Hindawi
Security and Communication Networks
Volume 2022, Article ID 8230263, 13 pages
https://doi.org/10.1155/2022/8230263

Research Article

Novel Hidden Bit Location Method towards JPEG Steganography

Binmin Pan,[1] Tong Qiao ,[1,2] Jiaming Li,[1] Yiyang Chen,[1] and Chunfang Yang [2]

[1]*School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, Zhengzhou, Henan, China*

Correspondence should be addressed to Tong Qiao; tong.qiao@hdu.edu.cn

Received 25 January 2022; Revised 5 March 2022; Accepted 20 April 2022; Published 19 May 2022

Academic Editor: David Megias

Image steganalysis has been widely studied, most of which can only complete the binary task of identifying the existence of hidden bits in an inquiry image. Currently, although some algorithms have been proposed to locate hidden bits, most of them mainly focus on the spatial domain, while usually ignoring the study of locating secret bits hidden in DCT domain for JPEG image. To address that challengeable problem, in this paper, towards two classical steganographic algorithms JSteg and F5, hiding bits in DCT domain, we propose a novel payload location method. The principal step of payload location is to estimate the cover image. We novelly propose to assign the different weights to the DCT coefficient residual in virtue of the texture of regions measured by the local variance, leading to the remarkable improvement of location results. Compared with the state of the art, the numerical experiments empirically verify that our proposed location method achieves the superior performance. In particular, when locating hidden bits in JSteg steganographic images with quality factor of 95 at the payload 0.1, the accuracy of location is remarkably improved from 46.18% to 90.22%.

1. Introduction

Steganography is an emerging technology that conceals secret information to achieve the aim of covert communication. In contrast, steganalysis focuses on the detection of multimedia carriers containing secret information operated by steganography. In particular, image steganography is to embed hidden bits in an image carrier. Considering the undetectability, one usually makes tiny changes (± 1) to pixels in the spatial or frequency domain. Thus, image steganography in the spatial and frequency domains is, respectively, proposed. Accordingly, steganalysis can arbitrarily be classified into two categories: spatial steganalysis and frequency steganalysis (see details in [1]).

In the early stage, in the spatial domain, LSBR (least significant bit replacement) is usually considered as a classical steganographic algorithm. It enables the embedding by only flipping the pixels. Thereafter, LSBM (least significant bit matching) steganography is designed, which overcomes the histogram artifacts of LSBR through randomly adding or subtracting one to the cover pixels. In the frequency domain, JSteg inherits the idea of LSBR, extending to the DCT domain while excluding 0 and 1 coefficients from AC [2]. Afterwards, to further improve the undetectability and capacity, F5 serves as the updated version of DCT domain-based steganography [3]. In the modern image steganography, one of the most successful models rather treats the message embedding as a source coding problem with a fidelity constraint [4]. Specifically, one intends to minimize the distortion traces left by embedding and to construct the cost function that guides the embedding path to hide information in the texture region. Besides, relying on Industrial Internet of Things (IIoT) [5] and 3-D mesh [6], many novel steganography techniques have been proposed to enrich the study of this community. Recently, the study of RDH has also advanced [7, 8].

Many modern adaptive steganographic algorithms have been devised, such as HUGO [9], WOW [10], S-UNIWARD [4], and HILL [11] for spatial domain and J-UNIWARD [4], UED [12], UERD [13], and GMRF [14] for DCT domain. To resist against postprocessing attacks such JPEG compression, some robust methodologies are recently proposed

[15–19]. By contrast, mainly relying on hand-crafted feature extraction [20–23] or statistical models [24], image steganalysis is also well developed, classifying between cover and stego images. Meanwhile, with the advance of deep neural networks, the end-to-end automatic image steganalysis gradually dominates the detection field (see [25–32] for instance).

Traditionally, image steganalysis is primarily established to counter steganography, mainly completing the binary task. However, in general, we tend to extend the study of steganalysis onto four principal layers (from easy to hard mode) in the progressive relations:

(1) Determine if an inquiry image contains hidden bits.

(2) Estimate the payload of hidden bits.

(3) Locate the position of hidden bits.

(4) Extract and reconstruct hidden bits.

To our knowledge, most of steganographic algorithms focus on the first and second layer while ignoring the latter two layers of studies [33–41]. In practice, the ultimate goal of steganalysis is to reconstruct the hidden bits, namely, forensic steganalysis [42]. Although a few payload location methods have been proposed, most of them extract hidden bits in the spatial domain while only the work in [40] opens the new way of locating bits hidden in the frequency domain towards JPEG image steganography. Nevertheless, the accuracy of location in [40] needs to be improved.

In this context, to address that tough issue, we carry out further research on payload location in the frequency domain for JPEG image. For clarity and simplicity, it is proposed to estimate the cover DCT coefficients in each subband, where the impact of different DCT coefficients on the cover estimation is well investigated. Straightforward, we propose a cover estimation algorithm based on the idea of weight assignment, in order to address the problem of payload location. The main contributions of this paper are as follows:

(i) In order to improve the accurate estimate of low-texture region and to reduce the negative effects of high-texture region on payload location accuracy, the well-designed weights are assigned according to each factor's importance.

(ii) Based on the coefficients in the same subband, the cover estimate is established from spatial to DCT domain. Meanwhile, the proposed weight assigning based method further improves the accuracy of payload location for JPEG image steganography.

(iii) Extensive experiments are comprehensively conducted on JPEG steganographic payload location. In particular, when locating hidden bits in JSteg steganographic images with quality factor of 95 at the payload 0.1, the accuracy of location is remarkably improved from 46.18% to 90.22%, better than the prior art.

The rest of the paper is organized as follows. Section 2 presents the related works. In Section 3, we mainly revisit the fundamental of payload location. Our proposed location method is mainly extended in Section 4. Section 5 demonstrates and analyzes the numerical results. Finally, Section 6 concludes this paper.

2. Related Work

Ker [33] first proposed an algorithm for locating hidden bits of LSBR based on the idea of weighted stego (WS) in 2008. The linear filter was adopted for predicting the average residual value of each pixel, where residual-based threshold is empirically prescribed for locating embedding position. In 2009, Ker [34] proposed a payload location method based on the wavelet absolute moment (WAM) filter, in which in the wavelet domain, the WAM filter is used to extract residuals for payload location. Luo et al. [35] improved the accuracy of payload location in [34]. In particular, two methods were presented by calculating residuals with Gaussian weighted averaging, which indeed outperform the WAM method [34].

To unify the location of hidden bits embedded by LSBR or LSBM, Quach [36] proposed maximum a posteriori (MAP) vector estimation method based on Viterbi decoding for cover image estimation, where the detection performance of the WS and WAM was enhanced. Quach [37] further proposed a Markov random field-based approach, which uses pairwise constraints to capture the two-dimensional statistic from cover image, coupled with existing estimators, effectively improving the accuracy of payload location.

Next, in order to further improve the payload location accuracy of LSBM steganography, Sun et al. [43] proposed a payload location algorithm based on deep learning, which takes payload location as a pixel binary classification problem. The features extracted from the stego image are fed into the pretrained deep neural network to distinguish the payload and non-payload pixels. However, this algorithm is designed for payload location in the spatial domain and is not applicable to frequency domain.

Towards JPEG decompressed image, Liu et al. [44] presented a steganographic payload location method for secret hidden in the spatial domain. This method firstly recovered most of the cover pixels by recompression and then determined the pixel difference distribution between the cover image and the stego image. Finally, the hypothesis testing theory was adopted to confirm the correctness of the embedding positions. Inspired by the work of Liu et al. [44], series of steganalysis methods are proposed to recover the stego key towards LSBR, LSBM [38], F5 [41], and OutGuess [45]. Recently, towards adaptive steganography, [46] proposed a solution.

