Hindawi
Security and Communication Networks
Volume 2021, Article ID 9153468, 15 pages
https://doi.org/10.1155/2021/9153468

Research Article

Improving Anticompression Robustness of JPEG Adaptive Steganography Based on Robustness Measurement and DCT Block Selection

Haocheng Fu,[1,2] **Xianfeng Zhao**,[1,2] **and Xiaolei He**[1,2]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering Chinese Academy of Sciences, Beijing 100195, China*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100195, China*

Correspondence should be addressed to Xianfeng Zhao; zhaoxianfeng@iie.ac.cn

Received 6 September 2021; Accepted 23 November 2021; Published 18 December 2021

Academic Editor: Jinwei Wang

With the development of the Internet, social network platforms (SNPs) have become the most common channel for image sharing. As a result, transmitting stego images in the public channels gives steganographers the best opportunity to transmit secret messages with behavioral security preserved. However, the SNPs typically compress uploaded images and damage the weak signal of steganography. In this study, a robust JPEG steganographic scheme based on robustness measurement and cover block selection (CBSRS) is proposed. We first design a deep learning-based model to fit the blockwise change rate of coefficients after JPEG recompression. Then, a cover block selection strategy is proposed to improve the robustness by optimizing the joint distortion function of transmission costs and classic costs. Moreover, by embedding indicator of cover block selection in chrominance channels of JPEG images, a shareable cover construction scheme is designed to solve the problem of auxiliary information transmission. The experimental results show that our proposed framework improves robustness while maintaining statistical security. Comparing with state-of-the-art methods, the framework achieves better performance under given recompression channels.

1. Introduction

Steganography is an advanced art of covert communication encoding secret messages into natural-looking covers while transmitting data without arousing attention of the others [1]. With the widespread use of JPEG format images, modern frameworks of JPEG image steganography are deeply researched and generally designed by minimizing modification distortion with matrix coding, e.g., Syndrome-Trellis codes (STCs) [2] and steganographic polar codes (SPCs) [3]. Meanwhile, distortion functions of JPEG images, such as J-UNIWARD [4], UED [5], and UERD [6], achieve highly statistical undetectability when against both high-dimensional feature extractors [7, 8] and deep learning-based steganalyzer [9–11]. However, most of these steganography schemes are proposed under the hypothesis that the communication relationship of the sender and receiver is secure and the transmission channel of JPEG stego images is lossless.

To overcome the deficiency of classic schemes, the traditional one-to-one transmission mode must be replaced or optimized. In [12], Zhao et al. proposed a sharing-based model with public channels for steganography, with which the both statistical security and behavioral security of covert communication can be maintained. In this model, social network platforms (SNPs), the most common channels for multimedia sharing, are adopted for the construction of sharing-based steganographic communication model in real-world. Since SNPs form a new way for individuals to update their trends of life with various carriers such as images and videos [13, 14], it provides a one-to-many transmission method which weakens the connectivity of the

parties of communication. However, SNPs generally recompress uploaded multimedia files to review their content and optimize storage spaces into a uniform format. The JPEG recompression operation, especially with the fixed quantization table, is the most common procedure of the lossy channel of JPEG image transmission. The studying of anticompression steganographic schemes is the key to solving this problem.

To improve the anticompression robustness, robust steganographic schemes are designed with many considerations. Figure 1 shows the typical framework of robust steganography. The stego elements in the selected embedding domain, which will be encoded by specific steganographic code, are expected to remain almost invariant after transmitted in the recompression channel. The error correction codes (ECCs) provide integrity of extracted message from stego images. Besides, the preprocessing and postprocessing are also introduced for better performance. By the optimization above, the robustness of adaptive steganography is significantly improved.

As pointed out in [15], the robustness of the steganographic algorithm and stego images varies from one lossy channel to another, which denotes that the properties of recompression channel affect the performance of robustness. Therefore, the robust adaptive steganographic frameworks can be divided into two categories: "General Robustness" and "Dedicated Robustness" according to the type recompression channel they aim at.

Steganographic frameworks in the "General Robustness" category are designed to improve comprehensive robustness by resisting general lossy properties of JPEG recompression and to preserve the integrity of secret message without considering the specific properties of JPEG recompression channel. In these frameworks, secret messages are embedded in different domains such as quantized pixel values [16–19] and the sign of DCT coefficients [20]. Typically, the amplitude of steganographic modification is larger than one, which introduces larger noise of steganography. As a result, the robustness performance is highly improved at the expense of the decrease of statistical security.

While, "Dedicated Robustness" is a class of robust adaptive steganography that provides reliable robustness performance for specific JPEG recompression channels. These schemes generally regard a JPEG recompression channel as a black box and optimize the procedure of steganography with the specific properties of channels [15, 21], by which the modification amplitude of coefficients is weakened, and the robustness of steganography improved, while the security performance is ensured to a certain extent. However, under the actual circumstances, the image data before and after recompression are available since the recompression channel of SNP is public. As a result, designing a robust steganographic framework in the "Dedicated Robustness" mode is appropriate.

Besides, as the quantization steps adopted in the recompression procedure are fixed in most SNP channels, the quantization tables of the cover JPEG image can be adjusted to the same as those of the recompression channel before steganographic embedding to reduce the error rate of stego image transmission, which shows that the problem of anticompression robust steganography under the same quantization table is more worthy of study.

In this study, a robust adaptive steganographic framework is proposed against any given recompression channel with the same quantization table. First, a deep regression model for DCT block robustness measurement is designed for transmission costs prediction. Then, the cost of steganographic embedding is combined with the blockwise transmission cost, with which the cover DCT block selection scheme is proposed. Furthermore, a shareable cover construction scheme is proposed for the receiver to reconstruct stego blocks and extract embedded messages. Therefore, the proposed framework can be used under any given recompression channel.

The main contributions of this study are as follows:

(1) A novel designed deep learning-based model for robustness measurement of the DCT block is proposed and can be extended to any recompression channel with the same quantization steps. To the best of our knowledge, it is the first model for quantitative analysis of the JPEG image robustness.

(2) The DCT cover block selection strategy is designed for improving both security and robustness performance. Comparing with state-of-the-art robust steganographic schemes, our framework achieves high robustness performance while preserving statistical security.

(3) The shareable cover construction scheme provides high accuracy of auxiliary information recovery, which supports a complete end-to-end robust steganography framework effectively

The main part of this study starts in Section 2, where we restate and expand the preliminaries of JPEG compression and the theory of classic adaptive steganography. In Section 3, the scheme of robustness measurement of the JPEG image is introduced first. Te framework of robust adaptive steganography based on cover block selection is described in Section 4. Section 5 gives the experimental results and analysis in detail. Finally, a brief conclusion of this study is listed in Section 6 as well as our future work.

2. Preliminaries and Related Works

2.1. Notions. In this study, matrices and vectors are written in boldface and sets are written in swash letters. Without loss of generality, let $X = (x_1, x_2, \ldots, x_n) \in \{\mathscr{L}\}^n$ represent a n pixels cover image and $Y = (y_1, y_2, \ldots, y_n) \in \{\mathscr{L}\}^n$ represent the stego image after steganographic embedding on X. $\mathscr{L}$ is the pixel dynamic range of image. As for JPEG images, $\mathscr{L} = \{-1024, -1023, \ldots, 1023\}$, and x_i is the DCT coefficients in i location. Besides, $Q = (q_{ij})$ stands for the quantization table of the JPEG images. The modification pattern of cover element x_i is formulated by $\mathscr{I}_i$. The k-ary entropy function can be denoted by $H_k(\pi)$.

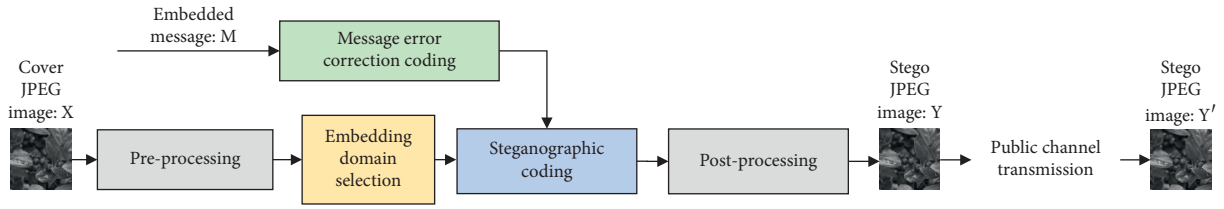

Figure 1: The typical framework of robust steganography.

