TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 06/13 pp614–624
DOI: 10.26599/TST.2019.9010069
Volume 25, Number 5, October 2020

Fast Carrier Selection of JPEG Steganography Appropriate for Application

Weixiang Ren, Yibo Xu, Liming Zhai, Lina Wang*, and Ju Jia

Abstract: In recent years, the improvement of the security of steganography mainly involves not only carrier security but also distortion function. In the actual environment, the existing method of carrier selection is limited by its complex algorithm and slow running speed, making it not appropriate for rapid communication. This study proposes a method for selecting carriers and improving the security of steganography. JPEG images are decompressed to spatial domain. Then correlation coefficients between two adjacent pixels in the horizontal, vertical, counter diagonal, and major diagonal directions are calculated. The mean value of the four correlation coefficients is used to evaluate the security of each JPEG image. The images with low correlation coefficients are considered safe carriers and used for embedding in our scheme. The experimental results indicate that the stego images generated from the selected carriers exhibit a higher anti-steganalysis capability than those generated from the randomly selected carriers. Under the premise of the same security level, the images with low correlation coefficients have a high capacity. Our algorithm has a very fast running speed, and the running time of a 2048×2048 image is less than 1 s.

Key words: steganography; steganalysis; carrier; JPEG; correlation coefficients

1 Introduction

Steganography is the technique of hiding information in regular-looking media for the implementation of secret communications[1,2]. The kinds of regular-looking media are varied, including not only images but also video[3], audio[4], or text files[5]. Image steganalysis[6], the countermeasure technology of image steganography, has to detect the distortion caused by embedding modification and distinguish the stego images from the normal images. With the development of detection techniques, low-dimensional features[7], rich models[8–13], and deep learning[14–16] are proposed to improve detection accuracy. The early steganography schemes aim to restrict the modification location and reduce the modification rate. However, these two advantages cannot be perfectly integrated until the embedding framework based on the Syndrome-Trellis Code (STC)[17] was proposed. Most of the latest steganography schemes[18–22] only design a distortion function to evaluate the risk value of each bit modification rather than study the entire embedding procedure. Obviously, the introduction of STC improves the security of steganography significantly because of its adaptive embedding modification and high coding efficiency. And the improvement of security is mainly established on the basis of the distortion function; however, the improvement declintes with the development of steganography.

Two aspects determine the security of one stego sample, namely, the steganography operation and its masking signal. The former includes the embedding algorithm and payload, and the latter is its original carrier, such as a JPEG image before embedding.

• Weixiang Ren, Liming Zhai, Lina Wang, and Ju Jia are with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan University, Wuhan 430000, China, and also with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430000, China. E-mail: {renweixiang, limingzhai, lnwang, jiaju123}@whu.edu.cn.
• Yibo Xu is with Micropattern Co. Ltd., Wuhan 430000, China. E-mail: xu_yi_bo@163.com.
∗ To whom correspondence should be addressed.

Manuscript received: 2019-10-24; accepted: 2019-11-13

Studies of embedding algorithm involve the former, and existing research on carrier effect, such as cover source mismatch[23–25], carrier selection[26–28], and calibration[29, 30], indicates that the latter has a significant influence on steganalysis. In other words, carrier signal disturbance or carrier selection before embedding helps hide information. Nevertheless, carriers with weak disturbance for steganalysis may lead to high-accuracy detection[26]. This means that the randomly selected carriers cannot provide a guarantee of expected security, even if an algorithm with a high security level and a low payload is utilized to embed secret information. From this point of view, carrier disturbance is absolutely essential for security level of steganography. Moreover, a large number (such as 100) of images, not one image, are probably needed to embed information in actual environment because of the limited capacity of only one carrier. A larger number (maybe 1000) of images need to be evaluated to determine the appropriate number of carriers for the final embedding process. Thus, a fast selection or evaluation algorithm is important in practice. This problem has not yet been well addressed in recent years. Most of the existing studies introduce not only a complex but also a slow computing method for carrier selection to decrease the probability of being detected, which is inappropriate for application. In many cases, a difficult challenge is to make a quantitative and accurate description of carrier disturbance quickly.

In this study, we determine that the security of JPEG image can be evaluated easily through its spatial pixels. A coefficient-correlation-based method of carrier selection is proposed to improve anti-steganalysis capability. Experiments show that the correlation between spatial pixels is related to the noise intensity or detection error of JPEG images. In our proposed scheme, images with strong noise or low pixel correlation coefficient increase the detection error by more than 5% after embedding. The relationship between C value and the nonzero Alternating Current (AC) coefficients indicates that the samples with low correlation coefficients can be embedded with more information and have the same level of security as the other samples. In addition, our method is easy to implement and has a fast running speed. Thus, it can complete the security evaluation of a 2048×2048 JPEG image less than 1 s.

2 Preliminary

2.1 Existing work

To our knowledge, many factors can considerably affect the detection accuracy or security of steganography, such as image size, compression parameters, image content, payload, and embedding algorithm. Under the premise that other variable factors are constant, both the image size and payload are positively related to detection accuracy. Embedding algorithms are widely studied in the past 20 years. By contrast, the image content was not considered. In the past 2 years, researchers have gradually realized the importance of carrier security. In Ref. [28], Wang et al. proposed a batch steganography method, which combines cover selection and payload allocation by steganographic distortion optimization. All of the images that are used for embedding must have the same individual distortion value of θ to minimize the total distortion. Steganography algorithms have to gradually adjust the individual distortion of value θ from a small initial value, such as 0.01. Moreover, for each image, 100 points of the payload-distortion curve must be calculated before embedding, which obviously decelerates the embedding speed. In Ref. [26], Wang et al. proposed an adaptive convolution-based evaluation method of steganalysis accuracy. Their experimental results proved that an image with a small S value has low detection accuracy. In fact, the S value is the justification for carrier selection. Several other methods[27] were proposed for robust watermarking. Most of the existing schemes for carrier selection have a complex procedure and do not consider the running speed, which make them unsuitable for large-scale application of steganography. However, this does not mean that all of the schemes, such as those presented in Refs. [26–28], are useless because a fast (although may not have an extremely high security level) algorithm, like the method proposed in this study, can be used for preselection to improve the entire running speed considerably. In Ref. [26], Wang et al. determined that the strength of pixel correlation indicates the noise level, which guarantees the security of the carrier. To further analyze the correlation between pixels, the linear regression of spatial pixels is discussed in the next subsection.

