

# New Design Paradigm of Distortion Cost Function for Efficient JPEG Steganography

Wenkang Su<sup>a</sup>, Jiangqun Ni<sup>a,\*</sup>, Xianglei Hu<sup>a</sup>, Jiwu Huang<sup>b</sup>

<sup>a</sup>*School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China*

<sup>b</sup>*College of Information Engineering, Shenzhen University, Shenzhen, China*

---

## Abstract

Recently, with the introduction of JPEG phase-aware steganalysis features, e.g., GFR, the design of JPEG steganographic distortion cost function turns to maintain not only the statistical undetectability in DCT domain but also in spatial domain. To tackle this issue, this paper presents a novel paradigm for the design of JPEG steganographic distortion cost function, which calculates the distortion cost via a generalized Distortion Cost Domain Transformation (DCDT) function. The proposed function comprises the decompressed pixel block embedding changes and their corresponding embedding distortion costs for unit change, where the pixel embedding distortion costs are represented in a more general exponential model, aiming to flexibly allocate the embedding data. In this way, the JPEG steganography could be formulated as the optimization problem of minimizing the overall distortion cost in its decompressed spatial domain, which is equivalent to maximizing its statistical undetectability against JPEG phase-aware steganalysis features. Experimental results show that the proposed DCDT equipped with HiLL (a spatial steganographic distortion cost function) is superior to other state-of-the-art JPEG steganographic schemes, e.g., UERD, J-UNIWARD, and GUED in resisting the detection of JPEG phase-aware feature-based steganalyzers GFR and SCA-GFR, and rivals BET-HiLL with one order of magnitude lower computational complexity, along with the possibility of being further improved by considering the mutually dependent embedding interactions. In addition, the proposed DCDT

---

\*Corresponding author

*Email addresses:* suwk3@mail.sysu.edu.cn (Wenkang Su), issjqni@mail.sysu.edu.cn (Jiangqun Ni), springhuxl@gmail.com (Xianglei Hu), jwhuang@szu.edu.cn (Jiwu Huang)

is also verified to be effective for different image databases and quality factors.

*Keywords:* information hiding, JPEG steganography, distortion cost function, domain transformation, exponential model

---

## 1. Introduction

Steganography is the science and art of covert communication without drawing suspicion from the Warden [1, 2]. With the rapid development of multimedia information technology, e.g., image, audio, and video, the steganography technology and its applications [3–17] have also made great progress in the past decades. And among them, the content-adaptive JPEG (image) steganography [13–18], which conceals secret messages in quantized DCT (Discrete Cosine Transform) coefficients, is currently the most popular and practical one since the ‘jpg’ format image is most commonly used in our lives.

With the emergence of the breakthrough coding method – STCs (Syndrome-Trellis Codes) [19] for minimal distortion embedding, the majority of the prevailing JPEG steganographic schemes focus on the design of effective steganographic distortion cost function, e.g., UERD [14], J-UNIWARD [15], GUED [16], and BET [17]. To be specific, UERD uses block energy, i.e., the sum of the absolute value of dequantized DCT coefficients within the  $8 \times 8$  DCT block, and JPEG quantization step to construct the distortion cost function. And the distortion function in J-UNIWARD is defined as the absolute sum of relative changes of the wavelet coefficients w.r.t. the cover image, where the wavelet coefficients are obtained by filtering the decompressed image using the Daubechies 8-tap wavelet directional filter bank. In consideration of the deficiency in UERD, the GUED is proposed to improve the distortion measures for DCT mode and DCT block, i.e., the absolute sum of decompressed spatial pixel block embedding changes and the absolute sum of Gabor residuals on decompressed spatial pixel block, respectively. To further improve the capability of JPEG steganography against the detection of JPEG phase-aware feature-based steganalyzers, e.g., GFR [20] and SCA-GFR [21], BET directly utilizes the embedding entropy of decompressed spatial pixel block to construct DCT block distortion measure, and by which, BET

becomes currently the most secure JPEG steganographic scheme.

The success of J-UNIWARD, GUED, and BET against the detection of JPEG phase-aware feature-based steganalyzers indicates that JPEG steganography should maintain not only the statistical undetectability in DCT domain but also in spatial domain. Following this philosophy of distortion cost function design, in this paper, we propose a novel paradigm for JPEG steganography, namely **Distortion Cost Domain Transformation (DCDT)** based JPEG steganography scheme, which formulates the JPEG steganography as the optimization on minimizing the overall distortion cost in its decompressed spatial domain. The basis of our proposed scheme is that the embedding priority for both the  $8 \times 8$  DCT block and its decompressed block in spatial should be the same since they represent the same image information. In our proposed scheme, a generalized distortion cost domain transformation function  $f$  is introduced to directly transform the decompressed spatial distortion cost into JPEG domain with the assumption that the spatial distortion cost is linearly proportional to the amplitude of embedding modification in its decompressed spatial domain. To further maintain the statistical undetectability, an exponential model is then developed for spatial distortion cost to improve the construction of  $f$ . Extensive experiments show that the proposed scheme equipped with HiLL has a more comprehensive security performance improvement than UERD with the same computational complexity, and is superior to J-UNIWARD and GUED in resisting the detection of GFR and SCA-GFR, along with the possibility of being further improved by considering the mutually dependent embedding interactions. Besides, it can also rival the state-of-the-art (SOTA) BET-HiLL with one order of magnitude lower computational complexity. What's more, the proposed scheme is also effective and widely applicable for other image databases and a variety of Quality Factors (QFs).

The remainder of this paper is organized as follows. In the next section, we firstly introduce the basis and motivation behind the proposed scheme in subsection 2.1, and then the selection strategy of spatial steganographic distortion cost function will be discussed in subsection 2.2. Subsequently, the construction of the generalized distortion cost domain transformation function is given in subsection 2.3. Additionally, we further make an extension for the proposed scheme in terms of mutually dependent

embedding in section 2.4, which is followed by the extensive experimental results and analysis in section 3. Finally, the paper is concluded in section 4, where we summarize the most important contributions given in this paper.

## 2. The proposed novel paradigm for the design of JPEG steganographic distortion cost function

In this section, we propose a novel paradigm for the design of JPEG steganographic distortion cost function, which obtains the JPEG distortion cost via directly transforming the spatial embedding distortion cost into JPEG domain. In the following, the basis and motivation behind this proposed scheme will be firstly elaborated. And then, the selection of spatial steganographic distortion cost function for the proposed scheme will be discussed subsequently. Next, the construction of the proposed generalized distortion cost domain transformation function, which is the core of our proposed scheme, will be explained in detail. Finally, the extension to mutually dependent embedding for the proposed scheme will be further presented.