The aforementioned payload location methods mainly deal with the issue of extracting bits hidden in the spatial domain, in which the location accuracy is endlessly enhanced by improving the accuracy of cover image estimation. However, the study of the location method for frequential domain steganalysis is less developed.

To overcome that limitation, Wang et al. [40] first proposed a payload location method for JPEG image steganography relying on estimating the DCT coefficients. More

specifically, this method first constructed the subimage consisting of the coefficients from the same subband, in which the correlation among DCT coefficients is investigated for estimation. Moreover, it introduced the well-designed linear filter and the WAM filter to estimate the quantized DCT coefficient. Meanwhile, to enhance the accuracy of payload location, the idea of maximum posterior probability was proposed. However, the location performance is not optimal in [40], which can be improved [47]. Without the loss of generality, the linear correlation among the corresponding DCT coefficients in the subimage is not as remarkable as that among the neighboring pixels in the spatial domain. Thus, the key step of improving the accuracy is to study the correlation among coefficients, in order to acquire more accurate DCT estimation.

To further improve the accuracy of payload location in JPEG image steganography, we explore the correlation of coefficients and adopt the idea of the weight assignment in DCT domain. Inspired by the work in [46], for simplicity, it is assumed that the correlation between the quantized DCT coefficient and its adjacent coefficients in the same subimage is not uniform. Intuitively, the high-texture regions are less correlated; the low-texture regions are more correlated. Therefore, we adaptively assign different weights to different DCT coefficients to improve the accuracy of payload location.

3. Fundamentals of Payload Location

In this article, we assume that the steganographer arbitrarily embeds the secret bits into a JPEG cover image with the same size and uses the same stego key. In fact, to our knowledge, the current payload location methods are always conducted on the premise of that. In this section, we will review the fundamentals of payload location, which guides us to design the proposed method.

Let $\{C_1, C_2, \ldots, C_L\}$ denote a set of cover elements, in which C_l can represent the pixel intensity in the spatial domain or the DCT coefficient in the frequency domain. In this context, we only focus on the frequency domain. Accordingly, a set of stego elements is denoted as $\{S_1, S_2, \ldots, S_L\}$, where the secret bits are hidden. Straightforward, it is assumed that for l_{th} stego image, the residual $R_l(i, j)$ of the coefficients at position (i, j) is formulated as

$$R_l(i,j) = \left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - C_l(i,j)\right], \tag{1}$$

where $\widetilde{S}_l(i, j)$ denotes the coefficient by flipping the LSB of coefficient $S_l(i, j)$. That is, $\widetilde{S}_l(i, j)$ denotes the inverse coefficient of $S_l(i, j)$. For instance, in the procedure of JSteg steganography, the inverse coefficient of 4 is 5; the inverse coefficient of −2 is −1. In addition, in the procedure of F5 steganography, the value of the inverse conversion coefficient for coefficient 2 is 3, while the value of the inverse conversion coefficient for −2 is −3.

Let us define p_0 and p_1 as the probability of non-changed and changed coefficients in $\{S_1(i, j), S_2(i, j), \cdots, S_L(i, j)\}$. Supposing that the secret bits consist of a pseudo-random sequence, the change magnitude of each available coefficient is defined as α. If (i, j) is confirmed as the payload position, the mean of residual $\overline{R}(i, j)$ of L stego images at the same position can be described as

$$\overline{R}(i,j) = \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - C_l(i,j)\right] = p_1\alpha^2. \tag{2}$$

In contrast, if (i, j) is not the payload position, the mean of residual $\overline{R}(i, j)$ is described as

$$\overline{R}(i,j) = 0. \tag{3}$$

From (2), we derive that the residual mean from payload positions is larger than zero, that is to say, the expectation value of the residual is estimated as $p_1\alpha^2$ (proof in (8)). Accordingly, from (3), we infer that the residual mean from non-payload positions would be equal to zero (proof in (9)). However, in practice, it hardly holds true that the cover image can be acquired. Instead, the cover element has to be estimated. Then, (1) can be modified as

$$\widehat{R}(i,j) = \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - \widehat{C}_l(i,j)\right]. \tag{4}$$

In our assumption, the cover element needs to offset for better estimation. Thus, let us define $\Delta_l(i, j)$ as the estimation error of cover DCT coefficient $C_l(i, j)$, and then the following expression can be established:

$$\begin{aligned}\widehat{R}(i,j) &= \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - C_l(i,j) + \Delta_l(i,j)\right]\\ &= \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - C_l(i,j)\right]\\ &\quad + \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l\right]\Delta_l(i,j)\\ &= \overline{R}(i,j) + \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\Delta_l(i,j).\end{aligned} \tag{5}$$

Moreover, let us assume that if (i, j) is confirmed as the payload position, the mean of residual can be expressed as

$$\widehat{R}(i,j) = p_1\alpha^2 + \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\Delta_l(i,j). \tag{6}$$

Otherwise, if (i, j) is not the payload position, the mean of residual is formulated as

$$\widehat{R}(i,j) = \frac{1}{L}\sum_{l=1}^{L}\left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\Delta_l(i,j). \tag{7}$$

When $\Delta_l(i, j) = 0$, the estimation error does not exist. Then, according to (6), the expected mean of the estimated residuals in the payload position can be given by

$$E\left\{\widehat{R}(i,j)\right\} = p_1\alpha^2. \tag{8}$$

According to (7), the expected mean of the estimated residuals in the non-payload position is defined as

$$E\left\{\widehat{R}(i,j)\right\} = 0. \tag{9}$$

In this context, for clarity and simplicity, it is proposed to assume that estimation error is not considered, where $\widehat{C}$ denotes the unbias estimation of C. Therefore, based on the mathematical and fundamental analysis of payload location, even in the case that no cover images can be acquired, if each stego image has the payload at the same locations, one has the ability of effectively distinguishing between payload and non-payload positions. To further visualize the feasibility of payload location relying on the DCT residual, let us illustrate the histogram of residual mean. In Figure 1, the horizontal coordinate indicates the values of residual mean; the vertical coordinate indicates the frequency of occurrence of each residual mean. By using (4), the residual mean can be smoothly calculated. It can be observed that the distributions of the residual between non-payload and payload positions behave remarkably discriminatively.

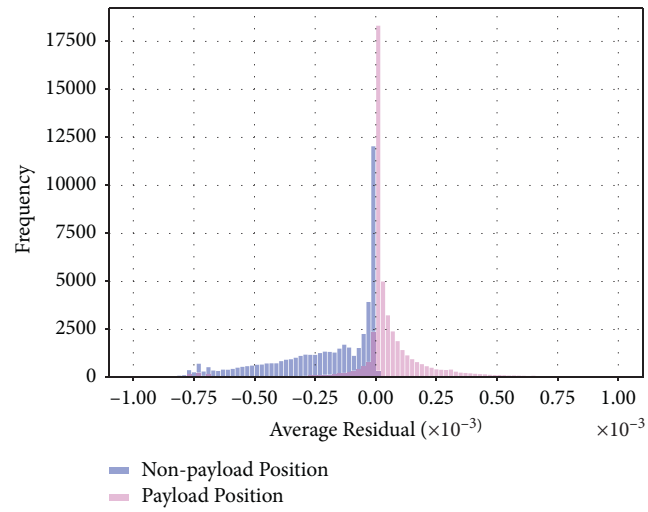

Figure 1: Histogram of the residual mean of DCT coefficients from 1,000 stego images with the embedding rate 0.5 towards JSteg steganography.

4. Our Proposed Payload Location

Prior to our discussion of the proposed method, we first illustrate the flowchart of the overall framework (see Figure 2). A set of L stego images with size $M \times N$, generated by adopting F5 or JSteg steganography, is used for locating the payload. The specific procedure of locating hidden bits in DCT domain is elaborated as follows:

(1) First, one can extract the DCT coefficients and regroup them into a subimage, where all the coefficients are from the same DCT subband. It is worth noting that the DCT coefficients are arranged in order. Thus, 64 subbands lead to 64 subimages.