2.2 Correlation between pixels

To our knowledge, steganalysis features are extracted by high-pass filtering[8, 9, 12], or transformation of spatial pixels[7, 8, 31, 32], or Discrete Cosine Transform (DCT) coefficients[9, 11]. The residual matrix $\boldsymbol{R}$ used for steganalysis can be represented as $\boldsymbol{R} = \boldsymbol{I} \times \boldsymbol{K}_h$, or $\boldsymbol{R} = \boldsymbol{I} - \boldsymbol{I} \times \boldsymbol{K}_l$, where $\boldsymbol{I}$ is the image and $\boldsymbol{K}_h$ and $\boldsymbol{K}_l$

are the high-pass and low-pass kernels, respectively. If the differences between cover and stego residuals are reduced, then steganography will be safer than before. However, reducing the distortions of all kinds of residuals is difficult, which is a problem need to be addressed. One possible solution is to increase the image noise of both cover and stego residuals, so that the classifier is unable to distinguish them easily. However, in reality, this is not a good solution because any artificial noise in images should be regarded as secret information. A feasible approach is to select the image with inherent and strong noise. In fact, the strong noise inevitably reduces the pixel correlation, which means that images with weak pixel correlation are suitable for embedding.

A total of 10 000 gray images of BOSSbase 1.01[33] are selected to conduct this experiment. These gray images are compressed to JPEG format with a Quality Factor (QF) of 75. Then, 100 000 local blocks (10 blocks from each image) with the size of 3 × 3 are selected randomly. Each block can be represented as $\boldsymbol{B}_{3\times 3}$, as expressed in Eq. (1). Notably, the spatial pixels are not integral type but decimal type because they are calculated by inverse DCT.

$$\boldsymbol{B}_{3\times 3}=\begin{pmatrix} X_1 & X_2 & X_3 \\ X_4 & Y & X_5 \\ X_6 & X_7 & X_8 \end{pmatrix} \tag{1}$$

To conduct this research conveniently, the correlation between pixels is considered a linear relationship. The linear relationship between the middle pixel value Y and its adjacent pixels $X=\{X_k\}$ $(k=1,2,\ldots,8)$ can be calculated by linear regression, as expressed in

$$Y=\theta_0+\sum_{t=1}^{8}\theta_t X_t \tag{2}$$

where θ_t $(t=0,1,\ldots,8)$ is the regression coefficient of each adjacent pixel. For convenience, the bias $\theta_0=0$. The regression coefficients can also be represented as a coefficient matrix, as expressed

$$\boldsymbol{\theta}_{3\times 3}=\begin{pmatrix} \theta_1 & \theta_2 & \theta_3 \\ \theta_8 & 0 & \theta_4 \\ \theta_7 & \theta_6 & \theta_5 \end{pmatrix} \tag{3}$$

The linear prediction of the middle pixel can be represented as $\boldsymbol{Y}=\boldsymbol{\theta}_{3\times 3}\times\boldsymbol{X}$. After linear regression, the coefficient matrix is expressed in Eq. (4), which is similar to the high-pass convolution kernel of SRM[8].

$$\boldsymbol{\theta}_{3\times 3}=\begin{pmatrix} -0.23 & 0.48 & -0.23 \\ 0.48 & 0 & 0.47 \\ -0.23 & 0.46 & -0.21 \end{pmatrix} \tag{4}$$

Moreover, the local block $\boldsymbol{B}_{5\times 5}$ with the size of 5 × 5 has weight matrix of $\boldsymbol{\theta}_{5\times 5}$, as expressed in the following:

$$\boldsymbol{\theta}_{5\times 5}=\begin{pmatrix} -0.02 & 0.09 & -0.16 & 0.08 & -0.02 \\ 0.07 & -0.29 & 0.53 & -0.27 & 0.07 \\ -0.15 & 0.56 & 0 & 0.55 & -0.14 \\ 0.07 & -0.27 & 0.53 & -0.28 & 0.07 \\ -0.02 & 0.06 & -0.13 & 0.06 & -0.01 \end{pmatrix} \tag{5}$$

Notably, adjacent or near pixels have a strong correlation, whereas the two distant pixels have a weak correlation. To our knowledge, steganography aims to increase the difficulty of pixel prediction, so that the high-pass filtering cannot get embedding modifications. This explains why the SRM[8] feature exhibits a good steganalysis performance not only in spatial images but also in JPEG images: All the kernels of SRM follow the relationship expressed in Eqs. (4) and (5), which show the most accurate linear prediction of pixels.

3 Proposed Scheme

3.1 Extraction of pixel pairs

According to the experiment presented in Section 2.2, the linear regression results indicate that the relationship between adjacent pixels in the 3 × 3 area is stronger than that between distant pixels because the adjacent weights used to predict the middle pixel are larger than the others. Obviously, the correlation between adjacent pixels determines the security of the carrier. By contrast, the relationship between distant pixels is usually weak and not suitable for steganalysis. We know that there are four different pixel pairs, that are independent of horizontal, vertical, counter diagonal, and major diagonal directions in the 3 × 3 area. In this study, the relationship between four different pixel pairs will be considered as the security of carrier. As shown in Fig. 1, $I_{i,j}$ is the i-th row and j-th column pixel in the JPEG image $\boldsymbol{I}_{H\times W}=\left(I_{i,j}\right)_{H\times W}$. $P_{\rightarrow}=\left\{I_{i,j},I_{i,j+1}\right\}$, $P_{\downarrow}=\{I_{i,j},I_{i+1,j}\}$, $P_{\nearrow}=\left\{I_{i,j},I_{i-1,j+1}\right\}$, and $P_{\searrow}=\{I_{i,j},I_{i+1,j+1}\}$ are the horizontal, vertical, counter diagonal, and major diagonal pixel pairs, respectively. To evaluate the security of a JPEG image, each pixel pair of the image is extracted, where $i=1,2,\ldots,H-1$ and $j=1,2,\ldots,W-1$.

The spatial pixel $I_{i,j}$ is decompressed from the inverse quantization of the DCT coefficient $f(u,v)$, and the calculation formulas are expressed in Eqs. (6) and (7).