### 2.1. The basis and motivation behind the proposed scheme

Concerning the JPEG steganography, it is well known that when we modify the DCT coefficient  $x_{a,b}^{m,n}$ , i.e., the one at mode  $(a, b)$  in the  $(m, n)^{th}$  DCT block, the corresponding spatial embedding changes can be easily derived by its inverse DCT transformation. Since JPEG compression is based on block DCT transformation, then the decompressed spatial embedding changes would only happen within its corresponding  $8 \times 8$  pixel block, which is associated with the quantization step  $q_{a,b}$ , irrespective of image content. Thus, the relationship between the DCT domain embedding modification and the spatial embedding changes can be explicitly expressed as:

$$\mathbf{s}_{a,b} = q_{a,b} \cdot (\mathbf{A}^T * \mathbf{t}_{a,b} * \mathbf{A}), \quad (1)$$

where

$$\mathbf{A} = \begin{bmatrix} a & a & a & a & a & a & a & a \\ b & d & e & g & -g & -e & -d & -b \\ c & f & -f & -c & -c & -f & f & c \\ d & -g & -b & -e & e & b & g & -d \\ a & -a & -a & a & a & -a & -a & a \\ e & -b & g & d & -d & -g & b & -e \\ f & -c & c & -f & -f & c & -c & f \\ g & -e & d & -b & b & -d & e & -g \end{bmatrix}, \quad (2)$$

$$\begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \end{bmatrix} = \frac{1}{2} \begin{bmatrix} \cos(\pi/4) \\ \cos(\pi/16) \\ \cos(\pi/8) \\ \cos(3\pi/16) \\ \cos(5\pi/16) \\ \cos(3\pi/8) \\ \cos(7\pi/16) \end{bmatrix}, \quad (3)$$

‘\*’ indicates the matrix multiplication, and  $\mathbf{A}^T$  is the transpose of  $\mathbf{A}$ ,  $\mathbf{t}_{a,b}$  represents the solitary modification on mode  $(a, b)$  among the 64 DCT modes,  $\mathbf{s}_{a,b}$  denotes the resultant corresponding spatial  $8 \times 8$  pixel block embedding changes.

As we know, the JPEG compression is based on block-wise DCT transformation, so the  $8 \times 8$  DCT block represents the same information with its corresponding decompressed  $8 \times 8$  pixel block, then the embedding priority of the  $8 \times 8$  DCT and pixel block shall be the same, which in turn constitutes the basis of our proposed scheme. In addition, the objective of content-adaptive spatial steganography is to minimize their overall distortion for given payload under the framework of minimal distortion embedding [19]. Therefore, referring to Eq. (1), if we can measure the spatial distortion for arbitrary modification amplitude, then the overall additive distortion of JPEG steganography in its decompressed spatial domain can be accordingly obtained. As thus, we can formulate the JPEG steganography under the framework of minimal distortion embedding as the optimization on minimizing the overall distortion cost in its decompressed

spatial domain, and therefore to improve the performance of JPEG steganography by maintaining the statistical undetectability in both spatial and DCT domains.

## 2.2. Discussion on the selection of spatial steganographic distortion cost function

As the key part in calculating the overall distortion cost in the decompressed spatial domain, the selection of spatial steganographic distortion cost function for the proposed scheme is of vital importance. With regard to the method of calculating the spatial distortion cost, there are many candidates, such as WOW [22], S-UNIWARD [15], HiLL [11], MiPOD [23] and etc. As stated earlier, the  $8 \times 8$  DCT and pixel block has the same embedding priority, then the better the spatial steganography cost function is utilized, the higher the security of the proposed scheme should be. Notably, the HiLL would be an excellent candidate because of its excellent security performance and minimal computational complexity<sup>1</sup>. To analyze its feasibility, we then make a simple experiment in the following, i.e., calculating and comparing the similarity in evaluating the DCT block embedding priority between HiLL and other JPEG steganographic distortion cost functions.

Without loss of generality, we randomly select 2,000 cover images from BOSSBase ver1.01 [24] at Q75 and Q95<sup>2</sup> separately and then use UERD, J-UNIWARD, GUED, and HiLL to calculate the embedding cost for each  $8 \times 8$  DCT or decompressed pixel block within the cover. In our experiment, it should be noted that the block embedding cost with HiLL is expressed by the sum of 64 pixels' embedding costs within this block of the decompressed image, while for J-UNIWARD, it is expressed by the reciprocal sum of the absolute value of  $23 \times 23$  wavelet filter residuals w.r.t this block in three directions. In addition, we will also randomly generate a set of DCT block embedding costs denoted as *Rand*, as a comparison to verify the validity of this experiment. Since the block embedding priority is determined by the block embedding cost, thus, the similarities of (DCT or pixel) block embedding priority among different steganographic schemes can be evaluated by calculating the similarities of their

---

<sup>1</sup>Actually, we have also tested other spatial steganographic distortion cost functions in section 3.3, and find that HiLL is indeed the one which yields the best security performance.

<sup>2</sup>In the rest of this paper, for brevity, we represent QF=75 and QF=95 by Q75 and Q95, respectively.

block embedding costs. As regards the choice of metric for similarity, we adopt the *Spearman Correlation Coefficient (SCC)* [25], which is one of the three popular statistical correlation coefficients and corresponds to the ‘corr’ Matlab command with type ‘Spearman’. The sign ‘+’ and ‘-’ of *SCC* represent positive correlation and negative correlation, respectively, and the magnitude represents the degree of correlation (0 is irrelevant, 1 is completely linear relevant). Finally, the average *SCCs* over 2000 cover images at Q75 and Q95 are summarized in Table 1.

Table 1: The average *Spearman Correlation Coefficients (SCCs)* over 2000 cover images at Q75 and Q95 between the DCT block embedding cost (Rand, UERD, J-UNIWARD, GUED) and the pixel block embedding cost (HiLL), respectively.