2.2. JPEG Recompression Procedure. The JPEG recompression is a lossy procedure for digital images because of the quantization and rounding operation, which can be divided into two parts: JPEG compression and JPEG decompression. Generally, for a spatial image $U = (u_i) \in \{0, 1, \ldots, 255\}^n$, with a given quantization table $\mathbf{Q}$, JPEG compress procedure performs mathematical operations on divided disjoint blocks of 8×8 pixels separately, which can be denoted as

$$D = \text{round}\left[\frac{\text{DCT}(U)}{Q}\right], \tag{1}$$

where D denotes the DCT coefficient in JPEG format, and the division above operates elementwise. The functions $\text{DCT}(\cdot)$ and $\text{round}[\cdot]$ represent the DCT operation and the rounding operation, respectively. Similarly, the JPEG decompression procedure operates on images blockwise, which is as follows:

$$U' = \text{round}[I\ DC\ T(D \cdot Q)], \tag{2}$$

where $\text{IDCT}(\cdot)$ denotes the inverse DCT operation.

Because of the nonlinearity of the rounding operation, for a given JPEG image, it is hardly able to restore the original one accurately after JPEG encoding and decoding procedure eventhough the quantization tables are the same. As a result, secret messages extracted from the JPEG stego images are possibly damaged after the basic JPEG recompression process as a result of the change of DCT coefficients [22, 23], not to mention the practical transcode channel in the real world.

2.3. Sharing-Based Public Channel for Steganography. In [24], Simmons proposed the prisoner-warden model, which defines a typical scenario of steganography, where steganographic schemes are expected to design for minimizing the perturbation of modification. This class of steganographic schemes mainly focuses on statistical security but ignore the insecurity of communication behavior.

To cover the deficiency of the classic steganographic model, Zhao et al. [12] proposed a sharing-based steganography model. As shown in Figure 2, the stego file is uploaded to the public platform by Alice which can be downloaded by all parties including Bob. In this scenario, the relationship of communication is established between Alice and Bob through the public channels, which is weakened, since the method of communication is one-to-many instead of point-to-point. As a result, both statistical and behavioral security performance is considered in the steganography communication.

However, the public channels will generally recompress the uploaded files to uniform the format and save the storage space, while the steganographic signal will be disturbed. As for the media of image, since the public channels, such as SNPs, typically utilize the fixed quantization table to transcode the uploaded files, the cover images can be recompressed with the same quantization table to minimize the disturbance of transcoding. Therefore, the sharing-based model of steganography is degraded to the problem of reliable steganography communication under the recompression channel with the same quantization table.

2.4. Optimal Steganographic Embedding. In the payload-limited sender (PLS) problem, steganographic schemes try to embed message $\mathbf{m}$ with calculated costs ρ into cover image $\mathbf{X}$ to generate stego image $\mathbf{Y}$ by solving the following optimization problem:

$$\min_\pi E_\pi[D] = \sum_{i=1}^{n} \sum_{s_i \in \mathcal{S}_i} \pi_i(s_i)\rho_i(s_i), \tag{3}$$

$$\text{Subjected to } H(\pi) = -\sum_{i=1}^{n} \sum_{s_i \in \mathcal{S}_i} \pi_i(s_i)\log_2 \pi_i(s_i) = |m|, \tag{4}$$

where s_i denote the modification patterns for pixel in i location and $\rho_i(s_i)$ denote the cost with modification pattern s_i for i^{th} cover element. D represents the sum of the costs with certain modification pattern $s = (s_1, s_2, \ldots, s_n)$ for cover image, that is,

$$D(s) = \sum_{i=1}^{n} \rho_i(s_i), \tag{5}$$

where $\pi_i(s_i)$ denotes the probability of modifying the i^{th} cover element. While solving the optimization problem shown in equation (3) with Lagrangian multiplier [25], the optimal probability of modification for each element is obtained:

$$\pi_i(s_i) = \frac{\exp[-\lambda\rho_i(s_i)]}{\sum_{s_i' \in \mathcal{S}_i} \exp[-\lambda\rho_i(s_i')]}, \tag{6}$$

where $\lambda > 0$ is a scalar parameter determined by equation (4). The optimal probability above is the best mapping from the modification probability to the cost and has been proven to have a Gibbs distribution [26].

2.5. The Sources of Extraction Errors in Recompression Channels Transmission. To further improve the robustness of adaptive steganography, lots of previous works have

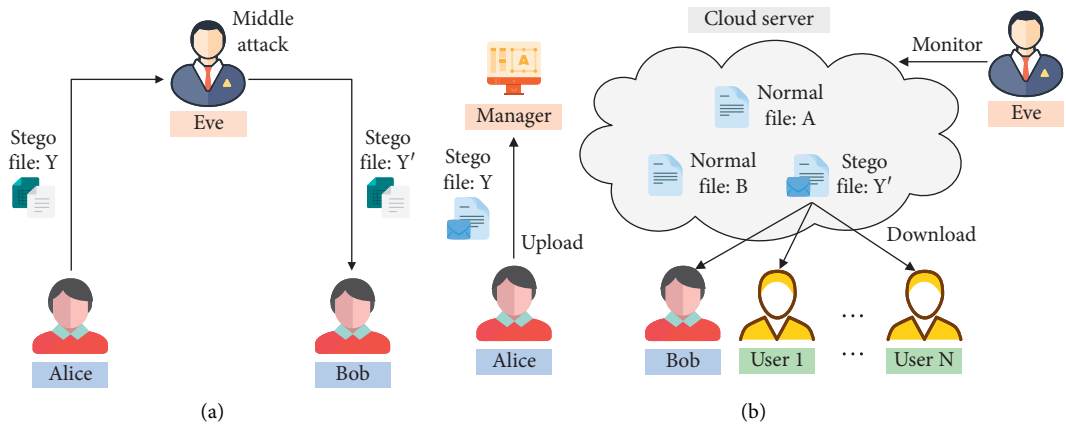

Figure 2: The basic model of steganographic communication scenario where Alice tries to communicate covertly with bob. (a) The prisoner-warden model, where a point-to-point communication is established between Alice and Bob. The stego files Y and Y' may be different which depend on whether active or passive mode of attack is used by Eve. (b) Illustration of the sharing-based model, in which the communication relationship between Alice and Bob is hiding.

analyzed the sources of message extraction errors. In [27], Bao et al. proposed an error model that mathematically analyzes the error diffusion phenomenon of STCs. The approximate bit error probability of extracted message deduced in [27] implies that the larger values of h and w take the higher error probability of extracted message. In other words, the increase of submatrix height h and the decrease of relative payload α reduce the correct rate of message extraction in steganography since the width of submatrix can be calculated as $w = \lfloor 1/\alpha \rfloor$ in STCs.

Furthermore, when a JPEG format stego image is transmitted in the recompression channel, bit errors will be generated in the extracted message for the changes of DCT coefficients. In modern JPEG steganography, the rate of modification is typically lower than the rate of embedding, i.e., relative payload, as a result of the matrix coding. Table 1 provides the statistical results of the number of modified coefficients per block using STCs with J-UNIWARD, where 4096000 samples of the DCT block partitioned from JPEG images of the ALASKA-JSMALL dataset (ALASKA-JSMALL dataset is obtained from RAW format images of the ALASKA database [28]. After center-cropped and rescaled to the size of 512×512, the format of which is converted to JPEG with different quality factors.) are adopted. The average and standard deviation of modification number, denoted as μ and σ, respectively, represent that no more than 2 coefficients per block are modified by the adaptive steganographic scheme on average when the quality factor is lower than 85.

Table 1: The number of modified coefficients under different relative payloads and quality factors using STCs with J-UNIWARD.

	0.2 bpnzAC		0.4 bpnzAC	
	μ	σ	μ	σ
QF = 75	0.359 7	1.003 8	0.793 8	1.688 3
QF = 80	0.422 4	1.098 4	0.932 9	1.854 3
QF = 85	0.511 3	1.238 5	1.126 2	2.088 8

3. Measurement Model of Robustness

3.1. Change Properties of DCT Block after Recompression. As discussed in Section 2.2, images are partitioned into blocks of 8×8 pixels in the lossy procedure of JPEG compression. As a result, the DCT block is selected as the basic unit of research on the change properties of JPEG image coefficients after recompression.

To investigate the change properties of the JPEG recompressed DCT block, simulated ±1 modifications are directly operated on randomly selected coefficients in each DCT block. The simulation is performed on 409600 samples of 3-channel DCT block generated from the ALASKA-JSMALL dataset with quality factor of 75, 80, and 85. The recompression channel is established with MozJPEG (MozJPEG is a patch for libJPEG-turbo that improves JPEG compression efficiency achieving higher visual quality and smaller file sizes at the same time. MozJPEG can be explored on https://github.com/mozilla/mozjpeg) which is widely used by SNPs in the real world. The number of modified coefficients is in the range of 1–9 according to results in Section 2.5 and the theorem of large numbers. To obtain more complete statistical results, operations on each block are repeatedly conducted for 30 times. As shown in Figure 3, the average percentage of changed coefficients per block after recompression, denoted as p_c, and is monotonically increasing with the number of modified coefficients per block n_m.