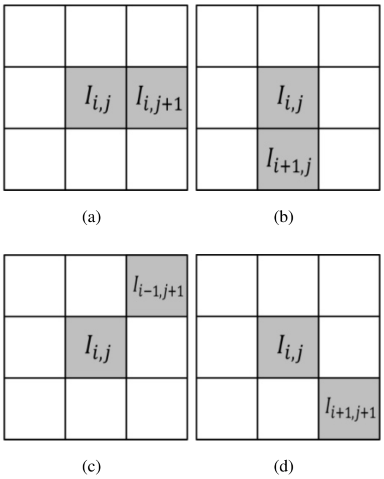


Fig. 1 Four types of pixel pairs in spatial domain.

$$I_{i,j} = I_{a,b}^{m,n} = \frac{1}{4} c(u)\, c(v) \times \left[\sum_{u=0}^{7}\sum_{v=0}^{7} f(u,v) \cos\frac{(2a+1)u\pi}{16} \cos\frac{(2b+1)v\pi}{16}\right] + 128 \tag{6}$$

$$\begin{cases} c(u) = \frac{1}{2}, c(v) = \frac{1}{2}, & u, v = 0; \\ c(u) = 1, c(v) = 1, & u, v \neq 0 \end{cases} \tag{7}$$

where $I_{a,b}^{m,n}$ denotes the a-th row and b-th column pixel $I_{i,j}$ in JPEG block $\boldsymbol{O}^{m,n}$ with the size of 8×8, $1 \leqslant m \leqslant \left[\frac{H-1}{8}\right] + 1$, $1 \leqslant n \leqslant \left[\frac{W-1}{8}\right] + 1$, $m = \left[\frac{i}{8}\right]$, $n = \left[\frac{j}{8}\right]$, $a = i - 8\left\lfloor\frac{i}{8}\right\rfloor$, and $b = j - 8\left\lfloor\frac{j}{8}\right\rfloor$.

3.2 Calculation of the correlation coefficient

Suppose A is a decompressed pixel of the JPEG image and B is an adjacent pixel of A, where $A \in \{I_{i,j}\}$ and $B \in \{I_{i,j+1}, I_{i+1,j}, I_{i-1,j+1}, I_{i+1,j+1}\}$. In general, the random variables A and B are not mutually independent. In this study, we use Pearson correlation coefficient $\rho(A, B)$ as expressed in Eq. (8), to assess the linear correlation between the variables of A and B,

$$\rho(A, B) = \frac{\operatorname{cov}(A, B)}{\sqrt{D(A)} \times \sqrt{D(B)}} \tag{8}$$

where $-1 \leqslant \rho(A, B) \leqslant 1$, $D(A)$ and $D(B)$ are the variances of A and B, respectively, and $\operatorname{cov}(A, B)$ is the covariance of A and B, which can be calculated as $\operatorname{cov}(A, B) = E(AB) - E(A)E(B)$, where $E(A)$, $E(B)$, and $E(AB)$ are the expectation of A, B, and AB, respectively. The correlation coefficients of the four pixel pairs shown in Fig. 1 can be calculated using Eqs. (9) – (12).

$$C_{\rightarrow} = \rho\left(I_{i,j}, I_{i,j+1}\right) \tag{9}$$

$$C_{\downarrow} = \rho\left(I_{i,j}, I_{i+1,j}\right) \tag{10}$$

$$C_{\nearrow} = \rho\left(I_{i,j}, I_{i-1,j+1}\right) \tag{11}$$

$$C_{\searrow} = \rho\left(I_{i,j}, I_{i+1,j+1}\right) \tag{12}$$

where $2 \leqslant i \leqslant H - 1$ and $2 \leqslant j \leqslant W - 1$. The four correlation coefficients of each spatial image represent the four types of relationships between adjacent pixels, and their mean value are calculated to evaluate the total correlation, as expressed in

$$C = \frac{1}{4}\left(C_{\rightarrow} + C_{\downarrow} + C_{\nearrow} + C_{\searrow}\right) \tag{13}$$

In theory, the C value ranges from -1 to $+1$. $C = -1$ indicates that a linear negative correlation exists between adjacent pixels and $C = 1$ indicates that a linear positive correlation exists between adjacent pixels.

Carrier-selection-based steganography

A large absolute value of C indicates that the adjacent pixels have a strong correlation. Actually, we observe that the C value is always a positive value. According to this hypothesis, JPEG images with a small C value are more suitable for embedding. The flowchart of our proposed method is shown in Fig. 2. The entire procedure is divided into the following steps:

(1) Extraction of pixel pairs: According to Eqs. (6) and (7), first, JPEG images are decompressed to spatial domain. Then the four types of pixel pairs (as shown in Fig. 2) are extracted.

(2) Calculation of the correlation coefficient: For a given JPEG image, the correlation coefficient of each type of pixel pair is calculated using Eqs. (8) – (12), and the mean values of $C_{\rightarrow}$, $C_{\downarrow}$, $C_{\nearrow}$, and $C_{\searrow}$ are used for security evaluation of the image.

(3) Carrier selection: The images with the value C lesser than T are selected for embedding, where the T is a threshold for selection.

(4) Embedding of secret information: Existing embedding algorithms, such as JC-UED[20] and J-UNIWARD[21], are adopted for steganography.

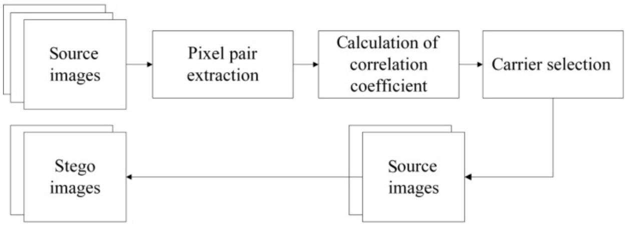


Fig. 2 Flow chart of proposed scheme.

4 Experiment

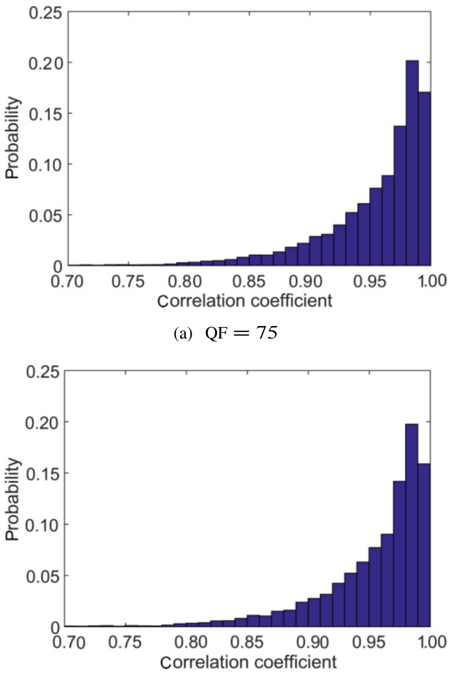
4.1 Preparation

In this section, DCTR[11], PHARM[12], and GFR[13] are used to evaluate the performance of our proposed scheme. Moreover, an ensemble classifier[10] is used for the classification of this high-dimensional feature. The cover images are 10 000 gray images of BOSSbase 1.01[33] compressed with the QF of 75 and 95. Then, the corresponding stego images are generated by the steganography algorithms JC-UED[20] and J-UNIWARD[21]. Each embedding algorithm adopts the payloads of 0.2, 0.3, and 0.4 bpnzAC, where the bpnzAC denotes the bits per nonzero AC coefficient.