Different schemes	Q75	Q95
$SCC(Rand,HiLL)$	0.0	0.0
$SCC(UERD,HiLL)$	+0.7801	+0.7777
$SCC(J-UNIWARD,HiLL)$	+0.8420	+0.8584
$SCC(GUED,HiLL)$	+0.8666	+0.8962

Referring to the results in Table 1, it is observed that  $SCC(Rand,HiLL)$  is close to 0, while others are around 0.8. Since the block embedding cost with Rand is randomly generated, while for UERD, J-UNIWARD, GUED, and HiLL, they are all well designed based on the statistical characteristics of cover image, so this result indicates that the proposed similarity metric *SCC* is reasonable. In addition, comparing  $SCC(J-UNIWARD,HiLL)$  with  $SCC(UERD,HiLL)$ , it is observed that J-UNIWARD is closer to HiLL than UERD in evaluating the block embedding priority along with higher security performance against steganalyzers, e.g., GFR. It is the same for GUED and J-UNIWARD. Furthermore, reviewing the performance of BET [17] and GUED [16], it shows that the BET-HiLL whose block embedding cost is constructed from HiLL is also superior to GUED in resisting the detection of GFR. In this regard, it is convinced that if the evaluation of block embedding priority of a JPEG steganographic scheme is closer to HiLL’s, then it would be more secure. Therefore, if the DCT block embedding

priority for a JPEG steganographic scheme is evaluated with HiLL on the corresponding block of the decompressed image, better security performance is expected to be achieved.

### 2.3. Construction of the proposed distortion cost domain transformation function

Referring to section 2.1, we know that the spatial distortion cost for arbitrary modification amplitude should be defined when we intend to formulate the JPEG steganography as the optimization on minimizing the overall distortion cost in its decompressed spatial domain. Note that the unit modification (+1/−1) on DCT coefficient will lead to non-unit spatial embedding changes, and on the other hand, although there exist a variety of fairly good distortion functions in spatial domain, they are almost all designed for measuring the distortion on unit embedding change. In this regard, we make a simple yet effective assumption that the spatial distortion cost is linearly proportional to the amplitude of modification for a pixel. As thus, for the  $\pm 1$  modification on DCT coefficient  $x_{a,b}^{m,n}$ , the resulting spatial additive distortion can be expressed as:

$$\rho_{a,b}^{m,n} = \sum_{i=1}^8 \sum_{j=1}^8 d_{m,n}(i,j) \cdot |s_{a,b}(i,j)|, \quad (4)$$

where  $d_{m,n}(i,j)$  represents the spatial distortion cost of the  $(i,j)^{th}$  pixel in corresponding block of decompressed image for unit embedding change,  $|s_{a,b}(i,j)|$  indicates the resulting spatial embedding changes within the corresponding  $8 \times 8$  block due to the unit embedding modification at DCT mode  $(a,b)$ , which can be obtained by Eq. (1). By taking into account the statistics both in spatial and DCT domains, the  $\rho_{a,b}^{m,n}$  in Eq. (4) could well evaluate the resulting distortions in both spatial and DCT domains arising from the embedding modification at DCT coefficient  $x_{a,b}^{m,n}$ , and be adopted as the distortion cost for the proposed JPEG steganographic scheme. Since  $\rho_{a,b}^{m,n}$  is obtained by transforming the spatial distortion cost into DCT domain, the proposed scheme can then be referred to as **Distortion Cost Domain Transformation (DCDT)** based JPEG steganographic scheme, and the Eq. (4) can be formulated as a distortion cost domain transformation function  $f(\mathbf{d}_{m,n}, \mathbf{s}_{a,b})$  as well, where  $\mathbf{d}_{m,n}$  and  $\mathbf{s}_{a,b}$  are the  $(m,n)^{th}$  decompressed  $8 \times 8$  pixel block distortion costs and decompressed  $8 \times 8$  spatial embedding changes for solitary modification on DCT mode  $(a,b)$ , respectively.

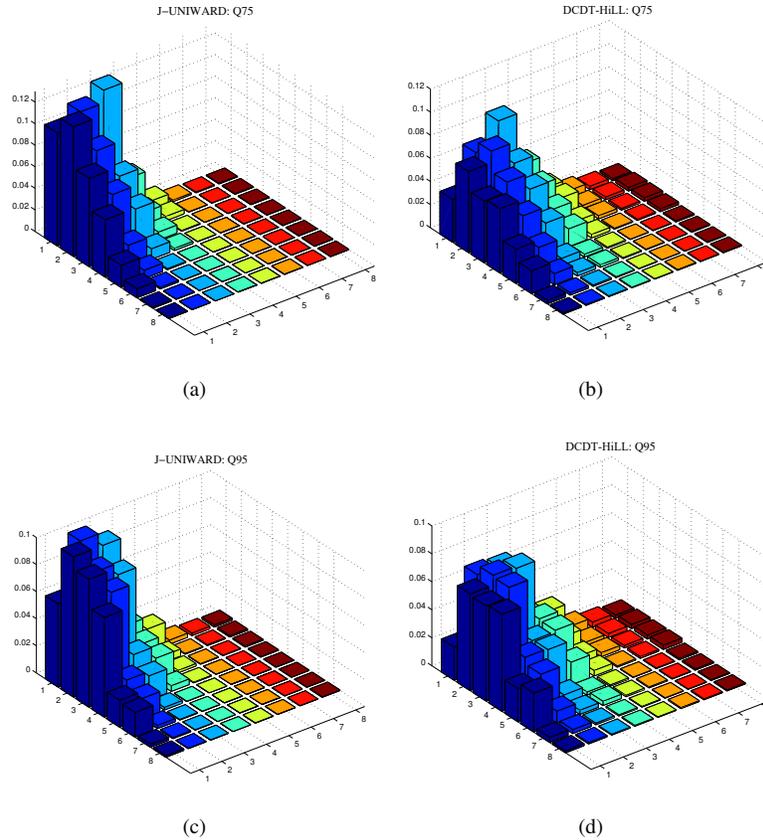


Figure 1: The statistical histogram for the percentage of average embedding modifications of 64 DCT modes under J-UNIWARD (Left) and DCDT-HiLL (Right) at relative payload 0.4 bpnzAC for Q75 (Top) and Q95 (Bottom).