(2) Next, cover element $\widehat{C}$ is accurately estimated by adopting the well-designed filter such as averaging filter or wavelet filter. Meanwhile, the flipped version of stego element $\widetilde{S}$ is obtained. According to (4), residual $\widehat{R}$ at each position can be easily acquired.

(3) The main contribution of this paper is to adopt the scheme of weight assignment. We calculate the weight based on the texture regions of inquiry image. By referring to (10), the weight can be obtained.

(4) For L images, it is proposed to normalize the residual R_L (see (11)) based on the adaptive weight factor.

(5) By sorting all residuals in descending order, the payload can be successfully located relying on the location map labeling the corresponding position of sorted residual.

In this paper, towards two classical steganographic algorithms JSteg and F5, we design the payload location method. The main contribution of this paper is to introduce the scheme of weight assignment, which indeed remarkably improves the accuracy of cover element estimation, leading to the more accurate payload location. In this section, we first present the specific scheme of weight assignment, which is applied to DCT estimation. At last, for practical location, we present the detailed procedure of payload location for JSteg and F5 steganography.

4.1. Weight Assignment of DCT Residual. In Section 3, we have already revisited the estimation procedure of the residuals. In this section, we consider to further improve the accuracy in the process of payload location by assigning different weights to the residuals. Let us define a weight factor as $w_{i,j}$ for each DCT coefficient at the position (i, j), mainly depending on the estimated coefficient neighbor's local variance $\sigma^2_{i,j}$.

In our assumption, the location variation $\sigma^2_{i,j}$ serves as the metric to evaluate the texture of the image region. In particular, large $\sigma^2_{i,j}$ represents the high-texture region, in which we accordingly assign a small weight to reduce the impact from inaccurate estimate, and vice versa. In fact, the low-texture region can indeed bring us the more accurate estimate. Therefore, let us empirically define the weight factor as

$$w_{i,j} = \frac{1}{\beta + \sigma^2_{i,j}}, \tag{10}$$

where β denotes a hyperparameter. In general, $\sigma^2_{i,j}$ can be calculated in the DCT block with size 3×3 in the subimage, where 9 DCT coefficients centering at position (i, j) are used for calculation. Thus, if the low-texture regions appear, $\sigma^2_{i,j}$ tends to be small, leading to the acquirement of large weight; if the high-texture regions appear, $\sigma^2_{i,j}$ tends to be large, leading to the acquirement of small weight. It makes sense that the DCT coefficients in the low-texture regions donate much more to the accurate estimation of residuals, where more correlated relation is exposed in an image. Relying on the adaptive weight assignment, the estimation of residual can be more sound.

Next, equipped with the well-designed weight, one can calculate the normalized weighted residuals by

$$R_L = \frac{\sum_{l=1}^{L} w_{i,j}\widehat{R}_l(i,j)}{\sum_{l=1}^{L} w_{i,j}}, \tag{11}$$

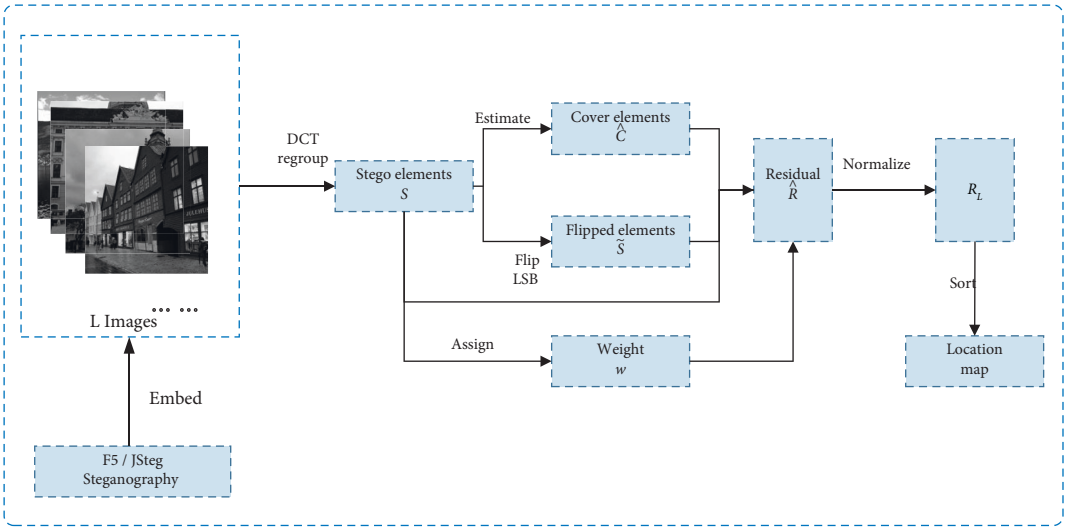

Figure 2: Illustration of the main procedure of payload location towards F5 and JSteg steganography.

where the estimated residual $\widehat{R}_l(i,j)$ for each coefficient can be described as

$$\widehat{R}_l(i,j) = \left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - \widehat{C}_l(i,j)\right] \begin{cases} \text{WAF} - F5 * (\text{QF} = 75) \\ \text{WAF} - \text{JSR} * (\text{QF} = 75). \end{cases} \tag{12}$$

Compared with the scheme of arithmetic average (see (4) for details), we propose to adopt the scheme of weighted average to acquire the more accurate estimation of residual R_L, directly resulting in the enhancement of location accuracy.

4.2. Estimation of DCT Coefficient. In order to obtain the residual, the estimation of cover DCT plays an important role. In general, the coefficients at each position represent the energy in the frequency domain as size of 8×8 block. Then, if the pixels in the spatial domain are very similar, the DCT coefficients at the same position in the adjacent blocks should also be similar (or strongly correlated). Since the contents of adjacent blocks are usually correlated, DCT coefficients at the same position are probably highly correlated. Thus, it is reasonable that all the DCT coefficients are regrouped as 64 subimages, where DCT cover elements are accurately estimated. The main steps of estimation are as follows:

(1) The inquiry JPEG image with the size of $M \times N$ is decompressed to obtain a quantized DCT coefficient matrix S_l.

(2) By regrouping all the coefficients at the same position in each DCT block, the generated subimage contains the coefficients from the same subband, where a total of 64 subimages are obtained.

(3) In each subimage, one can estimate the cover element by adopting the proposed low-pass filter. In particular, we construct two high efficient filters for estimation, which is extended in the following.

In image steganalysis, the linear correlation between adjacent elements of the matrix often serves as the basic prerequisite for cover estimation. For the design of estimator, one can adopt a simple but effective 4-neighborhood average filter. Specifically, in each subimage, the cover element is estimated by averaging four adjacent coefficients.

Besides, inspired by the WAM filter [34], we propose to apply the idea of filtering in the spatial domain to the wavelet domain. In fact, the wavelet transform has exhibited its excellent performance with good multidirectionality to capture fine-grained details of images, especially dealing with the problem of steganalysis. In particular, it is proposed to employ 8-tap Daubechies wavelet decomposition with one scale from the DCT domain to the wavelet domain. Then, the original DCT coefficients $\mathbf{S}$ are transformed to $\{\mathbf{S}^w_{LL}, \mathbf{S}^w_{HL}, \mathbf{S}^w_{LH}, \mathbf{S}^w_{HH}\}$, corresponding to low-frequency subband and high-frequency subbands (vertical, horizontal, and diagonal). We retain the low-frequency subband unchanged, while adopting the adaptive high-pass filter F to the remaining 3 subbands, which is formulated as

$$F(\mathbf{S}^w) = \frac{\gamma \mathbf{S}^w}{\sigma_0^2 + \boldsymbol{\gamma}}, \tag{13}$$

where σ_0^2 denotes the local noise variance and the parameter $\gamma = \{\gamma_i\}$ denotes the estimate of the local variance based on the four different neighborhoods with size of $K \times K$, which is formulated as

$$\gamma_i = \max\left(0,\ \min\left(\gamma_i^3, \gamma_i^5, \gamma_i^7, \gamma_i^9\right) - \sigma_0^2\right), \tag{14}$$

where $\gamma_i^K = 1/K^2 \sum_j (S_j^w)^2$. Finally, the four subbands in the wavelet domain, referred to as the original low-frequency $\mathbf{S}^w_{LL}$ and the filtered $\{\mathbf{S}^w_{HL}, \mathbf{S}^w_{LH}, \mathbf{S}^w_{HH}\}$ using (13), are inversely transformed to the DCT domain. Then, the cover element can be successfully estimated. It should be noted that in the first scale of wavelet decomposition, the filtering operation eliminates the high-frequency coefficients (mainly caused by embedding) while remaining are the low-frequency coefficients.