4.2 Distribution of the correlation coefficient

The correlation coefficients of cover images with the QF of 75 and 95 are calculated, and their probability distributions are shown in Fig. 3.

Most of the images have correlation coefficients in the interval of [0.8, 1], which indicates that the middle pixel has a positive and approximate linear correlation with its adjacent pixels. Moreover, through careful comparison, we determine that the C value of images with $\text{QF} = 95$ is smaller than that of images with $\text{QF} = 75$ mainly because DCT compression can be regarded as the denoising operation of spatial pixels, particularly compression with a small QF. Actually, the detection errors of images with $\text{QF} = 95$ are higher than those of images with $\text{QF} = 75$. Obviously, the QF influences carrier security.



(a) $\text{QF} = 75$

(b) $\text{QF} = 95$

Fig. 3 Probability distribution of correlation coefficient of cover images with QF equals 75 and 95.

4.3 Testing errors under different correlation coefficients

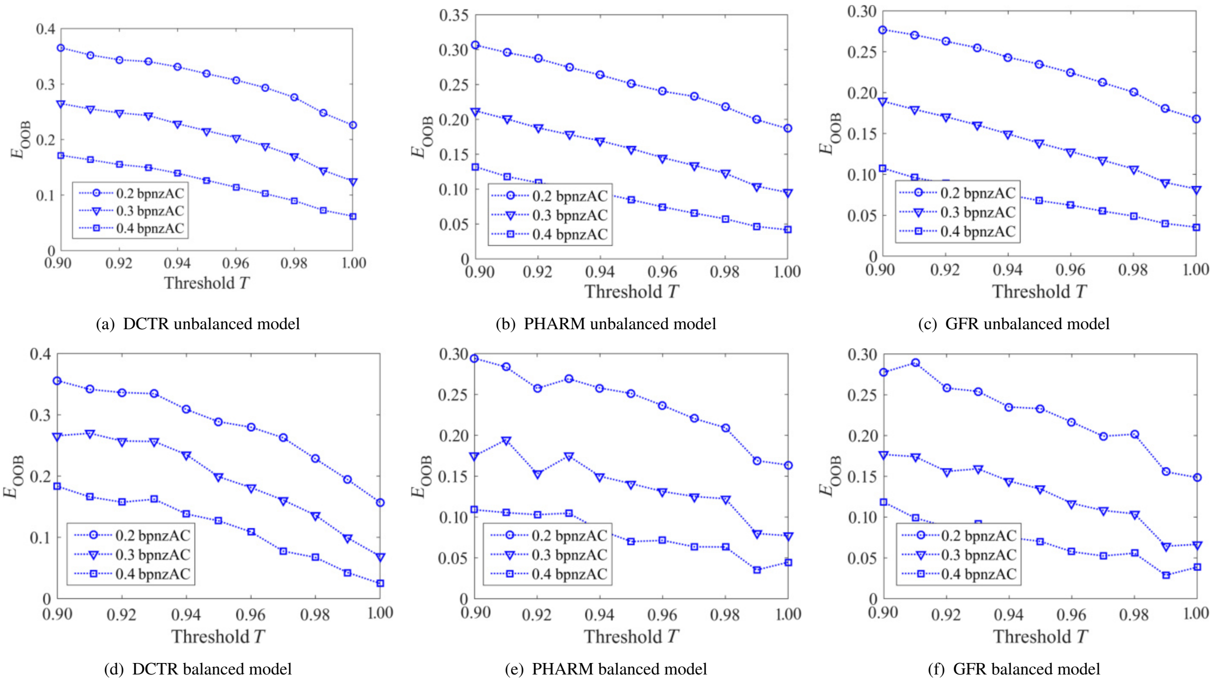
In this experiment, 5000 cover images and their corresponding 5000 stego images, which are represented as Trn5000, are randomly selected for training. The remaining cover images and their corresponding stego images, which are represented as Tst5000, are used for testing. To eliminate the effect of the discrepancies between different C values, two types of training and testing strategies involved in our experiments are as following.

Unbalanced model: The cover images of Tst5000 with the correlation coefficient $C < T$ are selected as the testing cover images and their corresponding stego images are selected as the testing stego images.

Balanced model: First, the cover images of Trn5000 are divided into 11 intervals according to $[T-0.01, T]$, $T = 1-0.01(i-1), i = 1, 2, \ldots, 11$. Then, 100 cover images and their corresponding stego images are randomly selected from each interval for training. Finally, the cover images of Tst5000 are also divided into the 11 intervals. Therefore, the C value is relatively evenly distributed in the training images, and the testing errors are evaluated on a relatively concentrated interval of the C value.

Each selection of training and testing images is repeated five times to obtain five groups. The mean testing error E_{OOB} of each group, which is evaluated using DCTR, PHARM, and GFR, is shown in Figs. 4 – 7.

The experiments show that the performance of DCTR, PHARM, and GFR similarly varies with the decrease in threshold T: All of the testing errors of different payloads obviously increase. The traditional scheme considers all of the carrier images to have the same security level, which corresponds to the situation of the unbalanced model with $T = 1$ in our proposed scheme. Notably, $T = 1$ has the lowest security level under any payload or embedding algorithm. As the T value decreases from 1 to 0.9, the detection errors increase by more than 10% points. Obviously, this rule has the same beneficial effect on different embedding algorithms and payloads.