It is noted that the existing content-adaptive spatial steganographic schemes, e.g., WOW [22], S-UNIWARD [15], HiLL [11], and MiPOD [23], are prone to embed messages in rich texture regions of the cover image. Therefore, the proposed DCDT may have a tendency to encourage more embedding modifications on mid-to-high frequency DCT coefficients, compared with the previous ones, e.g., J-UNIWARD. To validate this, we randomly select 2,000 covers images from BOSSBase ver1.01 [24] at Q75 and Q95 separately and then perform embedding with J-UNIWARD and DCDT-

HiLL<sup>3</sup> at relative payload 0.4 bpnzAC (bit per non-zero cover AC coefficient). As a result, the average embedding modification histograms of 64 DCT modes for the four stego sets are shown in Figure 1, indicating that whether on Q75 or Q95, DCDT-HiLL has more modifications on mid-to-high frequency DCT modes than J-UNIWARD. The distributions of embedding modifications on mid-to-high frequency DCT coefficients, however, should be well controlled, otherwise, the resulting spatial changes would become larger, especially at low QFs, which in turn make the embedding insecure. To tackle this issue, the distortion function in Eq. (4) is rewritten as the exponential form in Eq. (5) below:

$$\rho_{a,b}^{m,n} = f(\mathbf{d}_{m,n}, \mathbf{s}_{a,b}, p) = \sum_{i=1}^8 \sum_{j=1}^8 (d_{m,n}(i,j))^p \cdot |s_{a,b}(i,j)|, \quad (5)$$

where  $p$  is the exponent parameter, which is used to flexibly adjust the embedding distributions among different DCT blocks. With the distortion function defined in Eq. (5), the proposed JPEG steganographic scheme is developed under the STC-based minimal distortion embedding framework as shown in Fig. 2.

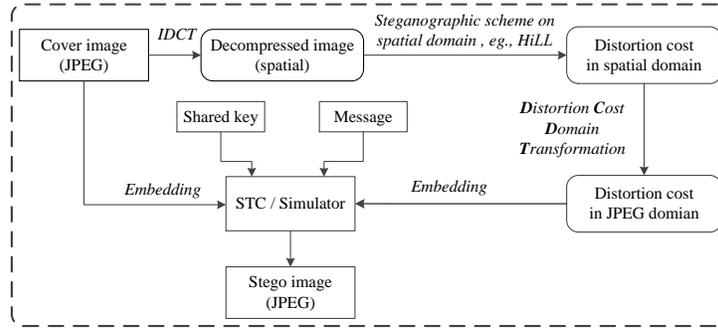


Figure 2: The diagram of the proposed scheme. (IDCT for Inverse Discrete Cosine Transform)

<sup>3</sup>Similar to the situation of BET-HiLL, it indicates that the DCDT scheme adopts HiLL as the spatial steganographic distortion cost function.

#### 2.4. Extension to mutually dependent embedding for the proposed scheme

In practical applications, multiple DCT coefficients in one DCT block may be modified simultaneously, then the Eq. (1) will be updated as:

$$\mathbf{s} = [\mathbf{A}^T * (\mathbf{t} \cdot \mathbf{q}) * \mathbf{A}], \quad (6)$$

where  $\mathbf{t}$  represents the simultaneous modifications on multiple DCT modes in one  $8 \times 8$  DCT block, and  $\mathbf{q}$  is the corresponding quantization step matrix. As thus, the influence of embedding modifications in spatial domain would be mutually dependent. Recently, several mutually dependent embedding schemes have been developed, which are generally called the **S**ynchronizing **M**odification **D**irection (SMD) strategy, e.g., CMD [26], Synch [27], ASYMM [28] and Dejoin [29][30], and by which, we can extend our proposed DCDT-HiLL to mutually dependent embedding, as illustrated in Figure 3. First of all, similar to the SMD embedding schemes, we perform the ternary embedding with DCDT-HiLL at the given payload, and then the embedding modification result, i.e., +1, 0, -1, for all the DCT coefficients in cover image can be accordingly obtained, for brevity, we call it the embedding modification map and denoted by  $M$ . Without loss of generality, we take the  $k^{th}$   $8 \times 8$  block  $m_k$  of  $M$  in alignment with the DCT block of the cover for example, and record the indexes of the non-zero elements inside block  $m_k$  as well as their number ( $n_k$ ). Subsequently, we traverse all the non-zero elements inside  $m_k$  for their adjustment of modification direction (+1/-1), which will then generates  $2^{n_k}$  embedding modification candidate blocks. Likewise, for each of these candidates, the corresponding JPEG embedding distortion cost can be obtained by

$$\rho_k = \sum_{i=1}^8 \sum_{j=1}^8 (d_k(i, j))^p \cdot |s_k(i, j)|, \quad (7)$$

where  $d_k(i, j)$  represents the spatial distortion cost of the  $(i, j)^{th}$  pixel in the  $k^{th}$  block of decompressed image for unit embedding change,  $|s_k(i, j)|$  indicates the spatial mutually dependent embedding changes on the  $(i, j)^{th}$  pixel in the corresponding block, and which can be obtained by Eq. (6).

After that, the optimal embedding modification block can be then obtained by finding out the one which yields the minimum embedding distortion cost among the  $2^{n_k}$

candidate blocks, and in this way, the optimal embedding modification map  $M'$  will be obtained after we traverse all the blocks in  $M$ . Finally, referring to  $M'$ , we appropriately update the original distortion cost  $\rho$  calculated by DCDT-HiLL, and then use the updated distortion cost  $\rho'$ , which is referred to as DCDT-HiLL\_ud, to perform ternary embedding once again. Similar to the SMD strategy, the proposed distortion cost updating has the following definition:

$$\rho'_{i,j}^+ = \begin{cases} \rho_{i,j}/v, M'_{i,j} = +1 \\ \rho_{i,j} * v, M'_{i,j} = -1 \\ \rho_{i,j}, M'_{i,j} = 0 \end{cases}, \rho'_{i,j}^- = \begin{cases} \rho_{i,j}/v, M'_{i,j} = -1 \\ \rho_{i,j} * v, M'_{i,j} = +1 \\ \rho_{i,j}, M'_{i,j} = 0 \end{cases}, \quad (8)$$

where the subscript  $\{i, j\}$  stands for the index of DCT coefficient  $x_{i,j}$ ,  $\rho'_{i,j}^+$  and  $\rho'_{i,j}^-$  are the updated distortion costs for modification  $x_{i,j} + 1$  and  $x_{i,j} - 1$ , respectively, and  $v$  is the penalty factor. The implementation of mutually dependent embedding does improve the performance at the cost of exponential complexity, therefore, unless otherwise specified, all the experiments in this paper are carried out with Mutually Independent (MI) embedding. And to the best of our knowledge, the MI embedding has also been used in J-UNIWARD and GUED with superior security performance.

