pp. 1-14.

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

Fridrich, J.; Filler, T. (2007): Practical methods for minimizing embedding impact in steganography. *Proceedings of the IS&T/SPIE Electronic Imaging, Photonics West*, vol. 6505, no. 2, pp. 1-15.

Guo, L.; Ni, J.; Shi, Y. (2012): An efficient jpeg steganographic scheme using uniform embedding. *Proceedings of the IEEE International Workshop on Information Forensics and Security*, pp. 169-174.

Holub, V.; Fridrich, J. (2015): Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219-228.

Holub, V.; Fridrich, J.; Denemark, T. (2014): Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1-13.

Huang, F.; Huang, J.; Shi, Y. (2012): New channel selection rule for JPEG steganography. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1181-1191.

Huang, F.; Luo, W.; Huang, J.; Shi, Y. (2013): Distortion function designing for jpeg steganography with uncompressed side-image. *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, pp. 69-76.

Ker, A. D.; Bas, P.; Böhme, R.; Cogranne, R.; Craver, S. et al. (2013): Moving steganography and steganalysis from the laboratory into the real world. *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, pp. 45-58.

Kodovský, J.; Fridrich, J.; Holub, V. (2012): Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Securit*y, vol. 7, no. 2, pp.

432-444.

Kodovský, J.; Pevný, T.; Fridrich, J. (2010): Modern steganalysis can detect YASS. *Proceedings of the IS&T/SPIE Electronic Imaging, Media Forensics and Security*, vol. 7541, no. 2, pp. 1-11.

Lu, W.; Lu, H.; Chung, F. L. (2010): Feature based robust watermarking using image normalization. *Computers & Electrical Engineering*, vol. 36, no. 1, pp. 2-18.

Ma, Y.; Luo, X.; Li, X.; Bao, Z.; Zhang, Y. (2018): Selection of rich model steganalysis features based on decision rough set α-positive region reduction. *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 1, no. 99, pp. 1-23.

Pevný, T.; Fridrich, J. (2007): Merging Markov and DCT features for multi-class JPEG steganalysis. *Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents*, vol. 6505, no. 3, pp. 1-13.

Song, X.; Liu, F.; Yang, C.; Luo, X.; Zhang, Y. (2015): Steganalysis of adaptive jpeg steganography using 2D gabor filters. *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, pp. 15-23.

Tsai, J. S.; Huang, W. B.; Kuo, Y. H. (2011): On the selection of optimal feature region set for robust digital image watermarking. *IEEE Transactions on Image Processing*, vol. 20, no. 3, pp. 735-743.

Tsai, J. S.; Huang, W. B.; Kuo, Y. H.; Horng, M. F. (2012): Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions. *Signal Processing*, vol. 92, no. 6, pp. 1431-1445.

Zhang, Y.; Luo, X.; Yang, C.; Liu, F. (2017): Joint JPEG compression and detection resistant performance enhancement for adaptive steganography using feature regions selection. *Multimedia Tools & Applications*, vol. 76, no. 3, pp. 1-20.

Zhang, Y.; Luo, X.; Yang, C.; Ye, D.; Liu, F. (2016): A framework of adaptive steganography resisting JPEG compression and detection. *Security and Communication Networks*, vol. 9, no. 15, pp. 2957-2971.

Zhang, Y.; Qin, C.; Zhang, W.; Liu, F.; Luo, X. (2018): On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*, vol. 146, pp. 99-111.