Furthermore, the average and standard derivation of p_c overall n_m from Figure 3 are calculated and given in Table 2, which implies that p_c remains almost constant as n_m increases since the standard derivation of p_c is less than 0.05%. As a result, the average percentage of changed coefficients after JPEG recompression can approximately represent the change properties of the DCT block.

3.2. The Model of Robustness Measurement. Since the JPEG compression procedure is nonlinear, the mathematical model of the recompression process in the analytical form

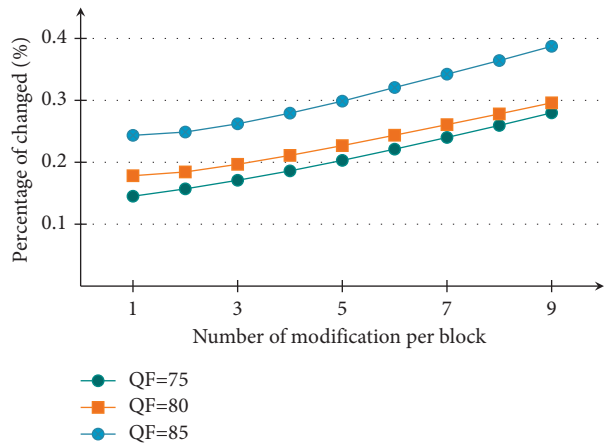

Figure 3: The average number of the changed coefficients after JPEG recompression over DCT blocks of 100 JPEG images sized 512 × 512 under different numbers of modification on each block.

Table 2: The average and standard deviation of the percentage of changed coefficients over different rates of modification that demonstrated in Figure 3.

	QF = 75	QF = 80	QF = 85
Average (%)	0.207 0	0.230 6	0.305 2
Std. dev. (%)	0.046 7	0.041 9	0.051 7

can be highly sophisticated. In other words, the heuristic designed features can hardly represent the change properties of the DCT block before and after the JPEG recompression. Nevertheless, deep learning-based methods have achieved start-of-the-art performance in many fields, especially those related to image and video processing. For image compression, lots of works have been proposed [29–31] with the structure of autoencoders that performed better than classic schemes, which indicates that it is operable to design a deep learning-based model to extract features of JPEG recompression channel.

Since the transcoding procedure between DCT and spatial coefficients is nonlinear, the robustness measurement model is designed to fit the coefficient change rate with generality and nonlinearity. Therefore, the coefficients of both DCT and spatial domain are inputted with two separate branches, and nonlinear activation functions are introduced in the model. Figure 4 shows the structure of the proposed model. The first branch, named D-branch, is designed for extracting the change features of DCT coefficients d_i in zigzag order, while the S-branch aims at catching information of the block in spatial domain, which is denoted as s_i. The features extracted by two branches are concatenated and activated by the TanH function for limiting the range of output before fed into the last pipeline. Batch normalization are utilized, and the activation function ReLU and leaky ReLU are introduced to improve the nonlinearity of the model. Dropout layers are also used after activation layers to overcome overfitting.

As the figure shows, η_i is one of the outputs that represents the average percentage of the changed coefficient in the DCT block after JPEG recompression, while ξ_i denotes the percentage of the change in block without any modification. It is worth mentioning that no activation function is adopted at the end of the output layers because the proposed model is designed for solving the regression problem.

In the training stage, 409600 samples in total are generated from the ALASKA-JSMALL dataset. Images are partitioned into blocks and of which the coefficients are randomly modified with different rates of modification for 30 times. Considering both the rate of modification and the accuracy of the generated samples, the numbers of modified coefficients in the experiment are all integers and range from 1 to 9.

In terms of the hyperparameters, the dropout rates are set to 0.25 in both feature extraction branches while 0.4 in other dropout layers. The negative slope of each leaky ReLU layer is set to 0.2. Adam optimizer is used with learning rate 0.000 1, and mini-batch gradient descent strategy is adopted with size 64. The loss function, which is defined as $l = \alpha \cdot l_\eta + \beta \cdot l_\xi$, is used for network optimization, where l_η and l_ξ are the loss of outputs η_i and ξ_i, respectively. Considering the properties of the DCT block both with and without recompression, α and β are all set to 0.5. MSE (mean square error) function is also used for fitting both η_i and ξ_i. The proposed model is trained for 100 epochs. All the training procedures are conducted on NVIDIA Tesla P100 GPU with 12 GB graphics memory.

3.3. Performance of the Robustness Measurement Model. Figure 5 shows the loss of training and validating stage, where the model converges rapidly at around 5th epoch. The loss of the model decreases with training and stabilizes at a small value. Therefore, the proposed model can efficiently estimate the robustness of the DCT block and provide high accuracy performance in quantitative analysis of robustness.

4. Proposed Framework

The proposed robust JPEG adaptive steganographic framework is shown in Figure 6. In the framework, we first use the robustness measurement model to estimate the

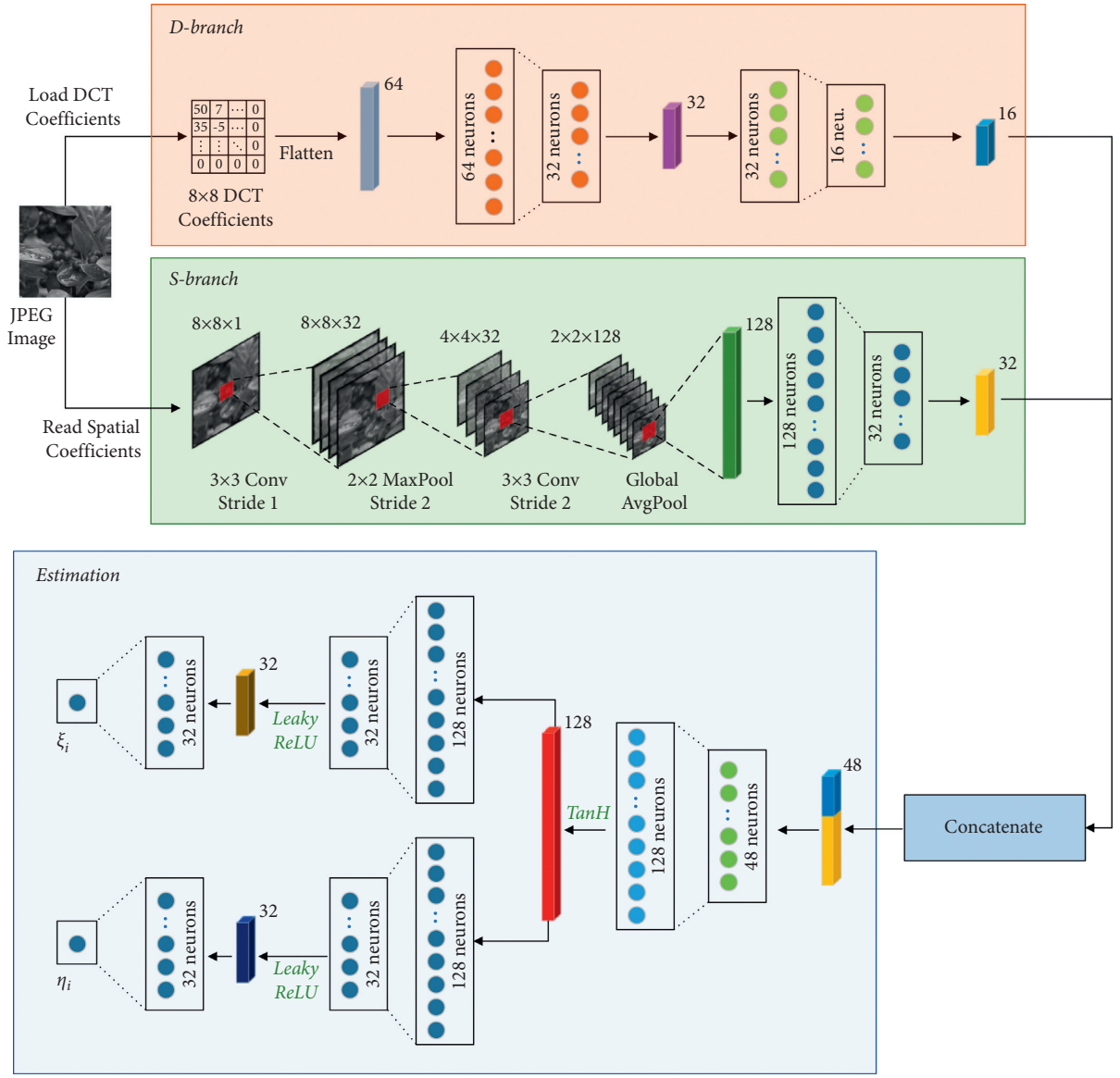

Figure 4: Structure of the proposed robustness measurement model. The parameter of convolutional layers and fully connected layers are labeled on each block. "TanH" and "Leaky ReLU" represent the activation function Tanh and leaky ReLU. Generally, ReLU activation functions are not labeled.