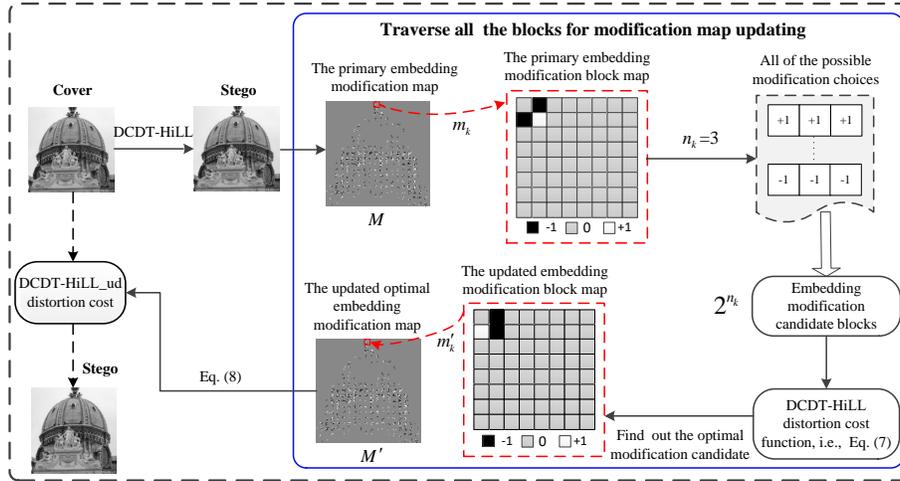


Figure 3: The diagram of the mutually dependent embedding extension of the proposed scheme, including primary embedding, embedding modification map optimization, distortion cost updating and secondary embedding.

### 3. Experimental results and analysis

#### 3.1. Experiment setups

All the experiments in this section are carried out on image database BOSSBase ver1.01 [24] and BOWS2 [31], and both of them contain 10,000 gray-scale images of size  $512 \times 512 \times 8$  bits. All the images in each database will be compressed by the JPEG Toolbox [32] at different Quality Factors (QFs) to obtain various JPEG image sets, and for each JPEG image set, one half of them are used for training, while others for testing. To differentiate among various dataset, in the following, we use the syntax of names for JPEG image set following the convention:  $name = \{primary\_dataset\}\{J\}\{QF\}$ , where  $primary\_dataset$  indicates the candidate image database, e.g., BOSSBase and BOWS2,  $J$  stands for JPEG compression option, and  $QF$  is the quality factor used in JPEG compression.

Several SOTA universal JPEG steganalyzers, including CC-JRM-22,510D [33], GFR-17,000D [20] and its selection-channel-aware version SCA-GFR-17,000D [21], are employed to evaluate the empirical security performance of the involved JPEG steganographic schemes, where the binary classifier is trained by the Fisher Linear Discriminants (FLD) ensemble [34] with default settings. The classification error probability  $P_E$  of FLD ensemble classifier, corresponding to the empirical security performance of the tested JPEG steganographic scheme, is reported by the mean value of the ensemble's testing errors based on ten times of randomly testing, and all the experiments are simulated at the corresponding payload distortion bound for relative payloads  $\alpha \in \{0.1, 0.2, 0.3, 0.4, 0.5\}$  bpnzAC.

#### 3.2. Determining the optimal exponent parameter $p$ in DCDT-HiLL

Since the exponent parameter  $p$  in Eq. (5) can be used to adjust the distributions of embedding modifications among DCT blocks, there should be an optimal  $p$  setting for given steganalyzer, QF, and relative payload. To determine the  $p$  in DCDT-HiLL for given QF and relative payload w.r.t. three SOTA JPEG steganalyzers CC-JRM, GFR, and SCA-GFR, we randomly select 5,000 images from BOSSBase with given QF, in which 2,500 JPEG images are used for training, while others for testing. We set  $p$  in

the range of  $[0.3, 1.5]$  and search with interval 0.1 to find the optimal  $p^*$  corresponding to the maximum classification error probability  $P_E^*$  at given relative payload  $\alpha$  for each of the three tested steganalyzers. The  $p^*$  for GFR versus relative payloads on BOSSbaseJ75 and BOSSbaseJ95 are illustrated in Fig. 4, it shows that the optimal parameters  $p$  is nearly irrelevant to relative payloads, and for simplicity, we finally set  $p^*$  as 0.7 and 1.1 for Q75 and Q95, respectively. Similarly, the optimal parameters  $p^*$  for Q75 and Q95 w.r.t. other tested steganalyzers can be obtained as well, which are all summarized in Table 2.

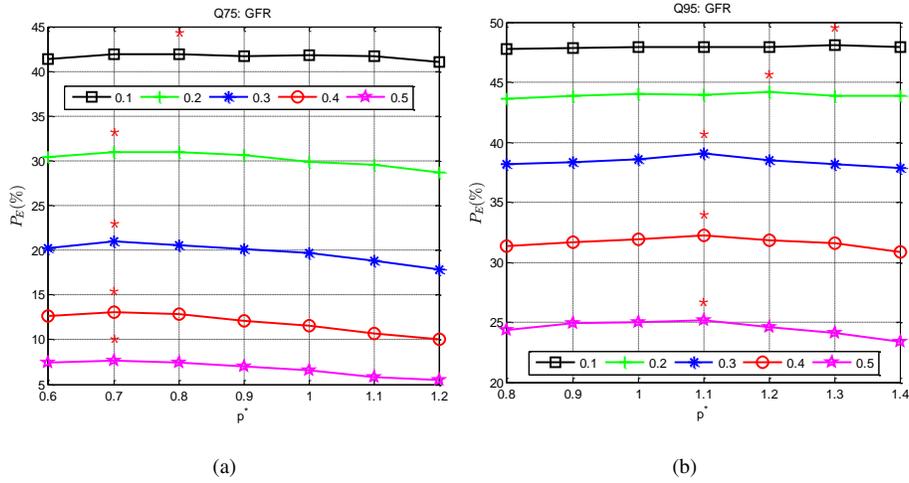


Figure 4: (a) and (b) are the classification error probability  $P_E$  associated with different  $p$  towards steganalyzer GFR versus relative payloads  $\alpha$  on BOSSbaseJ75 and BOSSbaseJ95, respectively. The optimal results are indicated with symbol \* in the figure.

Table 2: The optimal parameter  $p$  in DCDT-HILL for all the involved steganalyzers CC-JRM, GFR and SCA-GFR on BOSSBaseJ75 and BOSSBaseJ95.