(a) DCTR unbalanced model

(b) PHARM unbalanced model

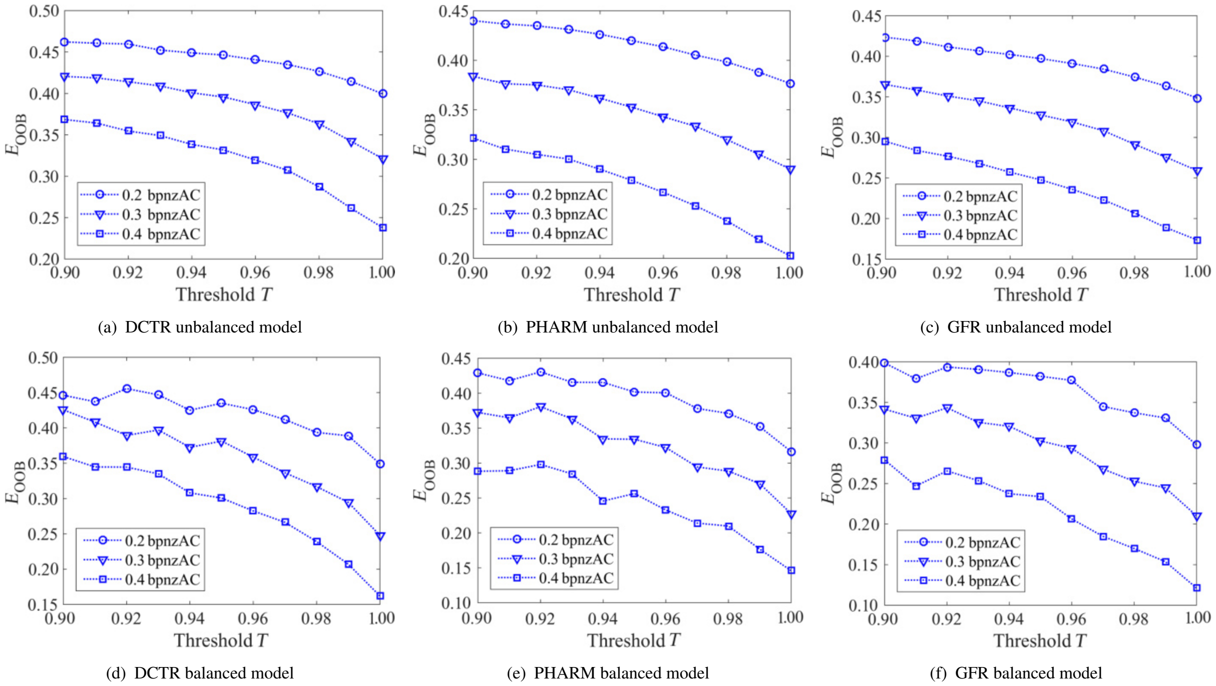
(c) GFR unbalanced model

(d) DCTR balanced model

(e) PHARM balanced model

(f) GFR balanced model

Fig. 4 Mean testing error E_{OOB} for JC-UED for quality factor 75.



(a) DCTR unbalanced model

(b) PHARM unbalanced model

(c) GFR unbalanced model

(d) DCTR balanced model

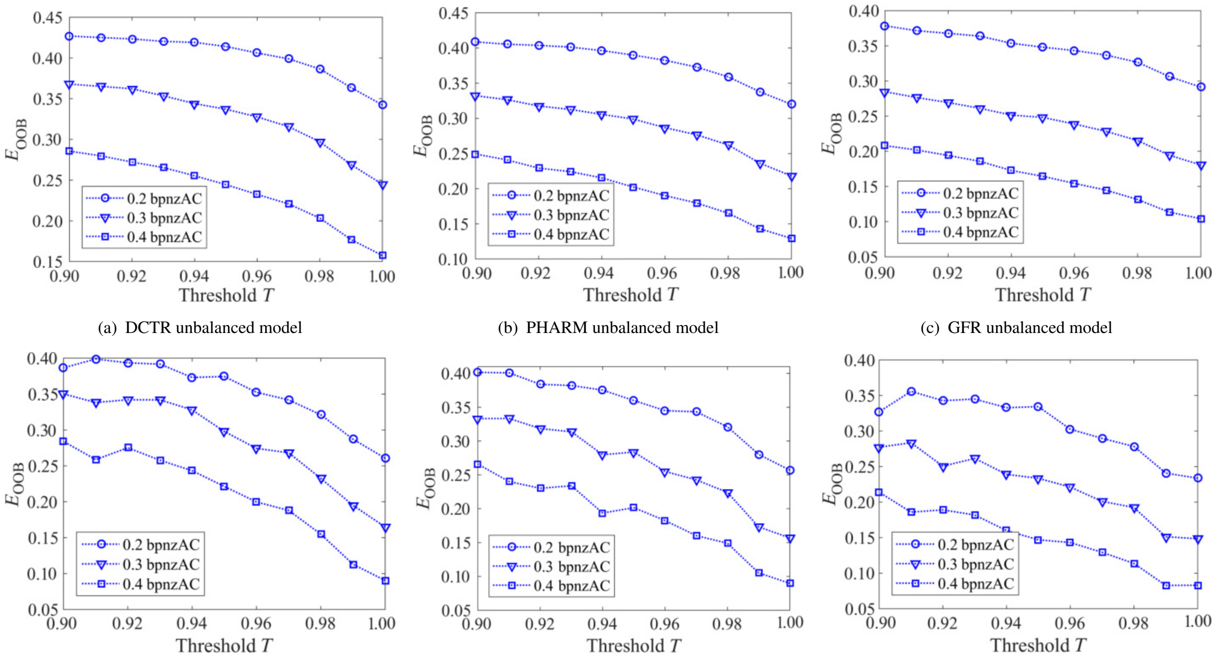
(e) PHARM balanced model

(f) GFR balanced model

Fig. 5 Mean testing error E_{OOB} for JC-UED for quality factor 95.

4.4 Study of the absolute embedding capacity

The experiments indicate that JPEG images with the same bpnzAC payload and a high pixel correlation coefficient have a high security level. However, the same bpnzAC payload does not represent the same embedding bits because the images have different ratios of nonzero AC coefficients. The relationship between the C value and the ratios of nonzero AC coefficients is shown in Fig. 8. In Fig. 8, JPEG images with the same bpnzAC payload have different numbers of AC coefficients, which result in different security levels between images with the same embedding bits. Under the premise of the same security level, a good embedding algorithm always tries to embed secret information as much as