4.3. Payload Location for JSteg Steganography. Based on the aforementioned payload location method, let us extend our scheme to the specific steganographic algorithm, such as JSteg. JSteg steganography replaces the LSB of JPEG image in DCT domain, where the DC coefficients and AC coefficients with values of 0 and 1 remain unchanged. In this case, when estimating the residuals for 0 or 1, one can set the value to 0. Straightforward, when dealing with JSteg steganography, referring to (12), the residual can be formulated as

$$\widehat{R}_l^{\mathrm{JSteg}}(i,j) = \begin{cases} 0, & \text{if } S_l(i,j) \in \{0,1\}, \\ \left[S_l(i,j) - \widetilde{S}_l(i,j)\right]\left[S_l(i,j) - \widehat{C}_l(i,j)\right], & \text{otherwise.} \end{cases} \tag{15}$$

In the practical payload location of JSteg, we consider the impact of DCT coefficients 0 and 1 for improving the accuracy of cover DCT estimation. It is worth noting that the proposed weighted residual mean is calculated by (11) based on the obtained $\widehat{R}_l^{\mathrm{JSteg}}(i,j)$. After DCT estimation, the residual can be smoothly obtained. Next, by assigning the weight, the normalized residual guides us to locate hidden bits (see details in Figure 2).

4.4. Payload Location for F5 Steganography. In this section, in the framework of our proposed payload location, we will deal with the problem of locating hidden bits in F5 steganographic JPEG image. Similarly, F5 steganography is carried out in DCT domain, where the LSB of the negative DCT coefficients is redefined unlike JSteg. Besides, the DC coefficients and AC coefficients with 0 value are non-embeddable. When the ready-to-be-embedded bit is equal to the secret bit, no change happens; if the ready-to-be-embedded bit is different from the secret bit, the absolute value of the original coefficient is subtracted by 1. According to the embedding rules of F5, the specific residuals are specialized as

$$\widehat{R}_l^{\mathrm{F5}}(i,j) = \left[S_l(i,j) - \widetilde{S}_l^{\mathrm{F5}}(i,j)\right]\left[S_l(i,j) - \widehat{C}_l(i,j)\right], \tag{16}$$

where the flipped version of stego elements need to be redefined as

$$\widetilde{S}_l^{F5}(i,j) = \begin{cases} \pm 1\,(\text{equiprobably}), & \text{if } S_l(i,j) = 0, \\ S_l(i,j) + 1, & \text{if } S_l(i,j) > 0, \\ S_l(i,j) - 1, & \text{if } S_l(i,j) < 0, \end{cases} \tag{17}$$

where ± 1 denotes that equiprobable binary choice is made as $S_l(i,j)$ equal to 0. Specifically, the probability of 0 or 1 is approximately equal to 0.5, which is manually controlled by a uniformly distributed pseudo-random sequence. It should be noted that the proposed weighted average residual is calculated by (11) based on the obtained $\widehat{R}_l^{\mathrm{F5}}(i,j)$. Next, relying on the proposed framework of payload location, we conduct the remaining steps to complete the task of locating payload. In the following, we will demonstrate and analyze the numerical experimental results in details.

5. Experimental Results

To verify the effectiveness of the proposed location method in this paper, we conduct experiments on the baseline Bossbase 1.01 dataset [47]. It contains 10,000 images in 512×512 8 bit grayscale (PGM format) from eight different digital cameras. We compress all the images into JPEG format with quality factors of 75 and 95. It is worth noting that if there exist a large number of zero coefficients in the quantized DCT coefficients of an image, it may cause the invalid position in the embedding path which fails to be embedded, leading to the error of payload location. Thus, in our experiments, we randomly select 1,000 original images for generating stego images. The stego images are generated by using F5 and JSteg steganography, with embedding rate ranging from 0.1 to 0.9 as interval 0.1. Then, for each steganographic algorithm, 18,000 stego images can be obtained. The specific settings are listed in Table 1.

Table 1: Experimental settings.

Image source	Bossbase 1.01
Image size	512×512
Image format	JPEG
Number of original images	1,000
Quality factor	75, 95
Embedding rate	0.1 ~ 0.9
Steganography	F5, JSteg (JSR), enhanced JSteg (JSM)
DCT estimator	Average filter, wavelet filter

In this paper, our proposed location method mainly tackles with JPEG stego image embedded by F5 or JSteg. Besides, to enrich the steganographic algorithms, we extend the traditional JSteg from LSB replacement to matching, in which the LSB of the DCT coefficient is randomly ± 1 instead of LSB replacement in the frequency domain. Then, let us define the traditional JSteg replacement as JSR for abbreviation; JSM represents for the proposed JSteg matching. In Section 4.2, we have presented two types of DCT estimators, referred to as 4-neighborhood average filter and wavelet filter. In the following experiments, we intend to comprehensively evaluate the effectiveness of the proposed method by combining two filters with/without weight assignment scheme. Then, towards three different steganographic algorithms, we compare overall 9 payload location methods (see Table 2 for illustration).

5.1. Parameter Settings. In this section, we discuss the setting of the hyperparameter β in (10). We adopt the WAF-JSR location method, where a 4-neighborhood average filter is used to estimate cover elements from JSR. Two quality factors of 75 and 95 are used to generate 6,000 stego images, with embedding rates of $\{0.1, 0.5, 0.9\}$, respectively. In this experiment, it is proposed to compare the experimental results and select the optimal parameter by modifying the value of β.

The experimental results are shown in Figure 3. Basically, the setting of the parameter β cannot remarkably affect the performance of payload location. In particular, one can observe that for a quality factor of 95 and embedding rate of 0.1, the accuracy of payload location decreases sharply with increasing β due to lack of hidden bits at the same embedding position. In contrast, for a quality factor of 75 and

Table 2: Notations of different specific location schemes adopted by different estimators.