QF	Steganalyzer		
	CC-JRM	GFR	SCA-GFR
75	0.7	0.7	0.5
95	0.9	1.1	0.9

### 3.3. The performance of the proposed JPEG steganographic scheme with various spatial steganographic distortion cost functions

To verify the effectiveness of the proposed JPEG steganographic scheme equipped with spatial steganographic distortion cost function HiLL, another two SOTA spatial distortion cost functions S-UNIWARD and MiPOD are then used for comparison. Similar to the procedure of HiLL in determining the optimal  $p$ , we can easily obtain the optimal parameters  $p$  for S-UNIWARD and MiPOD on BOSSBaseJ75 and BOSSBaseJ95 w.r.t. CC-JRM and GFR, which are shown in Table 3. Then, we compare the security performance of DCDT-HiLL with DCDT-S-UNIWARD and DCDT-MiPOD against the detection of CC-JRM and GFR on BOSSBaseJ75 and BOSSBaseJ95 at their corresponding optimal  $p$  as shown in Table 4. It is observed that the proposed DCDT equipped with HiLL exhibits the best security performance, and it is adopted in the rest of the paper unless otherwise specified.

Table 3: The optimal parameter  $p$  in DCDT-S-UNIWARD and DCDT-MiPOD for steganalyzers CC-JRM and GFR on BOSSBaseJ75 and BOSSBaseJ95.

QF	S-UNIWARD		MiPOD	
	CC-JRM	GFR	CC-JRM	GFR
75	1.2	1.3	0.7	0.7
95	1.9	2.0	0.7	0.7

### 3.4. Performance comparison of the proposed DCDT-HiLL with other SOTA JPEG steganographic schemes

We then compare the security performance of the proposed DCDT-HiLL with other SOTA JPEG steganographic schemes, e.g., UERD, J-UNIWARD, GUED, and BET-HiLL at different relative payloads on BOSSBaseJ75 and BOSSBaseJ95, which are summarized in Table 5 and 6, respectively. For brevity, the results of our proposed DCDT-HiLL (except *DCDT-HiLL-pro*) in Table 5 and 6 are obtained with the optimal parameter setting for SCA-GFR (i.e.,  $p=0.5$  and  $p=0.9$  for Q75 and Q95, respectively). This is because SCA-GFR is the most effective steganalyzer and the performance of the

Table 4: Classification error probability  $P_E$  (in %) of DCDT-S-UNIWARD, DCDT-MiPOD and DCDT-HiLL for CC-JRM and GFR versus relative payloads on BOSSBaseJ75 and BOSSBaseJ95.

Steganalyzer	QF	Scheme	Relative payload $\alpha$ (bpnzAC)				
			0.1	0.2	0.3	0.4	0.5
CC-JRM	75	DCDT-S-UNIWARD	46.48	39.66	32.01	23.68	16.52
		DCDT-MiPOD	45.97	39.27	31.27	23.20	15.86
		<b>DCDT-HiLL</b>	<b>46.62</b>	<b>40.10</b>	<b>32.25</b>	<b>24.10</b>	<b>17.02</b>
	95	DCDT-S-UNIWARD	49.39	47.39	43.77	38.49	31.19
		DCDT-MiPOD	49.27	46.99	42.60	35.96	28.52
		<b>DCDT-HiLL</b>	<b>49.44</b>	<b>47.84</b>	<b>45.05</b>	<b>40.12</b>	<b>33.53</b>
GFR	75	DCDT-S-UNIWARD	41.08	29.47	18.89	11.12	6.07
		DCDT-MiPOD	39.96	27.58	17.20	9.90	5.33
		<b>DCDT-HiLL</b>	<b>41.30</b>	<b>29.95</b>	<b>19.61</b>	<b>12.06</b>	<b>6.80</b>
	95	DCDT-S-UNIWARD	47.69	43.06	37.01	29.35	21.67
		DCDT-MiPOD	47.50	42.62	36.18	28.56	20.71
		<b>DCDT-HiLL</b>	<b>47.94</b>	<b>43.67</b>	<b>38.16</b>	<b>31.22</b>	<b>23.80</b>

proposed DCDT-HiLL with the same parameter setting won't change much as justified by our experiments.

As shown in Table 5 and 6, it is observed that for steganalyzer SCA-GFR, the proposed DCDT-HiLL achieves an overall superior performance than UERD, J-UNIWARD, and GUED. In addition, DCDT-HiLL also consistently outperforms BET-HiLL by a clear margin (increase the  $P_E$  by 1.4%-2.1% on average) for JPEG images of Q75, and shows comparable performance with BET-HiLL for Q95.

For the steganalyzer GFR, however, although our proposed DCDT-HiLL still exhibits excellent performance compared with other competing schemes except BET-HiLL for JPEG images of Q95, the performance gains are significantly narrowed for Q75. And it only shows comparable or slightly inferior performance than BET-HiLL whether for JPEG images of Q75 or Q95. The following two reasons may contribute to the performance degradation. One is that the suboptimal parameter setting for GFR. When the optimal parameter setting for GFR under Q75 is adopted, i.e.,  $p=0.7$  (*DCDT-HiLL-pro*), the performance of the proposed DCDT-HiLL is indeed improved as illustrated in Table 5. The other is the assumption of mutually independent embedding, which will be discussed later. Note that the effect of the quantization step, the embedding influence in the spatial domain for Q75 is much greater than that of Q95, which may lead to the performance decline for Q75 compared with the one for Q95.

When it comes to the steganalyzer CC-JRM, both BET-HiLL and the proposed DCDT-HiLL are inferior to J-UNIWARD and GUED. Likewise, there may be two reasons that contributed to the degradation of performance. One is the suboptimal parameter setting for CC-JRM. We simulate DCDT-HiLL with its optimal parameter setting for CC-JRM under Q75, i.e.,  $p=0.7$  (*DCDT-HiLL-pro*), and then its security performance is indeed improved as shown in Table 5. The other is that the DCDT-HiLL and BET-HiLL schemes modify too much mid-to-high frequency coefficients than J-UNIWARD and GUED to resist the detection of JPEG phase-aware feature-based steganalyzers, e.g., GFR and SCA-GFR, which would make their embedding traces easier exposed to steganalyzer CC-JRM. For validation, we remove the integral components of CC-JRM, which are sensitive to the changes of the statistics of DCT modes, especially the mid-to-high frequency modes, and the resulting feature is de-

Table 5: Classification error probability  $P_E$  (in %) of the involved JPEG steganographic schemes for CC-JRM, GFR and SCA-GFR versus relative payloads on BOSSBaseJ75.