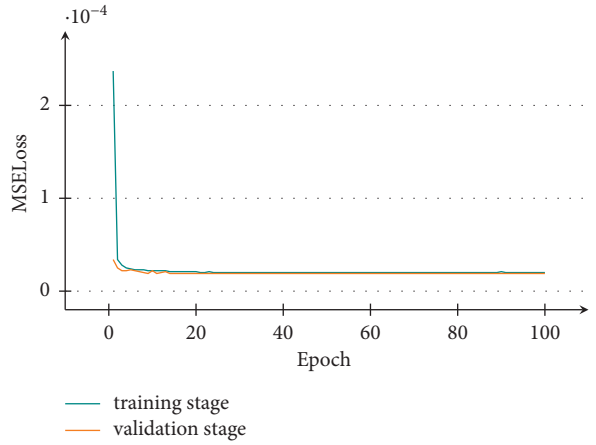

Figure 5: The average mean square error loss of the model in training and validating stage. The JPEG samples with quality factor of 85 are trained for 100 epochs.

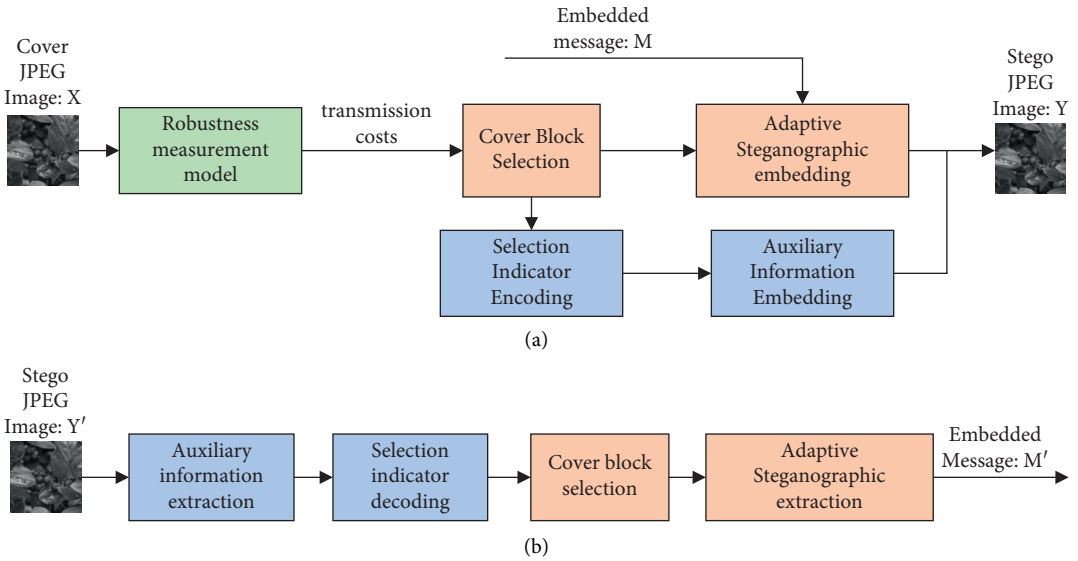

Figure 6: The proposed robust steganographic framework. (a) The embedding procedure. (b) The extraction procedure.

coefficient change rate of each DCT block after recompression. Then, DCT blocks with the available cover elements are selected by selection strategy. The messages are embedded by classic steganographic schemes, and the auxiliary information of selection is encoded with the coefficients in the chrominance channel. After receiving stego images from SNPs, the receiver can extract messages from reconstructed cover elements. We name our proposed framework cover block selection-based adaptive robust steganography (abbreviated to CBSRS). Each strategy will be explained in detail in the following subsections.

4.1. The Properties of Cover Selection. Defining the selection rate $\theta(0 < \theta < 1)$ as the ratio of selected block number to overall block number, the optimality of cover block selection is associated with the selection rate since the coding efficiency of STCs changes with the number of selected elements.

For the security performance of steganography after selection, the average classic distortion of steganographic embedding increases as the block selection is conducted. The smaller the selection rate, the greater the classic steganographic distortion. As a result, selecting the cover block according to the newly designed joint distortion function introduces navigate impact on security performance, and the optimal average classic distortion is unreachable for the element with top smallest costs cannot be selected.

Concerning the robustness performance, adaptive steganography with only transmission costs defined as

$$\rho_k^r(s_k) = \begin{cases} \eta_k, & s_k = 0, \\ \xi_k, & s_k = 1, \end{cases} \tag{7}$$

is discussed, where η_k and ξ_k are the predictions of the measurement model that, respectively, represent the robustness of the k^{th} block with and without modification after JPEG recompression, and $s_k \in \mathcal{J} = \{0, 1\}$ is the modification pattern of DCT block, where $s_i = 1$ denotes that the block is modified regardless of the number or the location of the modification, while $s_i = 0$ denotes that the block is not modified. In this scenario, given $|m|$ bits message sequence m and cover of b blocks $\mathbf{x} = (x_1, x_2, \cdots x_b)$, the blockwise transmission costs are calculated as $\rho^{\mathrm{r}} = (\rho_1^{\mathrm{r}}, \rho_2^{\mathrm{r}}, \ldots, \rho_b^{\mathrm{r}})$. The expectation of transmission costs is

$$E_p[D] = \sum_{i=1}^{b} \sum_{s_i \in \mathcal{J}} p_i^r(s_i)\rho_i^r(s_i), \tag{8}$$

where $\mathcal{J} = \{0, 1\}$. Referring to the optimal embedding theory in Section 2.4, the expectation of distortion has a minimal value only when the probability of modification on each block ρ^{r} follows Gibbs distribution. Assuming the number of embedded message bits is the same in each DCT block, the optimal probability of embedding satisfies

$$p_i^r(s_i) = \frac{\exp[-\lambda\rho_i^r(s_i)]}{\sum_{s_i' \in \mathcal{J}} \exp[-\lambda\rho_i^r(s_i')]}, \tag{9}$$

$$|m| = -b \cdot \sum_{i=1}^{b} \sum_{s_i \in \mathcal{J}} p_i^r(s_i)\log_2 p_i^r(s_i). \tag{10}$$

When the cover block selection is conducted with given selection rate θ, $b' = \mathrm{round}[\theta b]$ blocks are selected as $\mathbf{x}'$ with costs $\rho^{\mathrm{r}\prime} = (\rho_1^{\mathrm{r}'}, \rho_2^{\mathrm{r}'}, \ldots, \rho_{b'}^{\mathrm{r}'})$. To embed the same message $\mathbf{m}$ into selected cover blocks $\mathbf{x}'$, the optimal expectation of distortion is calculated by

$$E_{p'}[D'] = \sum_{i=1}^{b'} \sum_{s_i \in \mathcal{J}} p_i^{r'}(s_i)\rho_i^{r'}(s_i), \tag{11}$$

where the optimal probability of modification satisfies

$$p_i^{'r}(s_i) = \frac{\exp\left[-\lambda \rho_i^{'r}(s_i)\right]}{\sum_{s_i' \in \mathcal{J}} \exp\left[-\lambda \rho_i^{'r}(s_i')\right]}, \tag{12}$$

$$|m| = -b' \cdot \sum_{i=1}^{b'} \sum_{s_i \in \mathcal{J}} p_i^{'r}(s_i) \log_2 p_i^{'r}(s_i). \tag{13}$$

As the selection rate θ ranges from 0 to 1, number of cover blocks $b' < b$. To satisfy both constrains in equations (10) and (13), for each cover block in both $\mathbf{x}$ and $\mathbf{x}'$, since the optimal probability is a monotonic function of λ, we have

$$\sum_{s_i \in \mathcal{J}} p_i^r(s_i) \log_2 p_i^r(s_i) \geq \sum_{s_i \in \mathcal{J}} p_i^{'r}(s_i) \log_2 p_i^{'r}(s_i), \tag{14}$$

which denotes that the entropy of each selected block increases after selection. According to the piecewise monotonicity of the binary entropy function, the probability of $p_i^{'r}(0)$ and $p_i^{'r}(1)$ changes closer to 0.5 after selection. As $\rho_i^r(0) \equiv 0$, the expectation of embedding distortion $E_{\mathbf{p}'}[D']$ is smaller than $E_{\mathbf{p}}[D]$, which means that the cover block selection reduces the average distortion with optimal embedding.

4.2. Cover Block Selection Strategy. As discussed in Section 2.5, the error of message extraction in recompression channels is introduced from decoding procedure of STCs. As a result, the anticompression properties of the DCT block determine the correct rate of extracted messages regardless of whether the DCT block is modified or not. This inspires us that steganographic encoding can be adopted in the DCT block with higher robustness performance. In other words, selecting cover block before embedding improves robustness of steganography.

Since STCs are adopted, the candidate cover block can be also selected based on the cost of steganography. However, robustness and security performance are a pair of contradictions. To improve robustness through cover block selection while minimizing the security performance, in our framework, the measurement of robustness, regarded as transmission costs, is defined in equation (7) and used as the distortion of image lossy transmission that combined with the classic costs of steganography ρ^c.