(a) DCTR unbalanced model

(b) PHARM unbalanced model

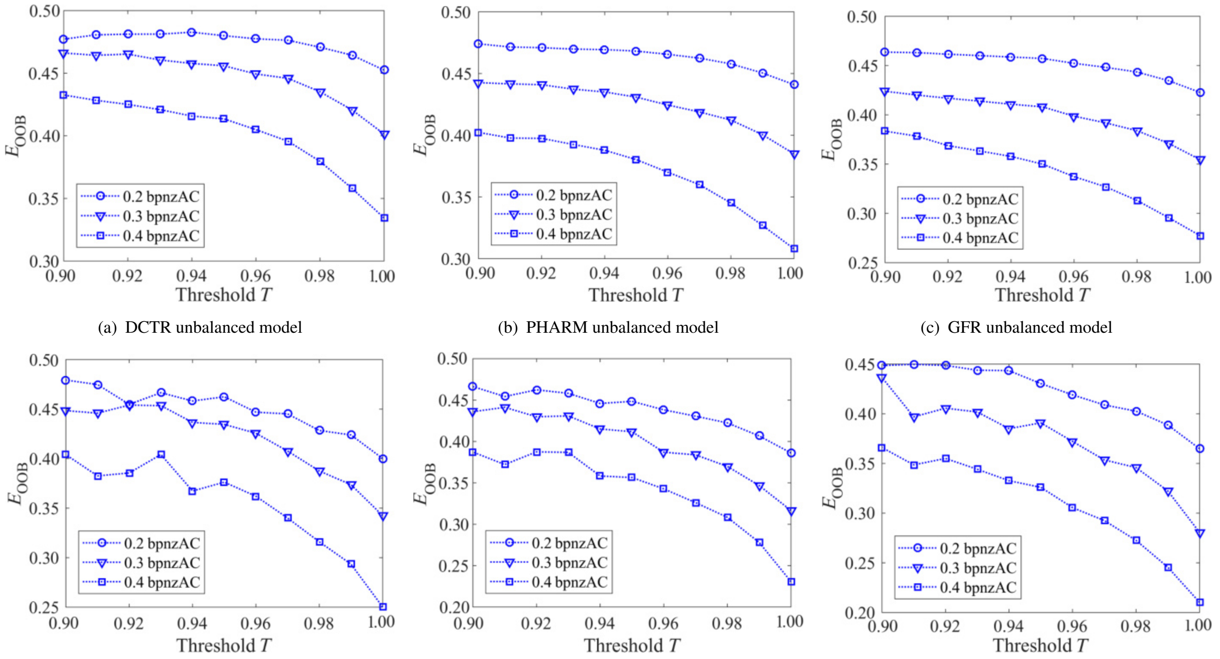
(c) GFR unbalanced model

(d) DCTR balanced model

(e) PHARM balanced model

(f) GFR balanced model

Fig. 6 Mean testing error E_{OOB} for J-UNIWARD for quality factor 75.



(a) DCTR unbalanced model

(b) PHARM unbalanced model

(c) GFR unbalanced model

(d) DCTR balanced model

(e) PHARM balanced model

(f) GFR balanced model

Fig. 7 Mean testing error E_{OOB} for J-UNIWARD for quality factor 95.

possible. In other words, under the premise of the same secret information, a good embedding algorithm tries to embed the information as securely as possible. All of the experiments prove that images with the same size and low C values are safer carriers than those with high C values. The embedding algorithm usually needs to embed not a bpnzAC payload but information with a given length in practical application. The embedding capacity depends on the ratio of nonzero AC coefficients, which is calculated by

$$R = \frac{\sum\limits_{i}^{i=k} \delta\left(A_i\right)}{k} \tag{14}$$

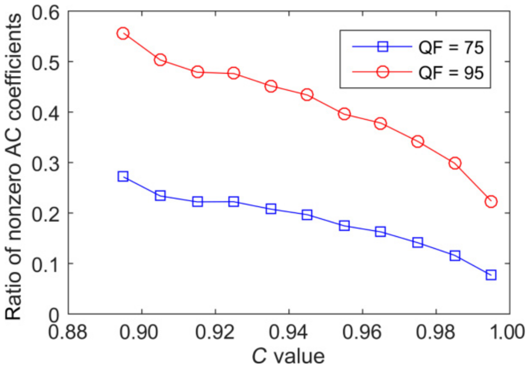


Fig. 8 Ratio of nonzero AC coefficients with different quality factors.

where A_i $(i = 1, 2, \ldots, k)$ is the AC coefficient after quantization, and $\delta(A_i) = 1$ and 0 denote $A_i \neq 0$ and $A_i = 0$, respectively. The original DCT coefficients a_i will be converted into A_i in the quantization process, as expressed in

$$A_i = \left[\frac{a_i}{q_i}\right] \tag{15}$$

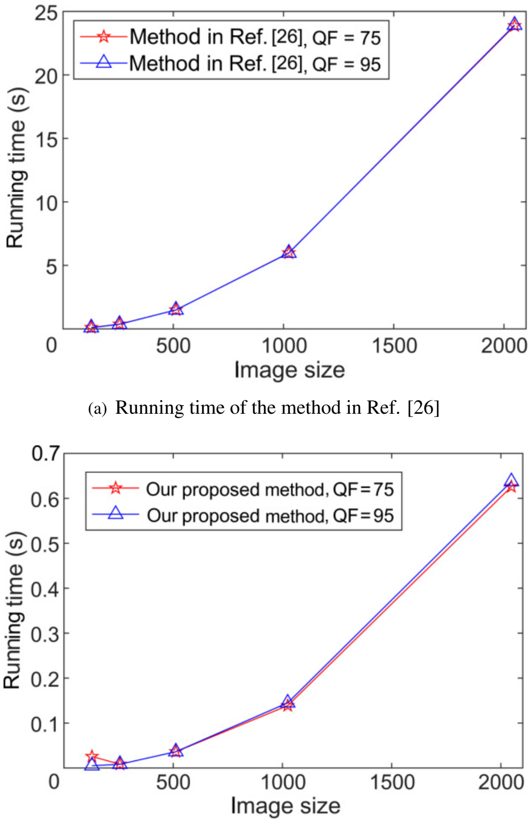
where the $[\cdot]$ is the rounding operation. Accordingly, the inverse quantization is formulated, as expressed in

$$a_i' = A_i \cdot q_i \tag{16}$$

where q_i is the quantization step and a_i' is the inverse coefficient of A_i. Normally, images with QF = 95 have a high ratio of nonzero AC coefficients because they have small quantization step. According to Eq. (16), the ±1 modification of A_i of an image with QF = 75 will have more significant effects on spatial pixels because its quantization step ±1 is larger than that of an image with QF = 95. The tests presented in Section 4.3 prove that QF is one of the important factors that influences the security of steganography.

4.5 Comparison of running speed

In this section, 1000 images are randomly selected from BOSSBase 1.01[33] and are resized to 128 × 128, 256 × 256, 1024 × 1024, and 2048 × 2048. Then, all of the images are compressed to JPEG images with QF = 75 and QF = 95. Including the original image with the size of 512 × 512, all of these images can be divided into 5 groups on the basis of their sizes, and each group has 1000 images. The C value of each image in each group is calculated, and the corresponding running time of each image in each group is shown in Fig. 9. To compare the running speeds, the running time in Ref. [26] is also given. All of the experiments on running speed are conducted on a PC with Windows 8.1 (64 bit), 500 GB solid state drives, 8 GB DDR3 RAM, Intel® Core™ i5-3470 CPU @ 3.20 GHz and MATLAB 2015b (64 bit).