Steganalyzer	Scheme	Relative payload $\alpha$ (bpnzAC)				
		0.1	0.2	0.3	0.4	0.5
CC-JRM <sup>3rd</sup>	UERD	45.89	38.93	30.91	23.22	16.53
	J-UNIWARD	47.10	41.25	34.00	26.83	19.29
	GUED	47.27	41.33	34.83	27.18	20.08
	BET-HiLL	46.76	40.57	32.71	24.74	17.36
	DCDT-HiLL	46.14	39.53	31.44	23.39	16.62
	<i>DCDT-HiLL-pro</i>	<i>46.62</i>	<i>40.10</i>	<i>32.25</i>	<i>24.10</i>	<i>17.02</i>
GFR <sup>2nd</sup>	UERD	39.97	27.80	18.01	10.47	6.05
	J-UNIWARD	41.38	28.96	18.29	10.46	5.58
	GUED	41.57	29.93	19.13	11.14	6.10
	BET-HiLL	41.95	31.32	21.18	13.38	7.56
	DCDT-HiLL	40.85	29.33	18.62	10.97	6.27
	<i>DCDT-HiLL-pro</i>	<i>41.30</i>	<i>29.95</i>	<i>19.61</i>	<i>12.06</i>	<i>6.80</i>
SCA-GFR <sup>1st</sup>	UERD	32.14	21.03	13.64	8.57	5.04
	J-UNIWARD	35.98	23.35	14.15	8.03	4.47
	GUED	36.55	23.20	13.59	7.85	4.42
	BET-HiLL	34.71	22.55	13.98	8.06	4.28
	DCDT-HiLL	36.85	24.51	15.51	9.49	5.95

† the detectability of the steganalyzers in Table 5 and 6 follows: SCA-GFR > GFR ≫ CC-JRM.

⊥ The darkness of the background in the Table 5 and 6 indicates the security of steganographic schemes, i.e., the darker the background, the higher the security of steganographic scheme.

Table 6: Classification error probability  $P_E$  (in %) of the involved JPEG steganographic schemes for CC-JRM, GFR and SCA-GFR versus relative payloads on BOSSBaseJ95.

Steganalyzer	Scheme	Relative payload $\alpha$ (bpnzAC)				
		0.1	0.2	0.3	0.4	0.5
CC-JRM <sup>3rd</sup>	UERD	49.04	46.57	42.02	35.97	29.04
	J-UNIWARD	49.55	47.94	45.07	40.76	35.13
	GUED	49.57	48.13	45.63	42.15	37.16
	BET-HiLL	49.51	47.74	44.92	40.56	34.30
	DCDT-HiLL	49.44	47.84	45.05	40.12	33.53
GFR <sup>2nd</sup>	UERD	46.07	39.62	32.45	24.68	17.84
	J-UNIWARD	47.55	42.74	35.88	28.17	20.54
	GUED	47.24	42.78	36.23	29.42	23.21
	BET-HiLL	48.01	43.91	38.51	31.82	25.29
	DCDT-HiLL	47.57	43.40	37.90	31.35	23.84
SCA-GFR <sup>1st</sup>	UERD	44.03	37.91	31.45	25.47	19.32
	J-UNIWARD	46.17	40.49	33.77	26.63	20.38
	GUED	44.97	37.94	30.98	24.99	19.62
	BET-HiLL	46.31	40.65	34.99	28.85	22.78
	DCDT-HiLL	46.22	40.60	34.95	28.53	23.98

noted as crop-CC-JRM-17,270D. Subsequently, applying the crop-CC-JRM to detect the tested schemes at 0.4 bpnzAC under Q75 and Q95, and the comparison results are shown in Table 7. It is observed that the security performance improvements of DCDT-HiLL can reach 2.42% and 2.85% at Q75 and Q95, respectively. And so is the BET-HiLL. While for J-UNIWARD and GUED, the improvements are relatively much less. Therefore, the newly emerged JPEG phase-aware feature-based steganalyzers, e.g., GFR and SCA-GFR, are not compatible with the conventional JPEG steganalyzer CC-JRM. Considering that both GFR and its selection-channel aware variant SCA-GFR are currently the most powerful hand-craft JPEG steganalyzers, and the proposed DCDT-HiLL is tailored for them by inevitably sacrificing the performance against CC-JRM to some extents.

Table 7: Classification error probability  $P_E$  (in %) of J-UNIWARD, GUED, BET-HiLL and DCDT-HiLL for CC-JRM and crop-CC-JRM at 0.4 bpnzAC under Q75 and Q95. ( $\Delta P_E$  is the difference of  $P_E$  between crop-CC-JRM and CC-JRM.)

Scheme	CC-JRM		crop-CC-JRM		$\Delta P_E$	
	Q75	Q95	Q75	Q95	Q75	Q95
J-UNIWARD	26.83	40.76	26.98	41.36	+0.15	+0.60
GUED	27.18	42.15	28.47	43.29	+1.29	+1.14
BET-HiLL	24.74	40.56	27.37	43.32	<b>+2.63</b>	<b>+2.76</b>
DCDT-HiLL	23.39	40.12	25.81	42.97	<b>+2.42</b>	<b>+2.85</b>

### 3.5. Practical evaluation of computational complexity

In this subsection, we further evaluate the computational complexity of our proposed DCDT-HiLL compared to UERD, J-UNIWARD, GUED, and BET-HiLL in terms of computation time (CmpTime). Considering that all the involved JPEG steganographic schemes are implemented under the same framework of STC-based minimal distortion embedding, i.e., the computation of embedding cost for each quantized DCT coefficient + STC encoding, therefore the major difference among them lies in the

adopted distortion cost function. And it is quite reasonable to evaluate the computational complexity of the tested schemes by comparing the practical computation times in the calculation of their distortion costs. In our experiment, we calculate the average CmpTimes of the distortion costs for UERD, J-UNIWARD, GUED, BET-HiLL, and DCDT-HiLL, over 2,000 JPEG images randomly selected from BOSSBaseJ75 and BOSSBaseJ95, respectively, using MATLAB 8.2 on a 3.0 GHz Intel Core i5-7400 CPU with 8GB memory. The results are summarized in Table 8. It is observed that: 1) the proposed DCDT-HiLL is extremely time-efficient, its CmpTime is one, two, and three orders of magnitude lower than BET-HiLL, GUED, and J-UNIWARD, respectively; 2) DCDT-HiLL could be implemented in a quite affordable time cost as UERD for practical applications.