According to the discussion above, the orders of magnitude between two types of distortion function is different. Thus, the combination of transmission costs and the classic costs is defined in the form of multiplication. The joint distortion for cover block selection of each block d^s is computed by

$$d^s = d^c \cdot d^r, \tag{15}$$

where d^c denotes the blockwise average of classic embedding distortion. In particular, let ρ_k^c represent all the classic distortion in the k^{th} DCT block. Before utilizing, ρ_k^c is updated by

$$\begin{cases} \beta \cdot \rho_k^c, & \text{if } \rho_k^r(0) < \rho_k^r(1), \\ \rho_k^c, & \text{otherwise}, \end{cases} \tag{16}$$

which demonstrates that steganographic embedding is encouraged if transmission cost under modification is smaller. Besides, d^r represents the expectation of transmission costs of each block, which is

$$d_k^r = p_k^r \rho_k^r(1) + (1 - p_k^r) \rho_k^r(0), \tag{17}$$

and p_k^r denotes the probability of modification of each block with the classic cost. Given the distortion of each coefficient in the j position of the k^{th} DCT block ρ_j^c, the optimal ± 1 modification probability p_j^c satisfies Gibbs distribution and is calculated by

$$p_j^c = \frac{\exp\left(-\lambda \rho_j^c\right)}{2\ \exp\left(-\lambda \rho_j^c\right) + 1}, \tag{18}$$

and p_k is calculated by

$$p_k^r = 1 - \prod_j \left(1 - p_j^c\right). \tag{19}$$

Based on the conclusion above, lower transmission cost and higher embedding cost are introduced by the cover block selection when the joint distortion function in equation (15) is used as the criteria. When the value of the selection rate θ is determined, θb blocks with the smallest joint distortion are selected as the cover element.

Meanwhile, for a given JPEG cover image, different robustness and security performance are acquired with different selection rate θ. To obtain the optimal trade-off between robustness and security in cover block selection, we introduce gain function for the decision of parameter θ.

Denote $\mathcal{B}_k = \{j \mid 1 \leq j \leq 8\}$ as the index set of the k^{th} DCT block as zig-zag order. The expectation of classic costs D^c and transmission costs D^r without cover block selection are calculated by

$$D^c = \sum_{k=1}^{b} \sum_{j \in \mathcal{B}_k} p_j^c \rho_j^c, D^r = \sum_{k=1}^{b} p_k^r \rho_k^r(1) + (1 - p_k^r) \rho_k^r(0), \tag{20}$$

which are defined as the standard expectation of distortion, where p_i^c is the optimal modification probability in equation (6) under the classic costs and p_k^r denotes the modification probability of the k^{th} block represented in equation (19). After block selection, b' blocks are selected as cover and the expectation of two costs are changed to

$$D^{c'}(\theta) = \sum_{k=1}^{b'} \sum_{j \in \mathcal{B}_k} p_j^{'c} \rho_j^c, D^{r'}(\theta) = \sum_{k=1}^{b'} p_k^{'r} \rho_k^r(1) + \left(1 - p_k^{'r}\right) \rho_k^r(0). \tag{21}$$

Based on the discussion above, the optimal expectation of classic costs increases while the average distortion defined by transmission costs decreases. As a result, the gain function is defined as

$$G(\theta) = \frac{D^{c\prime}(\theta) - D^{c}}{D^{c}} + \frac{D^{r\prime}(\theta) - D^{r}}{D^{r}}. \tag{22}$$

The optimal parameter θ_0 can be obtained by optimizing the gain function

$$\theta_0 = \underset{0<\theta<1}{\operatorname{argmin}} G(\theta), \tag{23}$$

$$\text{Subjected to } H(\theta_0) = -\sum_{k=1}^{b_0} \sum_{j \in \mathcal{B}_k} p_j^{\prime c} \log_2 p_j^{\prime c} = |m|, \tag{24}$$

where $b_0 = \text{round}(\theta_0 b)$ is the number of selected blocks.

In practice, to solving the optimization problem in equations (23) and (24), the optimal modification distribution of steganography $p_j^{\prime c}$ must be calculated first. However, the distribution $p_j^{\prime c}$ can be obtained only when the element of cover is specified, which means the problem cannot be directly optimized. In the proposed framework, $G(\theta)$ is numerically calculated, where $\theta \in \{0.2, 0.3, \ldots, 0.8\}$, and the suboptimal parameter can be obtained. The concrete method is described by Algorithm 1.

As for the value of update parameter β, few experiments are conducted on the BOSSBase dataset [32] for steganographic statistical security and robustness performance, which is shown in Figure 7. $\overline{P}_{\mathrm{E}}$ denotes the average detection error of the DCTR (discrete cosine transform residual) [8] extractor and $\overline{R}_{\mathrm{E}}$ represents the average error rate of message extraction. With the decrease of the value of β, the robustness performance improves while the statistical security declines markedly. To improve the robustness within the acceptable range of security performance, $\beta = 0.7$ is determined in our work.

4.3. Construction of Shareable Cover. For the sender of adaptive steganography, cover block selection improves the robustness performance. However, the auxiliary information about the selected block is nonshared with the receiver. To complete the steganographic channel, the shareable cover between the sender and receiver needs to be constructed. Classic JPEG steganography mainly focuses on the luminance channel while keeping the chrominance unmodified. Actually, DCT coefficients in the chrominance channel also have the capacity to carry messages. Therefore, the auxiliary information can be encoded into the chrominance channel.

In this study, JPEG images without chrominance channel subsampling are discussed. The sign of DCT coefficient is utilized as the embedding domain and the STCs are adopted to minimize the impact of auxiliary information encoding. As the experiment conducted in [19] shows, the coefficients in the higher frequency domain perform more stable after recompression while providing less security after modification. Besides, the DCT coefficients may shrinks towards 0 during JPEG recompression [33]. Since the relative payload of auxiliary information is low, the 5 AC coefficients at the lowest frequency are used for embedding.

Redefining $\mathcal{B}_k = \{i, j | 1 \le i, j \le 8\}$ as the index of rows and columns of coefficients in separate DCT blocks, in the proposed strategy, the cover element $x_{i,j}^k$ can be formulated by

$$x_{i,j}^k = \begin{cases} 1, & \text{if } c_{i,j}^k > 0, \\ 0, & \text{if } c_{i,j}^k < 0, \\ i \bmod 2, & \text{if } c_{i,j}^k = 0, \end{cases} \tag{25}$$

where $c_{i,j}^k$ denotes the DCT coefficient of (i, j) position in k^{th} block. The modification distance is defined as

$$h_{i,j}^k = \begin{cases} q_0 - c_{i,j}^k, & \text{if } c_{i,j}^k > 0 \\ -q_0 - c_{i,j}^k, & \text{if } c_{i,j}^k < 0 \\ \infty, & \text{if } c_{i,j}^k = 0 \end{cases} \tag{26}$$

The unit cost of each coefficient $\rho_{i,j}^k$ is calculated by the distortion function of J-UNIWARD, and the embedding cost $\zeta_{i,j}^k$ is calculated by

$$\zeta_{i,j}^k = \left| h_{i,j}^k \right| \cdot \rho_{i,j}^k. \tag{27}$$

where the multiplication is operated elementwise. These denote that cover element flipping will change the coefficient to the magnitude of q_0 with opposite sign and the zero valued coefficients will remain unchanged.

Besides, to ensure the integrity of auxiliary information, RS codes are adopted with bit-interleaved coding instead of random shuffle, which further improves the integrity of auxiliary information. The performance of cover reconstruction accuracy is discussed in Section 5.4.

5. Experiments

5.1. Experimental Setups. The experiments for performance analysis are all conducted on images in JPEG format center-cropped and resized to the size of 512×512, which are converted from the RAW format BOSSBase [32] dataset. Adaptive steganographic schemes are utilized in the proposed framework. The ternary multilayered version of STCs is used with the parameter h fixed of 3 for the best performance of robustness. Baseline algorithms JCRISBE [21] and GMAS [19] are selected as well as classic steganographic schemes J-UNIWARD [4] to compare with the proposed CBSRS framework, since JCRISBE and GMAS are the representative algorithms of the dedicated robustness and general robustness, respectively. Besides, the samples with quality factor of 75, 80, and 85 are evaluated for the SNPs will not transcode images with low quality. All the JPEG recompression procedures in the experiments are implemented with MozJPEG, and all samples are in color.