Steganographic algorithms	Average filter without weight	Average filter with weight (ours)	Wavelet filter without weight	Wavelet filter with weight (ours)
JSR	AF-JSR [40]	WAF-JSR	WF-JSR [40]	WWF-JSR
JSM	AF-JSM	WAF-JSM	WF-JSM	WWF-JSM
F5	AF-F5 [40]	WAF-F5	WF-F5 [40]	WWF-F5

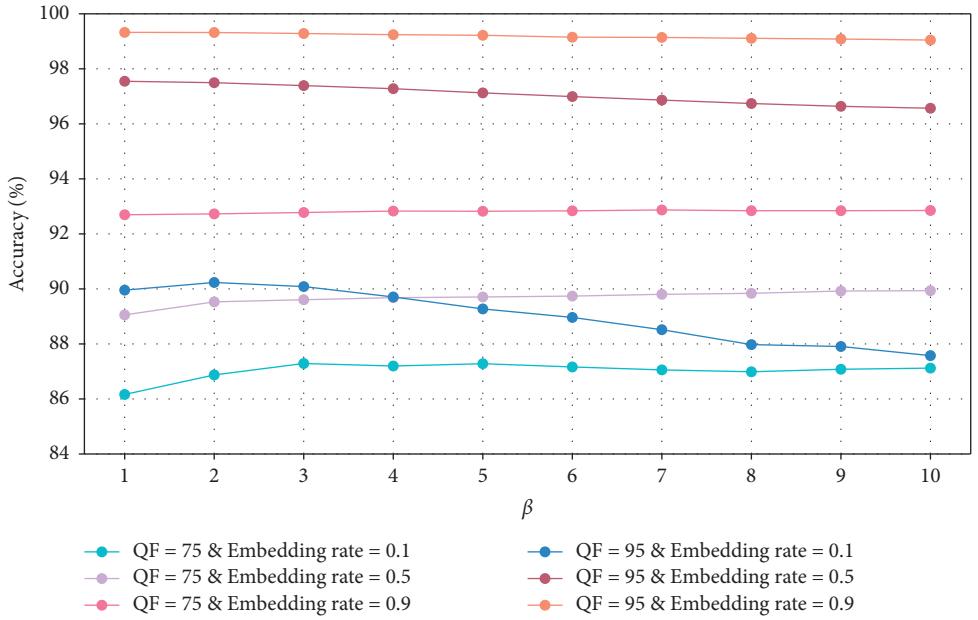

Figure 3: Accuracy comparison of payload location performance with different β.

embedding rate of 0.1 and 0.5, the accuracy of payload location slightly increases with increasing β, where it basically remains unchanged at 5. Additionally, at the embedding rate of 0.9, for the quality factor of 75 or 95, the accuracy remains very high since more hidden bits provide enough information for location.

To our knowledge, the high compression ratio directly affects the correlation among the neighboring coefficients in the subimage, where more correlated information is discarded. That is, the image with a quality factor of 75 has less correlated relationship than that of the image with a quality factor of 95. As illustrated in Figure 3, the location performance of images with the quality factor of 95 is superior to that of 75. In our location, the aim of assigning weight to the residuals is to maximize the correlated coefficients on the low-texture region while excluding the influence of the high-texture region. However, the parameter β is fixed for payload location unlike adaptive σ^2 in (10). Thus, β basically cannot remarkably impact the detection results. Based on our analysis, we empirically adopt $\beta = 3$ for our choice, which is applied in the following compared experiments.

5.2. Performance of Compared Methods. Next, to verify the validity of our proposed payload location method based on weighted DCT residual, it is proposed to conduct the comprehensive experiments. It should be noted that a set of payload locators is compared (see Table 2), towards three different JPEG image steganographic algorithms (JSR, JSM, and F5), including two quality factors of 75 and 95 and ten different embedding rates ranging from 0.1 to 0.9, where 1,000 stego images are used for payload location. Besides, it is worth noting that AF-JSR, AF-F5, WF-JSR, and WF-F5 were originally designed in [40]. Then by introducing the scheme of weight assignment in this paper, its enhanced version proposed by us refers to as WAF-JSR, WAF-F5, WWF-JSR, and WWF-F5.

First of all, let us compare our proposed payload locators with the scheme of weight assignment to the locators without assigning weight of Wang et al. [40]. As illustrated in Figure 4, it can be observed that when the quality factor remains unchanged, the accuracy of all the payload locators basically increases as the embedding rate increases. Overall, most of the locators with weight assignment perform better than the locators without weight assignment for all the given embedding rates. However, for JSR, if the wavelet filter is adopted for estimation, the locator with weight assignment (WWF-JSR) is basically similar to (even slightly worse than) the locator without weight assignment (WF-JSR). This is because the wavelet filter itself can provide the accurate enough estimation for JSR, where the strategy of weight assignment cannot largely improve the location accuracy any more.

Additionally, as we expected, it can be obviously observed that the locators perform better for dealing with JSR,

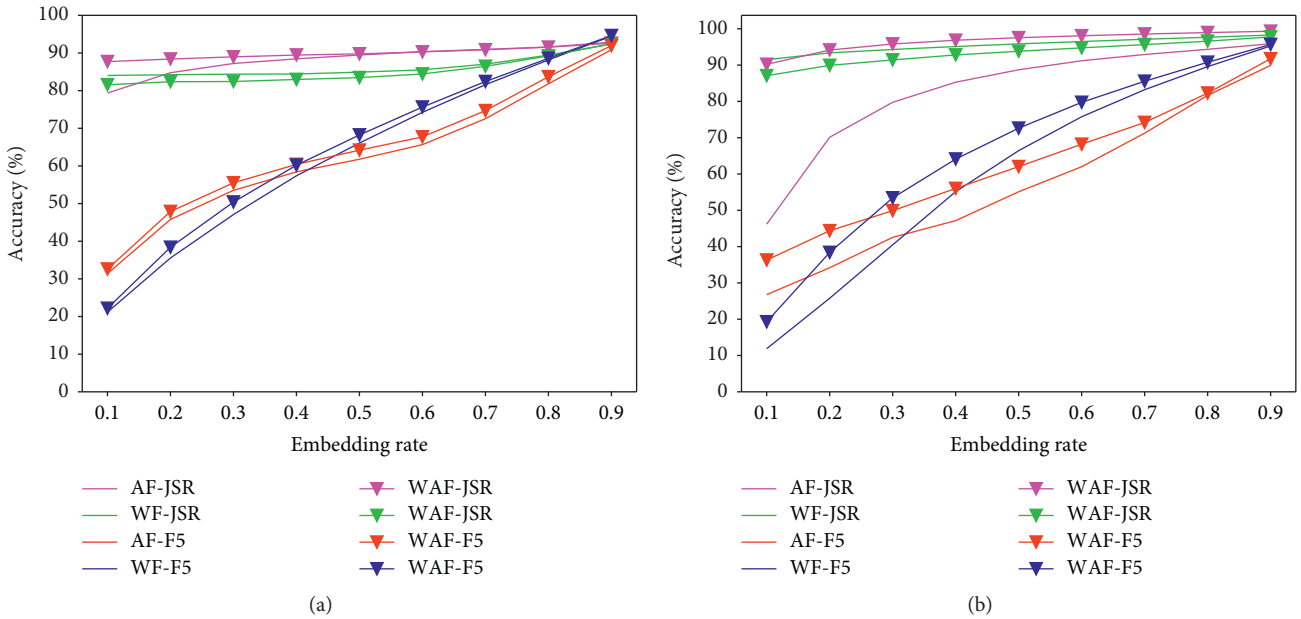

Figure 4: Accuracy comparison of payload location methods towards JSR and F5 with the quality factors of 75 and 95. (a) QF = 75. (b) QF = 95.

compared with F5. For the comparison of two filters, when the strategy of the weight assignment is considered, the 4-neighborhood average filter (AF) is better than the wavelet filter (WF) for dealing with JSR. For locating hidden bits of F5, the 4-neighborhood average filter (AF) performs better at the low embedding rate while the wavelet filter (WF) is superior at the high embedding rate.

It should be noted that when the embedding rate is high enough, 0.9 for instance, the performance of all the locators is very similar. Since that more hidden bits are embedded, the advantage of the strategy of weight assignment is not very obvious. In fact, as a smart steganographer, the low embedding rate is always selected to bring the sufficient undetectability in the practical steganography. Thus, it is of importance that the improvement of location accuracy can be achieved when adopting our proposed method at the low embedding rate. For instance, in Figure 4(b), when the embedding rate is 0.1, the accuracy of the locator without assigning weight (AF-JSR) is only 46.18%. However, our proposed location method by considering the strategy of weight assignment (WAF-JSR) is able to achieve an accuracy of 90.22%.