(a) Running time of the method in Ref. [26]

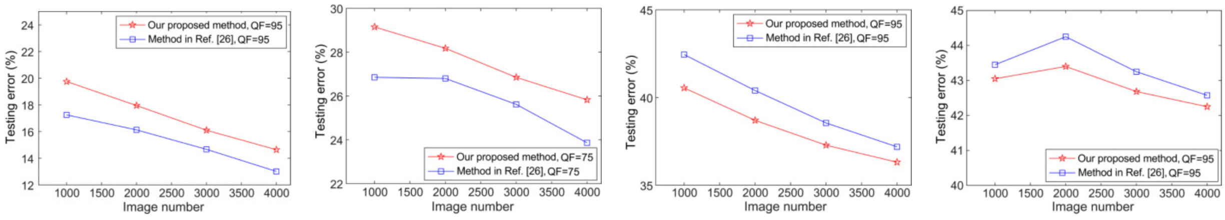
(b) Running time of our proposed scheme

Fig. 9 Running time of images with different image sizes.

Notably, the running time in Ref. [26] increases from approximately 1 s to 18 s with the increase in image size. Obviously, the proposed scheme in this study has a faster running speed than that in Ref. [26]. The running time of the proposed method increases from approximately 0 s to 0.8 s with the increase in image size. The mean running time of a 2048 × 2048 image which is large and common, is less than 1 s. For 100 images with the size of 1024 × 1024, the calculation represented in Ref. [26] will take approximately 7 min, whereas the calculation using our proposed scheme will only take approximately 20 s. Furthermore, the mean running time for an image with a large size proves that our method is fast and can be easily applied in the actual environment.

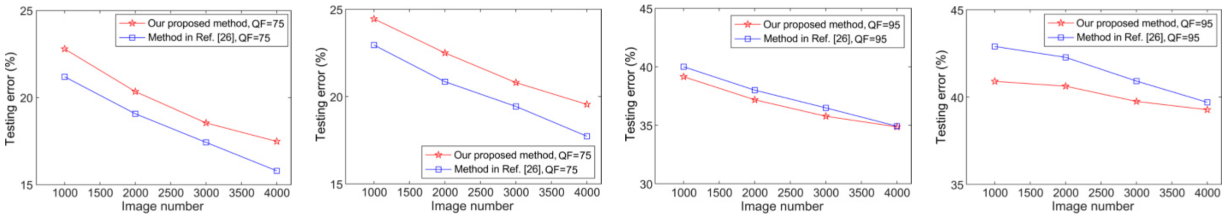
4.6 Comparison of the testing errors

In this section, the top 1000, 2000, 3000, and 4000 images are selected from Tst5000 on the basis of their $S^{[26]}$ and C values to compare their performance. The testing errors of JC-UED and J-UNIWARD with a payload of 0.3 bpnzAC evaluated using DCTR, PHARM, and GFR are shown in Figs. 10 – 12. Notably, the proposed scheme exhibits a better performance on



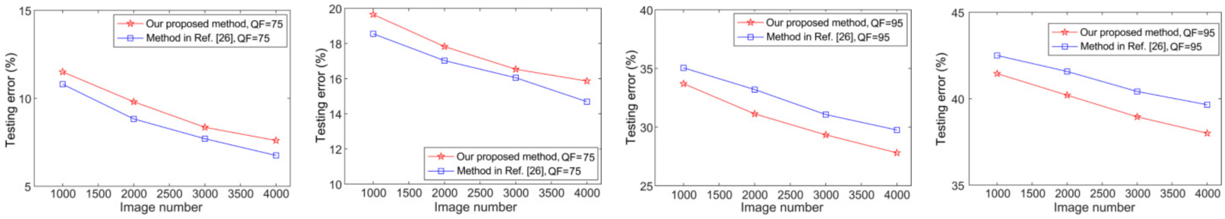
(a) JC-UED (b) J-UNIWARD (c) JC-UED (d) J-UNIWARD

Fig. 10 Testing error of DCTR.



(a) JC-UED (b) J-UNIWARD (c) JC-UED (d) J-UNIWARD

Fig. 11 Testing error of PHARM.



(a) JC-UED QF=75 (b) J-UNIWARD QF=75 (c) JC-UED QF=95 (d) J-UNIWARD QF=95

Fig. 12 Testing error of GFR.

images with QF $=$ 75 but exhibits a worse performance compared with the scheme presented in Ref. [26] on images with QF $=$ 95. Generally, the proposed scheme exhibits a similar performance to the scheme presented in Ref. [26].

5 Conclusion

The correlation between spatial pixels determines whether the middle pixels can be predicted using its surrounding pixels. If a JPEG image has weak correlations between its spatial pixels, then it will make a less accurate prediction of pixels leading to hard steganalysis. According to this principle, the security of steganography can be improved effectively through carrier selection. Conversely, the randomly selected carriers cannot provide a guarantee of expected security, even if an algorithm with a high security level and a low payload is utilized to embed secret information. Many factors, including image size, compression parameters, embedding algorithm, embedding payload, and the correlation between spatial pixels, affect security of steganography. Many images can be easily collected for carrier selection in the real world because of the powerful Internet. However, embedding algorithms have to evaluate the security of each image separately, which may lead to slow embedding, particularly with a wide variety and large number of images. A quick, feasible, and efficient algorithm for security evaluation seems more important than complex and one-sided security evaluation. In essence, the correlation coefficient used for security evaluation, such as the C value, is a ranking method of carrier security, so that the method is comparable and can be improved in terms of validity in the future.

Acknowledgment

This work was supported by the National Key Program of Natural Science Foundation of China (No. U1536204) and the National Natural Science Foundation of China (Nos. U1836112, 61876134, and 61872275).

References

[1] M. C. Trivedi, S. Sharma, and V. K. Yadav, Analysis of several image steganography techniques in spatial domain: A survey, in *Proceedings of the Second International*

Conference on Information and Communication Technology for Competitive Strategies, Rajasthan, India, 2016, p. 84.

[2] M. Hussain, A. W. Wahab, Y. I. Idris, A. T. Ho, and K. Jung, Image steganography in spatial domain: A survey, *Signal Processing-Image Communication*, vol. 65, pp. 46–66, 2018.

[3] Y. Zhang, M. Zhang, X. Yang, D. Guo, and L. Liu, Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC, *Tsinghua Science & Technology*, vol. 22, no. 2, pp. 198–209, 2017.

[4] S. Xu, P. Zhang, P. Wang, and H. Yang, Performance analysis of data hiding in MPEG-4 AAC Audio, *Tsinghua Science & Technology*, vol. 14, no. 1, pp. 55–61, 2009.