To evaluate the security performance, the ensemble classifier [34] is trained to discriminate the cover and stego samples. High-dimensional features are extracted from the samples and randomly divided into two groups. Half of the features are input into the classifier for training, while the others are used for testing. The performance of steganalysis is evaluated by the detection error of the classifier, which is defined as

Input: JPEG cover image **X**, elementwise classic cost ρ^c, blockwise transmission cost ρ^r
Output: cover selection indicator **K**

For each DCT block $\mathbf{B}_k$ in **X** do
  for $j = 1$ **to** 64 **do** // elementwise
    $p_j^c \leftarrow [\exp(\lambda\rho_j^c)]/[2\exp(\lambda\rho_j^c) + 1]$
  end
  $p_k^c \leftarrow 1 - \prod_{j=1}^{64}(1 - p_j^c)$ // blockwise
  $d_k^c \leftarrow 1/64\sum_{j=1}^{64}\rho_j^c$
  if $\rho_k^r(0) < \rho_k^r(1)$ **then** // update
    $d_k^c = 0.7 \cdot d_k^c$
  end
  $d_k^r \leftarrow p_k^r\rho_k^r(1) + (1 - p_k^r)\rho_k^r(0)$
  $d_k^s \leftarrow d_k^c \cdot d_k^r$ // joint cost
end
$D^c \leftarrow (\rho^c, \rho^c, l)$ expection_cost
$D^r \leftarrow (\rho^r, \rho^c, l)$ expection_cost_r
for each θ in $\{0.2, 0.3, \ldots, 0.8\}$ **do**
  $D^{c\prime} \leftarrow (\rho^c, \rho^c, \theta)$ expection_cost_c
  $D^{r\prime} \leftarrow (\rho^r, \rho^c, \theta)$ expection_cost_r
  // calculate gain function
  $G(\theta) \leftarrow [D^{c\prime}(\theta) - D^c]/D^c + [D^{r\prime}(\theta) - D^r]/D^r$
end
$\theta_0 \leftarrow \mathrm{argmin}_\theta G(\theta)$ // suboptimal
$K \leftarrow$ block_selection (threshold(X, θ_0))

Algorithm 1: Cover block selection algorithm.

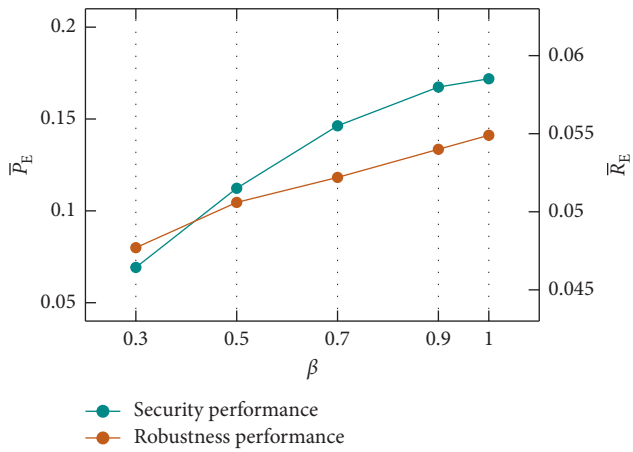

Figure 7: Security and robustness performance of CBSRS with different values of parameter β.

$$P_E = \frac{1}{2}(P_{FA} + P_{MD}), \tag{28}$$

where P_{FA} and P_{MD} are the probability of false alarm and missed detection rate, respectively. Practically, the evaluation is conducted 10 times, and the average output of multiple tests, denoted as $\overline{P}_E$, is adopted as the final result. In the experiments, the DCTR and PHARM (PHase Aware pRojection Model) [7] feature extractor are utilized.

Furthermore, the error rate of the extracted secret message is calculated by

$$R_E = \frac{n_E}{|m|}, \tag{29}$$

where **m** represents the original embedded secret message and $|m|$ is the length of bit of **m**, and n_E represents the number of bit error of extracted secret message. Note that the payload mentioned in the experiments denotes the original embedding rate calculated by the length of not encoded secret message.

5.2. Robustness Performance of the Proposed Framework. To demonstrate the effectiveness of cover block selection strategy, the robustness is evaluated by the bit error of message extraction defined by equation (29). All the sample images from BOSSBase 1.01 are utilized, which are converted to JPEG format with the size of 512×512.

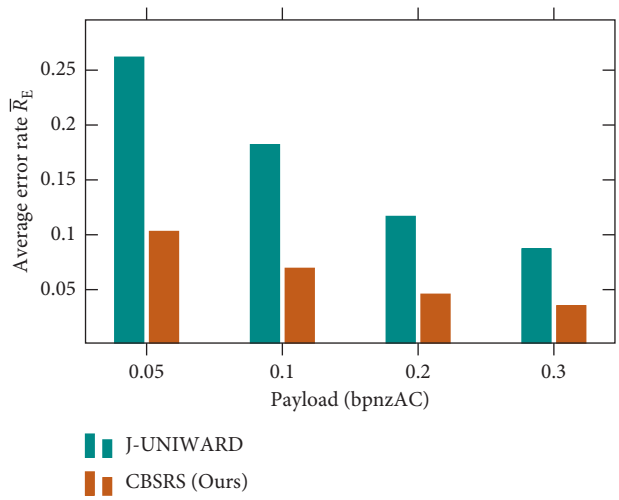

Figure 8: Average extraction error rate of the classic J-UNIWARD algorithm and the proposed CBSRS framework over 10,000 cover images of quality factor of 85.

Chrominance subsampling is disabled during the cover image conversion process. Stego samples are generated with payloads of 0.05, 0.1, 0.2, and 0.3 bpnzAC for comprehensive evaluation.

As Figure 8 shows, no matter under any relative payload, the proposed CBSRS framework significantly improves the robustness under the lossy channel constructed by MozJPEG. And the compare result shows that the classic steganographic schemes are not capable of covert communication under JPEG recompression channel.

To further illustrate the effectiveness of the proposed CBSRS framework, the state-of-the-art robust steganographic schemes JCRISBE and GMAS are compared. The function imread and imwrite from MATLAB are utilized in the transport channel matching procedure of JCRISBE. Note that RS codes or BCH codes are adopted in JCRISBE and GMAS, but no ECCs are used in CBSRS framework. Table 3 provides the result of extraction error rate of different steganographic schemes. Compared with the classic scheme, the robustness performance of these robust steganographic schemes is improved to varying degrees. While, GMAS outperforms other algorithms in the class of dedicated robustness as watermarking modulation mode is adopted.

As for dedicated robustness, the extraction error rate of JCRISBE is higher than which of the CBSRS framework especially when at the lower relative payload, which denotes that the robustness performance will decrease when the channel is not completely matched in JCRISBE. However, CBSRS is designed by mastering the recompression properties of aimed lossy channel. For robustness, the proposed CBSRS framework performs better than the baseline algorithm of the class of dedicated robustness.

5.3. Security Performance Comparison. In this experiment, security performance is evaluated by using the detection error defined in equations (10) and (28) and converted images in color JPEG format from BOSSBase are utilized. To compare the statistical security with the steganographic algorithms, only steganalytic features of luminance channel are extracted. Figures 9–11 show the security performance of the proposed CBSRS and compared schemes. The statistical result of J-UNIWARD is also presented as the baseline of steganalytic security.

Since the amplitude of modification is large, the steganographic security of the GMAS scheme is quite unsatisfactory when comparing with other dedicated robustness schemes. However, both JCRISBE and CBSRS basically maintain the statistical security while providing robustness of steganography. However, the proposed CBSRS framework surpasses the state-of-the-art robust steganographic scheme for statistical security since the ECCs are adopted in JCRISBE. The experimental results demonstrate that the model of proposed robustness measurement is effective, and the strategy of cover block selection is capable of optimizing the trade-off between the robustness and the security of steganography.

Besides, the position distribution of modification of each steganographic scheme is investigated. As shown in Figure 12, the modification position of the proposed CBSRS scheme is more concentrated than which of other schemes. Therefore, the affected area of steganographic noise in the image is smaller which contributes to the high statistical security.

5.4. Accuracy of Cover Reconstruction. The experimental results of both the reconstruct successful rate and the bit error rate of auxiliary information are given in Table 4. The successful reconstruct rate is considerable especially at the higher quality factor of channel. This is because the lower quantization step provides higher accuracy of sign-based stego element. Besides, the average information error rate maintains low and increases with relative payload, which denotes that steganographic embedding in the luminance channel of JPEG affects the robustness of element in the chrominance channel. As a result, the coefficient sign-based cover reconstruction strategy is effective in recompression channel.

Table 3: The bit error rate of message extraction with different steganographic schemes under different actual payloads.