The aim of weight assignment is to strengthen the DCT residuals that are reliably estimated (corresponding to low-texture region) and weaken the residuals that are poorly estimated (corresponding to high-texture region). In such case, one can assign different weights to the residual based on the texture of regions. According to the aforementioned experimental results, we can empirically verify that the proposed payload locator with the strategy of weight assignment has higher accuracy compared to the locator without assigning weight [40], especially in the case that the embedding rate is not high.

Moreover, in this context, we propose an enhanced version of JSteg steganography, referring to JSM (see details in Table 2). Then, let us compare the locators dealing with the problem of locating hidden bits in the stego image generated by JSM. Similarly, the schemes with and without weight assignment are compared. As illustrated in Figure 5, the accuracy of our proposed method is higher than that of the locator without assigning weight. Still, it should be noted that the improvement of location accuracy is more remarkable at the low embedding rate than that at the high embedding rate.

Additionally, we intend to investigate the location performance of the proposed methods when different numbers of stego images are adopted for payload location. As illustrated in Tables 3 and 4, with increasing the number of stego images, the location accuracy is gradually improved. Still, as we expected, the performance with the quality factor of 95 is better than that of 75, since more correlated information is provided. The locator towards F5 is worse than the locator towards JSR or JSM, since better estimation of cover DCT coefficients leads to better location accuracy.

Last but not least, let us investigate if our proposed location method has achieved the upper bound of location. In this scenario, it is assumed that the cover elements C have been known for residual calculation. According to (2), we can easily obtain the DCT residual for payload location, in which the location results can serve as the theoretical upper bound of location. Then, the location results based on the estimated cover elements $\widehat{C}$ serve as the empirical results. As illustrated in Figure 6, when adopting the 4-neighborhood average filter, as the embedding rate increases, our proposed locator "empirical WAF-JSR" gradually approaches its theoretical upper bound while the "empirical AF-JSR" performs worse due to its inaccurate estimation.

To our knowledge, Sun et al. [43] pioneered the application of deep learning to payload location. Although the algorithm was used for hidden bit location in spatial domain,

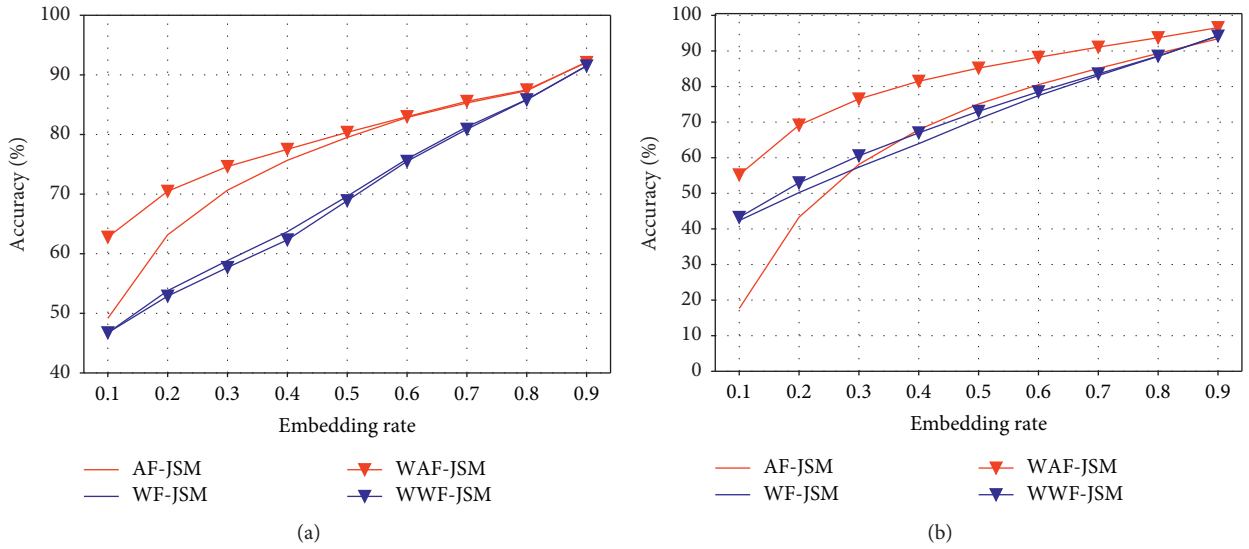

Figure 5: Accuracy comparison of payload location methods towards JSM with the quality factors of 75 and 95. (a) QF = 75. (b) QF = 95.

Table 3: Accuracy comparison of payload location methods based on different numbers of stego images with quality factor of 75.

L	WAF-JSR (%)	WAF-JSM (%)	WAF-F5 (%)	WWF-JSR (%)	WWF-JSM (%)	WWF-F5 (%)
10	48.84	45.48	54.68	48.97	45.69	**55.26**
50	**64.19**	56.45	59.40	61.28	56.07	61.57
100	**69.33**	60.49	60.30	64.85	58.64	63.36
300	**80.82**	71.11	62.17	74.03	64.56	66.98
500	**84.91**	75.38	63.10	78.08	66.69	67.65
1000	**89.81**	80.39	64.15	83.53	68.89	68.23

The bold values denote the optimal results.

Table 4: Accuracy comparison of payload location methods based on different numbers of stego images with quality factor of 95.

L	WAF-JSR (%)	WAF-JSM (%)	WAF-F5 (%)	WWF-JSR (%)	WWF-JSM (%)	WWF-F5 (%)
10	**61.15**	54.56	58.51	60.76	56.06	57.38
50	**74.69**	63.30	61.82	72.31	63.75	63.29
100	**82.03**	68.33	62.43	77.90	66.82	66.04
300	**91.90**	76.64	62.30	86.03	70.59	70.39
500	**94.98**	80.35	62.09	89.58	71.81	71.28
1000	**97.54**	85.18	62.04	93.85	72.94	72.64

The bold values denote the optimal results.

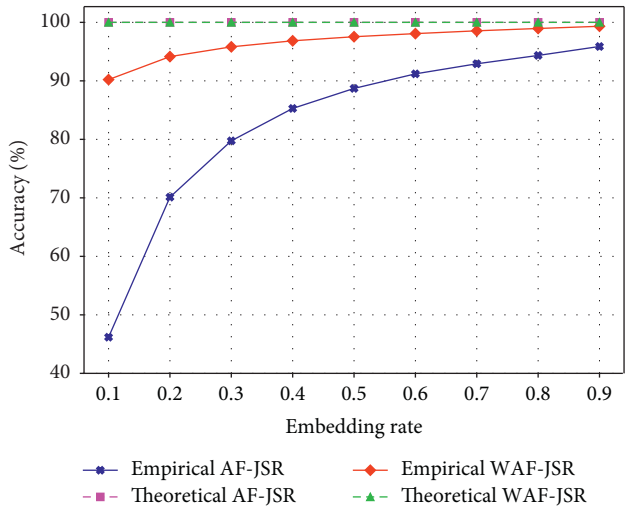

Figure 6: Accuracy comparison of empirical and theoretical location performance towards JSR with quality factor of 95.

Table 5: Accuracy comparison of deep learning method and our method with the quality factor of 75.

Steganographic algorithms	Deep learning (100 images)	Our method (100 images)	Deep learning (500 images)	Our method (500 images)	Deep learning (1000 images)	Our method (1000 images)
JSR	60.64	**69.33**	67.98	**84.91**	72.15	**89.81**
JSM	**61.36**	60.49	63.92	**75.38**	70.36	**80.39**
F5	54.94	**63.36**	**70.36**	67.65	55.67	**68.23**

The bold values denote the optimal results.

Table 6: Accuracy comparison of payload locators originally designed for JSR, towards F5 stego images with the quality factors of 75 and 95.