[5] W. Ren, Y. Liu, and J. Zhao, Provably secure information hiding via short text in social networking tools, *Tsinghua Science & Technology*, vol. 17, no. 3, pp. 225–231, 2012.

[6] K. Karampidis, E. Kavallieratou, and G. Papadourakis, A review of image steganalysis techniques for digital forensics, *Journal of Information Security and Applications*, vol. 40, pp. 217–235, 2018.

[7] T. Pevny, P. Bas, and J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215–224, 2010.

[8] J. Fridrich and J. Kodovsky, Rich models for steganalysis of digital images, *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[9] J. Kodovsky and J. Fridrich, Steganalysis of JPEG images using rich models, in *Proceedings of Media Watermarking, Security, and Forensics*, Burlingame, CA, USA, 2012, pp. 81–93.

[10] J. Kodovsky, J. Fridrich, and V. Holub, Ensemble classifier for steganalysis of digital media, *IEEE Transactions on Information Forensics and Security*. vol. 7, no. 2, pp. 432–444, 2012.

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

[12] X. Song, F. Liu, C. Yang, X. Luo, and Y. Zhang, Steganalysis of adaptive JPEG steganography using 2D Gabor filters, in *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, Portland, OR, USA, 2015, pp. 15–23.

[13] V. Holub and J. Fridrich, Phase-aware projection model for steganalysis of JPEG images, in *Proceedings of Media Watermarking, Security, and Forensics*, San Francisco, CA, USA, 2015, pp. 259–269.

[14] J. Zeng, S. Tan, B. Li, and J. Huang, Large-scale JPEG image steganalysis using hybrid deep-learning framework, *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1200–1214, 2018.

[15] S. Wu, S. Zhong, and Y. Liu, Deep residual learning for image steganalysis, *Multimedia Tools and Applications*, vol. 77, no. 9, pp. 10437–10453, 2018.

[16] M. Boroumand, M. Chen, and J. Fridrich, Deep residual network for steganalysis of digital images, *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1181–1193, 2019.

[17] T. Filler, J. Judas, and J. Fridrich, Minimizing additive distortion in steganog-raphy using syndrome-trellis codes, *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935. 2011.

[18] T. Pevn, T. Filler, and P. Bas, Using high-dimensional image models to perform highly undetectable steganography, *Information Hiding*, doi: 10.1007/978-3-642-16435-4_13.

[19] C. Wang and J. Ni, An efficient JPEG steganographic scheme based on the block entropy of DCT coeffcients, in *Proceedings of 2012 IEEE International Conference on Acoustics, Speech and Signal Processing*, Kyoto, Japan, 2012, pp. 1785–1788.

[20] L. Guo, J. Ni, and Y. Shi, Uniform embedding for efficient JPEG steganography, *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 814–825, 2014.

[21] V. Holub and J. Fridrich, Digital image steganography using universal distortion, in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, Montpellier, France, 2013, pp. 59–68.

[22] V. Sedighi, R. Cogranne, and J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2015.

[23] J. Kodovsky, V. Sedighi, and J. Fridrich, Study of cover source mismatch in steganalysis and ways to mitigate its impact, in *Proceedings of Media Watermarking, Security, and Forensics*, San Francisco, CA, USA, 2014, pp. 204–215.

[24] Q. Gibouloto, R. Cogranneo, and P. Bas, Steganalysis into the wild: How to define a source? *Electronic Imaging*, vol. 2018, no. 7, p. 318, 2018.

[25] M. Yedroudj, M. Chaumont, and F. Comby, How to augment a small learning set for improving the performances of a CNN-based steganalyzer? *Electronic Imaging*, vol. 2018, no. 7, p. 317, 2018.

[26] L. Wang , Y. Xu , L. Zhai, Y. Ren, and B. Du, A posterior evaluation algorithm of steganalysis accuracy inspired by residual co-occurrence probability, *Pattern Recognition*, vol. 87, pp. 106–117, 2019.

[27] M. S. Subhedar and V. H. Mankar, Curvelet transform and cover selection for secure steganography, *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8115–8138, 2018.

[28] Z. Wang, X. Zhang, and Z. Yin, Joint cover-selection and payload-allocation by steganographic distortion optimization, *IEEE Signal Processing Letters*, vol. 25, no. 10, pp. 1530–1534, 2018.

[29] J. Kodovsky and J. Fridrich, Calibration revisited, in *Proceedings of the 11th ACM Workshop on Multimedia and Security*, Princeton, NJ, USA, 2009, pp. 63–74.

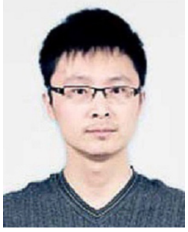
[30] F. Li, K. Wu, J. Lei, M. Wen, and Y. Ren, Unsupervised steganalysis over social networks based on multi-reference sub-image sets, *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 17953–17971, 2018.

[31] X. Song, F. Liu, L. Chen, C. Yang, and X. Luo, Optimal Gabor filters for steganalysis of content-adaptive JPEG steganography, *KSII Transactions on Internet and Information Systems*, vol. 11, no. 1, pp. 552–569, 2017.

[32] B. Li, Z. Li, S. Zhou, S. Tan, and X. Zhang, New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator, *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1242–1257, 2018.

[33] P. Bas, T. Filler, and T. Pevny, Break our steganographic system: The ins and outs of organizing BOSS, *Information Hiding*, vol. 6958, pp. 59–70, 2011.

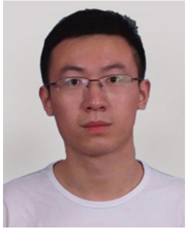
Weixiang Ren received the BS degree from Zhengzhou University, China in 2010, and the MS degree from Guizhou University, China in 2016. He is a PhD candidate in the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His main research interests include information hiding, machine learning, and deep learning.



Yibo Xu received the MS degree from Hefei University of Technology, China in 2012, and the PhD degree from Wuhan University, China in 2018. He is a researcher in Micropattern Company, Wuhan, China. His current research interests include information hiding, machine learning, and watermarking.

Liming Zhai received the BS degree from Shanxi University, China in 2014. He is now a PhD candidate in the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His main research interests include steganography and steganalysis, machine learning, and deep learning.

Lina Wang received the PhD degree from Northeastern University, China in 2001. She is a professor in the School of Cyber Science and Engineering, Wuhan University. She is a member of China Computer Federation. Her main research interests include system security and information hiding.



Ju Jia received the BS degree from Wuhan University of Science and Technology, China in 2014 and the MS degree from Central China Normal University, China in 2017. He is a PhD candidate in the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His main research interests include steganography and steganalysis, machine learning, and deep learning.