Method		Payload (bpnzAC)			
		0.05	0.1	0.2	0.3
J-UNIWARD [4]	QF = 75	0.215 0	0.148 1	0.094 2	0.070 5
	QF = 80	0.255 8	0.180 2	0.116 7	0.087 8
	QF = 85	0.261 8	0.182 1	0.116 7	0.087 1
JSCRIBE [21]	QF = 75	0.166 7	0.108 1	0.063 4	0.043 4
	QF = 80	0.166 3	0.105 6	0.060 9	0.041 0
	QF = 85	0.181 6	0.115 3	0.066 5	0.044 6
GMAS [19]	QF = 75	0.084 1	0.041 7	0.020 9	0.004 5
	QF = 80	0.079 5	0.039 9	0.020 6	0.003 9
	QF = 85	0.074 8	0.039 1	0.018 5	0.003 4
CBSRS (ours)	QF = 75	0.111 6	0.078 8	0.052 5	0.041 1
	QF = 80	0.110 4	0.072 5	0.046 9	0.035 9
	QF = 85	0.103 0	0.069 4	0.045 8	0.035 3

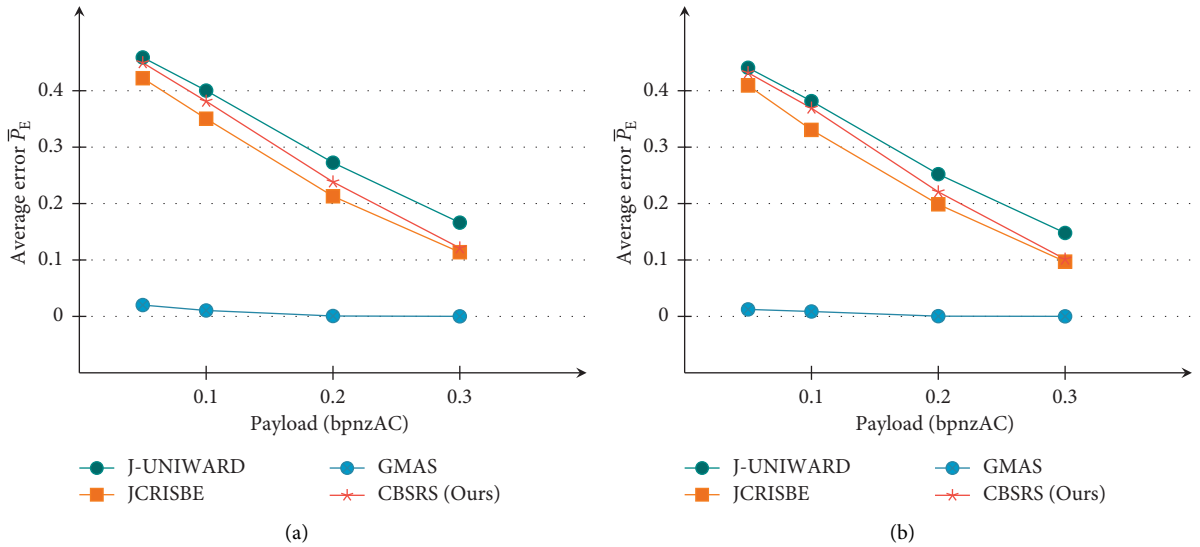

Figure 9: The detection error of the steganalysis detector under different steganographic algorithms with quality factor of 75. (a) Security performance with DCTR features. (b) Security performance with PHARM features.

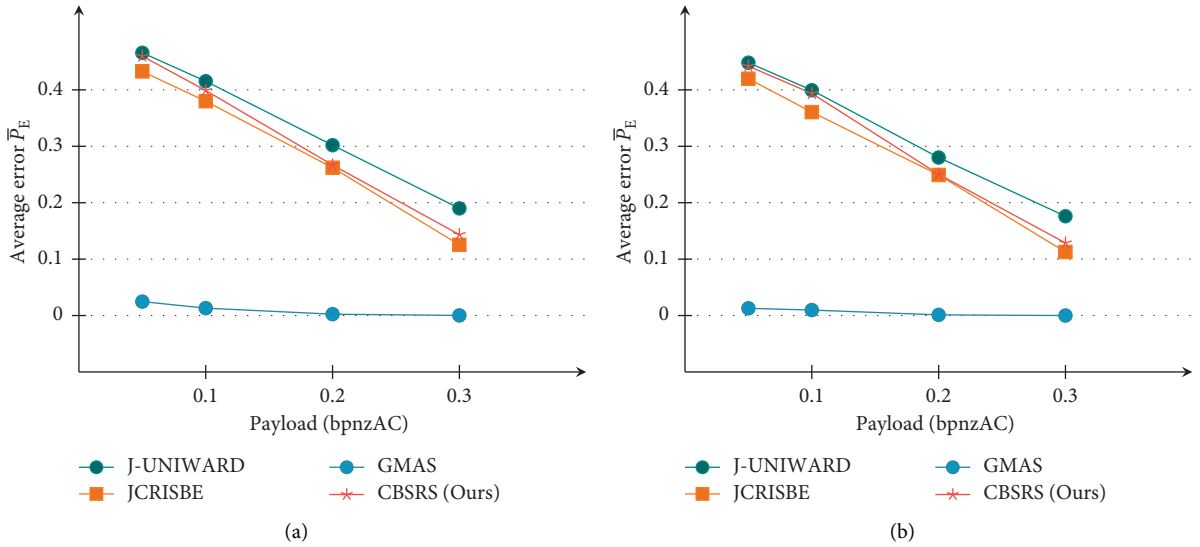

Figure 10: The detection error of the steganalysis detector under different steganographic algorithms with quality factor of 80. (a) Security performance with DCTR features. (b) Security performance with PHARM features.

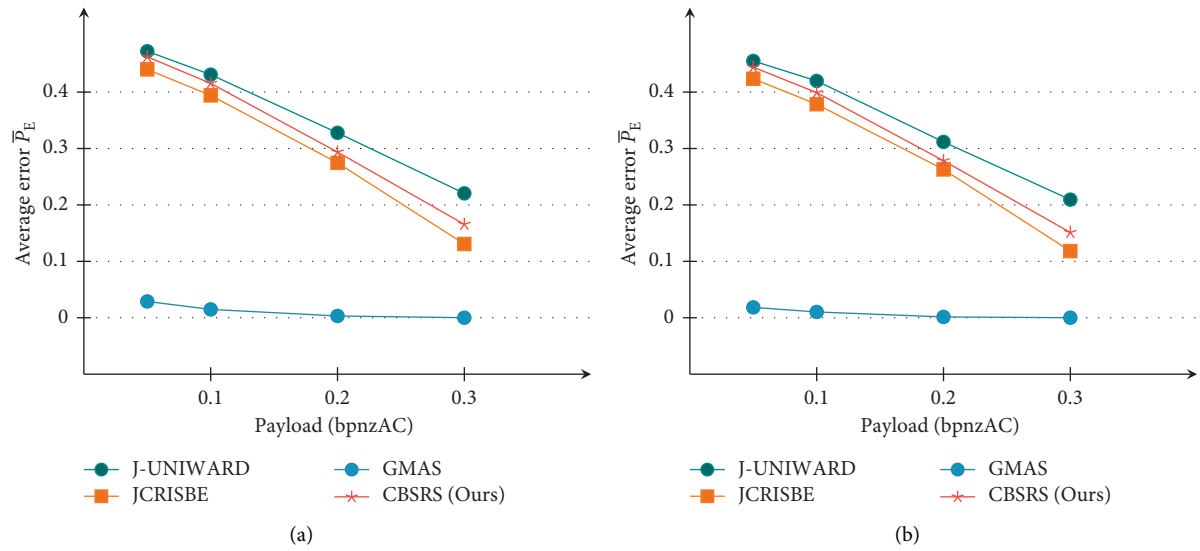

Figure 11: The detection error of the steganalysis detector under different steganographic algorithms with quality factor of 85. (a) Security performance with DCTR features. (b) Security performance with PHARM features.