Embedding rate	$WAF - F5*(QF = 75)$	$WAF - F5*(QF = 75)$	$WAF - F5*(QF = 75)$	$WAF - F5*(QF = 75)$
0.1	8.11%	6.56%	**8.66**%	7.05%
0.2	18.07%	16.89%	**18.10**%	16.90%
0.3	28.78%	27.97%	**29.14**%	28.40%
0.4	**39.99**%	39.80%	39.91%	39.57%
0.5	**50.94**%	50.77%	50.87%	50.88%
0.6	61.49%	**61.77**%	61.21%	61.62%
0.7	71.61%	**72.18**%	71.71%	72.05%
0.8	81.68%	**82.16**%	81.68%	82.12%
0.9	91.55%	**91.85**%	91.55%	91.79%

we modify the original method to apply it to frequency domain steganalysis. As illustrated in Table 5, the performance of Sun et al. [43] is weaker than the algorithm proposed in this paper, especially in the case of a large number of images. Besides, the computation cost of the deep learning based algorithm is much higher due to the procedure of model training.

6. Robustness Performance of Proposed Method

In the prior evaluation, our proposed payload location method has performed its efficacy towards three different steganographic algorithms (JSR, JSM, and F5) with different embedding rates. In fact, the hidden bits are successfully extracted based on the premise that the embedding algorithms have been known. In that case, the design of our proposed residual estimators is more targeted. In these experiments, it is proposed to evaluate the robustness of the locators when the embedding algorithms are unknown. Next, we will carry out the following non-target location experiments. When locating the hidden bits generated by F5, we adopt the residual estimator originally designed for JSR (see (15)); location results are illustrated in Table 6. Meanwhile, when locating the hidden bits generated by JSR, the residual estimator originally designed for F5 (see (16)) is used for payload location; location results are illustrated in Table 7. Here, we have added the symbol $*$ for distinguishing from the payload locators in Table 2. It can be observed that when the steganographic algorithms (JSR and F5) are unknown, our proposed payload locator hardly completes the task of locating hidden bits at the low embedding rate. However, at the high embedding rate (not smaller than 0.8), the location results are relevantly satisfying. Additionally, it is worth noting that although our proposed locator WAF-JSM actually uses the residual estimator (see (15)) originally designed for WAF-JSR, the location results are also encouraging at the high embedding rate (see Figure 5 for illustration).

Next, we intend to investigate the performance of our proposed method dealing with the challengeable scenario, where all the stego images are generated by random key. That is to say, for each image, it is not required that the secret bits are hidden in the same position. As illustrated in Table 8, our proposed location method nearly becomes invalid. It should be noted that, at the high embedding rate, the location results are satisfying. Nevertheless, our proposed location method performs very well on the premise that the same key is used for embedding.

Besides, it is proposed to verify the robustness of our locating method dealing with different image sizes. In fact, the algorithm proposed in this paper is nearly independent on image size. As illustrated in Table 9, the experimental results are conducted under the same conditions of 256×256 and 512×512, in which the location results are very close by adopting each pair of location methods.

Finally, let us further verify the effectiveness of our method for adaptive steganography such as J-UNIWARD. We use the method in this paper to carry out payload location experiments for different embedding rates and different numbers of J-UNIWARD stego images. The experimental results are shown in Table 10. At low embedding rate, since adaptive steganography embeds secret bits into regions with high texture, the residual obtained from these regions will also be high. With the increase of embedding rate, the detection accuracy rate is obviously lower than the embedding rate, indicating that the location is completely invalid.

Table 7: Accuracy comparison of payload locators originally designed for F5, towards JSR stego images with the quality factors of 75 and 95.

Embedding rate	$WAF - JSR*(QF = 75)$	$WAF - JSR*(QF = 75)$	$WAF - JSR*(QF = 75)$	$WAF - JSR*(QF = 75)$
0.1	0.68%	8.24%	0.88%	**8.81**%
0.2	1.50%	**18.69**%	1.84%	18.22%
0.3	3.55%	**29.36**%	5.09%	28.18%
0.4	8.30%	**38.47**%	18.12%	38.25%
0.5	29.81%	47.74%	38.75%	**48.46**%
0.6	50.31%	57.85%	55.71%	**58.70**%
0.7	66.76%	68.83%	**69.43**%	69.23%
0.8	80.13%	80.00%	**80.95**%	80.14%
0.9	91.32%	91.10%	**91.37**%	90.99%

Table 8: Accuracy comparison of payload location methods based on different stego keys with quality factors of 75 and 95.

Embedding rate	WAF-JSR (QF = 75)	WAF-JSR (QF = 95)	WWF-JSR (QF = 75)	WWF-JSR (QF = 95)
0 (%).1	12.58	12.83	12.46	**13.70**
0.2	22.41	**23.74**	22.62	23.47
0.3	32.31	**33.56**	32.29	33.35
0.4	42.11	**43.35**	42.13	43.05
0.5	52.07	**52.92**	51.95	52.79
0.6	61.65	**62.63**	61.67	62.56
0.7	71.27	**72.30**	71.27	72.26
0.8	80.33	**81.93**	80.33	81.92
0.9	87.54	91.37	87.60	**91.56**

The bold values denote the optimal results.

Table 9: Accuracy comparison of payload location method towards JSR stego images with different image sizes involving quality factors of 75 and 95.

Embedding rate	WAF-75 (%) (256 × 256)	WAF-75 (%) (512 × 512)	WAF-95 (%) (256 × 256)	WAF-95 (%) (512 × 512)	WWF-75 (%) (256 × 256)	WWF-75 (%) (512 × 512)	WWF-95 (%) (256 × 256)	WWF-95 (%) (512 × 512)
0.1	88.05	87.71	87.37	90.22	82.32	81.56	84.51	87.07
0.2	89.34	88.39	92.74	94.14	82.82	82.37	88.30	89.92
0.3	89.87	88.97	94.74	95.82	83.14	82.43	90.36	91.42
0.4	89.89	89.46	95.86	96.85	83.44	82.97	91.96	92.80
0.5	90.48	89.76	96.92	97.54	83.84	83.46	93.30	93.80
0.6	90.69	90.28	97.54	98.08	84.74	84.43	94.39	94.75
0.7	91.36	90.86	98.10	98.55	86.75	86.46	95.29	95.64
0.8	92.09	91.54	98.59	98.95	89.72	89.21	96.54	96.58
0.9	92.94	92.59	99.13	99.33	92.74	92.42	97.73	97.77

Table 10: Accuracy comparison of our payload location method towards J-UNIWARD with quality factor of 75.

Embedding rate	1 image (%)	10 images (%)	50 images (%)	100 images (%)	300 images (%)	500 images (%)	1000 images (%)
0.1	39.03	38.66	40.00	34.66	39.08	36.76	**40.32**
0.2	43.60	43.06	36.49	36.13	40.83	39.53	**45.21**
0.3	46.12	44.34	39.20	41.27	43.15	42.09	**47.99**
0.4	50.11	47.60	42.05	44.00	45.60	46.56	**53.15**
0.5	52.01	50.61	46.73	47.54	47.79	50.18	**56.08**
0.6	54.62	53.00	50.14	51.31	50.45	53.73	**58.17**
0.7	57.82	55.33	54.12	55.93	53.70	57.68	**60.22**
0.8	59.95	59.05	58.80	58.65	58.25	59.45	**60.90**
0.9	**83.38**	62.85	64.46	63.52	76.61	75.84	62.34

The bold values denote the optimal results.

7. Conclusion and Limitation

In this paper, we propose a novel payload location method for two classical steganographic algorithms, referred to as JSteg and F5. In fact, most of the current payload locators only focus on the secrets hidden in the spatial domain and usually neglect the frequency domain. This paper focuses on the study of payload location in the frequency domain and achieves encouraging results. The main novelty of this paper is to assign weights to estimator based on image region

texture, in order to improve the accuracy of DCT coefficient estimate. Large-scale experiments are conducted to evaluate the effectiveness of the proposed method. Compared with current arts, the location accuracy is remarkably improved. However, the limitation of current methods for payload location is that multiple stego images with the same stego key are used for detection.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Fundamental Research Funds for the Provincial Universities of Zhejiang (grant no. GK219909299001-007), the National College Students Innovation and Entrepreneurship Training Program of China (grant nos. 202010336027 and 202110336033), the National Natural Science Foundation of China (grant nos. 61872448, U1804263, and 62172435), and the Zhongyuan Science and Technology Innovation Leading Talent Project of China (grant no. 214200510019).