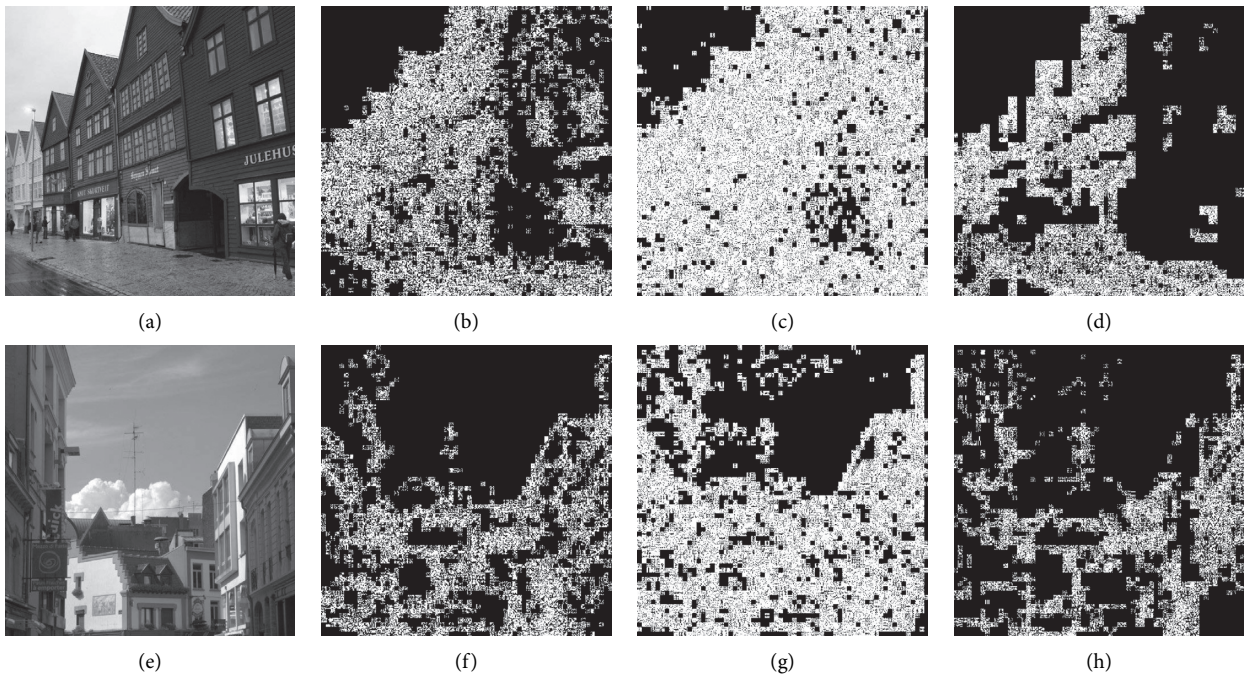

Figure 12: Two cover examples, i.e., (a) No. 10 and (e) No. 6222 in BOSSBase and the corresponding modification position in spatial domain generated by J-UNIWARD, i.e., (b) and (f), GMAS, i.e., (c) and (g), and CBSRS, i.e., (d) and (h) for relative payload 0.3 bpnzAC with quality factor of 85 and STCs, respectively. In this subsection, the accuracy of the cover reconstruction is evaluated. For the cover images size 512×512, 4096 bit indicators are required to reconstruct the location of the cover element. To decrease the size of auxiliary information and increase the accuracy of the cover reconstruction, the indicators of each block are quantized in each 2×2 units for the robustness distribution in natural images continuous with the image content. Meanwhile, (31, 15) RS codes are adopted with bit-interleaved coding to further reduce the extraction error rate. Thus, 2,170 bit auxiliary information is encoded with the chrominance channel of each cover image in the experiment.

Table 4: The experimental results of cover reconstruction accuracy.

Payload (bpnzAC)	Successful decode rate			Information error rate		
	QF = 75	QF = 80	QF = 85	QF = 75	QF = 80	QF = 85
0.05	0.8480	0.9174	0.9596	0.0768	0.0407	0.0181
0.1	0.8435	0.9152	0.9581	0.0831	0.0444	0.0222
0.2	0.8461	0.9164	0.9581	0.0905	0.0482	0.0231
0.3	0.8430	0.9158	0.9586	0.0967	0.0512	0.0244

6. Conclusion and Future Works

In this study, we propose a robust steganographic framework with the strategy of cover block selection, which are capable of resisting JPEG recompression while maintaining high steganographic security. Besides, a deep learning-based model for robustness measurement of DCT block is designed, and a joint distortion function of cover block selection is defined. The comparison results show that our proposed framework highly decreases the bit error rate under the lossy channel with the same quantization table while maintaining statistical security by mastering the properties of the lossy channel, and the CBSRS framework outperforms the state-of-the-art steganographic schemes in a specific lossy channel. Furthermore, a synchronous transmission strategy of block selection auxiliary information is investigated to construct shareable cover with sender and receiver, which builds up the first framework of auxiliary information-based robust steganography for JPEG images.

In the future, the model of robustness measurement will be updated, and the proposed robust steganographic framework will be expanded to the lossy channel with different quantization tables. In addition, we will design a suitable error correction scheme to further improve the robustness of adaptive steganography.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the NSFC (61972390, U1736214, 61872356, and 61902391) and National Key Technology Research and Development Program (2019QY0701).

References

[1] J. Fridrich, *Steganography in Digital media: Principles, Algorithms, and Applications*, Cambridge University Press, Cambridge, United Kingdom, 2009.

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

[3] W. Li, W. Zhang, L. Li, H. Zhou, and N. Yu, "Designing near-optimal steganographic codes in practice based on polar codes," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 3948–3962, 2020.

[4] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 2014, no. 1, p. 1, 2014.

[5] L. Linjie Guo, J. Jiangqun Ni, and Y. Q. Yun Qing Shi, "Uniform embedding for efficient jpeg steganography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 814–825, 2014.

[6] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using statistical image model for jpeg steganography: uniform embedding revisited," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2669–2680, 2015.

[7] V. Holub and J. Fridrich, "Phase-aware projection model for steganalysis of jpeg images," in *Proceedings of the Media Watermarking, Security, and Forensics 2015, Vol. 9409*, March 2015, Article ID 94090T.

[8] 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, 2014.

[9] G. Xu, H.-Z. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Processing Letters*, vol. 23, no. 5, pp. 708–712, 2016.

[10] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-net: an efficient cnn for spatial steganalysis," in *Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2092–2096, IEEE, Calgary, AB, Canada, April 2018.

[11] 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, 2018.

[12] X. Zhao, C. Yang, and F. Liu, "On the sharing-based model of steganography," in *Proceedings of the International Workshop on Digital Watermarking*, pp. 94–105, Springer, Melbourne, VIC, Australia, November 2020.

[13] S. K. Ernala, M. Burke, A. Leavitt, and N. B. Ellison, "How well do people report time spent on facebook? an evaluation of established survey questions with recommendations," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–14, New York, NY, United States, April 2020.

[14] S. Loeb, T. Carrick, C. Frey, and T. Titus, "Increasing social media use in urology: 2017 american urological association survey," *European urology focus*, vol. 6, no. 3, pp. 605–608, 2020.

[15] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards robust image steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 594–600, 2018.

[16] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A jpeg-compression resistant adaptive steganography based on relative relationship between dct coefficients," in *Proceedings of*

the 2015 10th International Conference on Availability, Reliability and Security, pp. 461–466, IEEE, Toulouse, France, August 2015.

[17] 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 and Applications*, vol. 76, no. 3, pp. 3649–3668, 2017.

[18] Y. Zhang, X. Zhu, C. Qin, C. Yang, and X. Luo, "Dither modulation based adaptive steganography resisting jpeg compression and statistic detection," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 17913–17935, 2018.

[19] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, and N. Yu, "Robust adaptive steganography based on generalized dither modulation and expanded embedding domain," *Signal Processing*, vol. 168, Article ID 107343, 2020.

[20] Z. Zhu, N. Zheng, T. Qiao, and M. Xu, "Robust steganography by modifying sign of dct coefficients," *IEEE Access*, vol. 7, pp. 168613–168628, 2019.

[21] Z. Zhao, Q. Guan, H. Zhang, and X. Zhao, "Improving the robustness of adaptive steganographic algorithms based on transport channel matching," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1843–1856, 2018.

[22] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y.-Q. Shi, "An effective method for detecting double jpeg compression with the same quantization matrix," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1933–1942, 2014.

[23] T. H. Thai and R. Cogranne, "Estimation of primary quantization steps in double-compressed jpeg images using a statistical model of discrete cosine transform," *IEEE Access*, vol. 7, pp. 76203–76216, 2019.

[24] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology*, pp. 51–67, Springer, Heidelberg, Germany, 1984.

[25] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents IX, Vol. 6505*, February 2007, Article ID 650502.

[26] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 705–720, 2010.

[27] Z. Bao, X. Luo, Y. Zhang, C. Yang, and F. Liu, "A robust image steganography on resisting jpeg compression with no side information," *IETE Technical Review*, vol. 35, no. sup1, pp. 4–13, 2018.

[28] R. Cogranne, Q. Giboulot, and P. Bas, "The Alaska steganalysis challenge: a first step towards steganalysis," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, pp. 125–137, New York, NY, USA, July 2019.

[29] O. Rippel and L. Bourdev, "Real-time adaptive image compression," in *Proceedings of the International Conference on Machine Learning*, pp. 2922–2930, Sydney NSW Australia, August 2017.

[30] M. Li, W. Zuo, S. Gu, D. Zhao, and D. Zhang, "Learning convolutional networks for content-weighted image compression," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 3214–3223, Salt Lake City, UT, USA, June 2018.

[31] F. Mentzer, E. Agustsson, M. Tschannen, R. Timofte, and L. Van Gool, "Conditional probability models for deep image compression," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4394–4402, Salt Lake City, UT, USA, June 2018.

[32] P. Bas, T. Filler, and T. Pevný, ""Break our steganographic system": the ins and outs of organizing BOSS," in *Proceedings of the International workshop on information hiding*, pp. 59–70, Springer, Prague, Czech Republic, May 2011.

[33] E. Y. Lam and J. W. Goodman, "A mathematical analysis of the dct coefficient distributions for images," *IEEE Transactions on Image Processing*, vol. 9, no. 10, pp. 1661–1666, 2000.

[34] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2011.