References

[1] M. Hassaballah, *Digital Media Steganography: Principles, Algorithms, and Advances*, Academic Press, Cambridge, Massachusetts, 2020.

[2] D. Upham, "Jsteg steganographic algorithm," 1999, http://www.filewatcher.com/m/jpeg-jsteg-v4.diff.gz.8878-0.html.

[3] A. Westfeld, "F5-A steganographic algorithm, Information Hiding," in *Proceedings of the International Workshop on Information Hiding*, pp. 289–302, Springer, Pittsburgh, PA, USA, Apri 2001.

[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, pp. 1–13, 2014.

[5] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A novel image steganography method for industrial internet of things security," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 7743–7751, 2021.

[6] H. Zhou, W. Zhang, K. Chen, W. Li, and N. Yu, "Three-dimensional mesh steganography and steganalysis: a review," *IEEE Transactions on Visualization and Computer Graphics*, p. 1, 2021.

[7] Z. Tang, M. Pang, C. Yu, G. Fan, and X. Zhang, "Reversible data hiding for encrypted image based on adaptive prediction error coding," *IET Image Processing*, vol. 15, no. 11, pp. 2643–2655, 2021.

[8] C. Yu, X. Zhang, X. Zhang, G. Li, and Z. Tang, "Reversible data hiding with hierarchical embedding for encrypted images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 2, pp. 451–466, 2021.

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

[10] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 234–239, IEEE, Tenerife, Spain, December 2012.

[11] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP)*, pp. 4206–4210, IEEE, Paris, France, October 2014.

[12] 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.

[13] 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.

[14] W. Su, J. Ni, X. Hu, and J. Fridrich, "Image steganography with symmetric embedding using Gaussian Markov random field model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 3, pp. 1001–1015, 2020.

[15] 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.

[16] 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, 2019.

[17] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection," *IEEE Access*, vol. 7, pp. 24282–24289, 2019.

[18] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Multiple robustness enhancements for image adaptive steganography in lossy channels," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2750–2764, 2020.

[19] T. Qiao, S. Wang, X. Luo, and Z. Zhu, "Robust steganography resisting jpeg compression by improving selection of cover element," *Signal Processing*, vol. 183, p. 108048, 2021.

[20] 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.

[21] J. Kodovskỳ, J. 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, 2012.

[22] W. Tang, H. Li, W. Luo, and J. Huang, "Adaptive steganalysis based on embedding probabilities of pixels," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 734–745, 2016.

[23] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, "Selection of rich model steganalysis features based on decision rough set α-positive region reduction α-positive region reduction," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 336–350, 2019.

[24] T. Qiao, F. Retraint, R. Cogranne, and C. Zitzmann, "Steganalysis of jsteg algorithm using hypothesis testing theory," *EURASIP Journal on Information Security*, vol. 2015, no. 1, pp. 1–16, 2015.

[25] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.

[26] 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, 2017.

[27] 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.

[28] M. Chen, M. Boroumand, and J. Fridrich, "Deep learning regressors for quantitative steganalysis," *Electronic Imaging*, vol. 2018, no. 7, pp. 1–7, 2018.

[29] B. Li, W. Wei, A. Ferreira, and S. Tan, "Rest-net: diverse activation modules and parallel subnets-based cnn for spatial image steganalysis," *IEEE Signal Processing Letters*, vol. 25, no. 5, pp. 650–654, 2018.

[30] W. You, H. Zhang, and X. Zhao, "A siamese cnn for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 291–306, 2020.

[31] M. Yedroudj, M. Chaumont, F. Comby, A. Oulad Amara, and P. Bas, "Pixels-off: data-augmentation complementary solution for deep-learning steganalysis," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, pp. 39–48, NY, USA, February 2020.

[32] T.-S. Reinel, A.-A. H. Brayan, B.-O. M. Alejandro et al., "Gbras-net: a convolutional neural network architecture for spatial image steganalysis," *IEEE Access*, vol. 9, pp. 14340–14350, 2021.

[33] A. D. Ker, "Locating steganographic payload via ws residuals," in *Proceedings of the 10th ACM Workshop on Multimedia and Security*, pp. 27–32, NY, USA, September 2008.

[34] A. D. Ker and I. Lubenko, "Feature reduction and payload location with wam steganalysis," *Media forensics and security*, vol. 7254, p. 72540A, 2009.

[35] Y. Luo, X. Li, and B. Yang, "Locating steganographic payload for lsb matching embedding," in *Proceedings of the 2011 IEEE International Conference on Multimedia and Expo*, pp. 1–6, IEEE, Barcelona, July 2011.

[36] T.-T. Quach, "Optimal cover estimation methods and steganographic payload location," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1214–1222, 2011.

[37] T.-T. Quach, "Cover estimation and payload location using Markov random fields," *Media Watermarking, Security, and Forensics 2014*, vol. 9028, p. 90280H, 2014.

[38] J. Liu, Y. Tian, T. Han, J. Wang, and X. Luo, "Stego key searching for lsb steganography on jpeg decompressed image," *Science China Information Sciences*, vol. 59, no. 3, pp. 1–15, 2016.

[39] Q. Liu, T. Qiao, M. Xu, and N. Zheng, "Fuzzy localization of steganographic flipped bits via modification map," *IEEE Access*, vol. 7, pp. 74157–74167, 2019.

[40] J. Wang, C. Yang, P. Wang, X. Song, and J. Lu, "Payload location for jpeg image steganography based on co-frequency sub-image filtering," *International Journal of Distributed Sensor Networks*, vol. 16, no. 1, Article ID 1550147719899569, 2020.

[41] J. Liu, C. Yang, J. Wang, and Y. Shi, "Stego key recovery method for f5 steganography with matrix encoding," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1–17, 2020.

[42] J. Fridrich, M. Goljan, D. Soukal, and T. Holotyak, "Forensic steganalysis: determining the stego key in spatial domain steganography," *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, pp. 631–642, 2005.

[43] Y. Sun, H. Zhang, T. Zhang, and R. Wang, "Deep neural networks for efficient steganographic payload location," *Journal of Real-Time Image Processing*, vol. 16, no. 3, pp. 635–647, 2019.

[44] J.-f. Liu, Y.-g. Tian, T. Han, C.-f. Yang, and W.-b. Liu, "Lsb steganographic payload location for jpeg-decompressed images," *Digital Signal Processing*, vol. 38, pp. 66–76, 2015.

[45] C. Xu, J. Liu, J. Gan, and X. Luo, "Stego key recovery based on the optimal hypothesis test," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 17973–17992, 2018.

[46] T. Qiao, X. Luo, B. Pan, Y. Chen, and X. Wu, "Toward steganographic payload location via neighboring weight algorithm," *Security and Communication Networks*, vol. 2022, Article ID 1400708, 17 pages, 2022.

[47] J. Wang, C. Yang, M. Zhu, X. Song, Y. Liu, and Y. Lian, "Jpeg image steganography payload location based on optimal estimation of cover co-frequency sub-image," *EURASIP Journal on Image and Video Processing*, vol. 2021, no. 1, pp. 1–14, 2021.

[48] T. Qiao, X. Luo, T. Wu, M. Xu, and Z. Qian, "Adaptive steganalysis based on statistical model of quantized dct coefficients for jpeg images," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2736–2751, 2019.

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