Table 8: Average CmpTimes on a 3.0 GHz Intel Core i5-7400 CPU with 8GB memory over 2,000 JPEG images of  $512 \times 512 \times 8$  bits under Q75 and Q95 in calculation of distortion costs for UERD, J-UNIWARD, GUED, BET-HiLL (0.4bpnzAC) and DCDT-HiLL. The unit of time is second (s).

QF	Average computation times (s)				
	UERD	J-UNIWARD	GUED	BET-HiLL	DCDT-HiLL
75	<b>0.046</b>	12.12	1.28	0.789	<b>0.054</b>
95	<b>0.051</b>	12.04	1.29	0.906	<b>0.053</b>

### 3.6. Further study on the applicability of our proposed scheme

Recalling the optimal exponent parameter  $p$  in the proposed distortion function is obtained experimentally from the specific image database BOSSBase ver1.01 [24] at Q75 and Q95, therefore the applicability of our proposed scheme for other image database and QFs remains to be further investigated.

- Performance of the proposed DCDT-HiLL on other image database

We use image database BOWS2 [31] to evaluate the applicability of our proposed scheme with the exponent parameter  $p$  trained on BOSSBase. For brevity, we only compare the empirical security performance of the proposed DCDT-HiLL with J-UNIWARD, which is one of the most popular JPEG steganographic

schemes, using the most effective steganalyzer SCA-GFR on BOWS2J75 and BOWS2J95, which are shown in Table 9. Likewise, the proposed DCDT-HiLL shows an overall superior performance than J-UNIWARD as done in BOSSBase, indicating the effectiveness of our proposed DCDT-HiLL on various databases.

Table 9: Classification error probability  $P_E$  (in %) of J-UNIWARD and the proposed DCDT-HiLL against steganalyzer SCA-GFR on BOWS2J75 and BOWS2J95.

QF	Scheme	Relative payload $\alpha$ (bpnzAC)				
		0.1	0.2	0.3	0.4	0.5
75	J-UNIWARD	37.94	25.06	15.49	8.77	4.59
	DCDT-HiLL	<b>38.60</b>	<b>26.37</b>	<b>16.45</b>	<b>9.47</b>	<b>5.20</b>
95	J-UNIWARD	47.04	42.14	35.30	28.05	21.40
	DCDT-HiLL	<b>47.06</b>	<b>42.18</b>	<b>35.95</b>	<b>29.27</b>	<b>22.08</b>

- Performance of the proposed DCDT-HiLL on other QFs

In section 3.2, only the optimal exponent parameters  $p$  in the proposed DCDT-HiLL for Q75 and Q95 are investigated, while for other QFs, the empirical rule to determine the corresponding  $p$  should be developed, because it is impractical to search for the optimal  $p$  for each QF. Note that SCA-GFR is the most effective JPEG steganalyzer and the performance of the proposed DCDT-HiLL with the same parameter setting as SCA-GFR's for other steganalyzers won't change much, then referring to the procedure of determination on the optimal  $p$  in section 3.2, we can easily obtain the optimal parameters  $p$  for DCDT-HiLL at Q80, Q85, and Q90 in resisting the detection of SCA-GFR as shown in Table 10.

Then, we can build an empirical rule for parameter  $p$  by using an linear regression model w.r.t.  $p$  and QF according to the results in Table 10, i.e.,

$$p = 0.02 \times (\text{QF} - 75) + 0.48. \quad (9)$$

Table 10: The optimal parameter  $p$  in DCDT-HiLL for the most effective steganalyzer SCA-GFR at Q75, Q80, Q85, Q90 and Q95.

Steganalyzer	QF				
	75	80	85	90	95
SCA-GFR	0.5	0.6	0.6	0.8	0.9

The QF in Eq. (9) is kept in the interval  $[75, 95]^4$ , and as for the one outside this interval, we can follow this procedure and rebuild a new regression model as well. Subsequently, we further compare the empirical security performance of our proposed DCDT-HiLL with J-UNIWARD for steganalyzer SCA-GFR on BOSSBaseJ80, BOSSBaseJ85, and BOSSBaseJ90 using this empirical rule. Referring to the results in Table 11, it is observed that on various QFs, our proposed DCDT-HiLL exhibits better performance than J-UNIWARD as well.

Table 11: Classification error probability  $P_E$  (in %) of J-UNIWARD and the proposed DCDT-HiLL against steganalyzer SCA-GFR on BOSSBaseJ80, BOSSBaseJ85 and BOSSBaseJ90.

QF	Scheme	Relative payload $\alpha$ (bpnzAC)				
		0.1	0.2	0.3	0.4	0.5
80	J-UNIWARD	38.06	25.88	16.71	10.14	5.92
	DCDT-HiLL	<b>38.25</b>	<b>26.57</b>	<b>17.57</b>	<b>11.14</b>	<b>6.99</b>
85	J-UNIWARD	39.41	28.16	19.10	12.15	7.51
	DCDT-HiLL	<b>39.57</b>	<b>28.89</b>	<b>20.01</b>	<b>13.58</b>	<b>8.84</b>
90	J-UNIWARD	<b>42.72</b>	33.31	24.44	17.33	11.85
	DCDT-HiLL	42.26	<b>33.38</b>	<b>25.48</b>	<b>18.69</b>	<b>13.09</b>

<sup>4</sup>The reason for the selection of interval  $[75, 95]$  is that the QFs in this interval are most commonly used in our lives.

### 3.7. Evaluation on the mutually dependent embedding extension of our proposed scheme

To verify the claim in section 3.4 that the mutually dependent embedding of our proposed DCDT-HiLL helps to improve the performance, especially at Q75, we then compare the performance of the mutually dependent version DCDT-HiLL<sub>ud</sub> with the original DCDT-HiLL on BOSSBaseJ75 at 0.2 bpnzAC against the detection of CC-JRM, GFR and SCA-GFR with their corresponding optimal parameter  $p$  setting. Since the computational complexity of DCDT-HiLL<sub>ud</sub> is exponentially increased with  $n_k$ , we make a constraint that if  $n_k$  is large than a threshold  $T$ , then this block will be skipped for distortion cost updating. In this paper, we set the threshold  $T$  and penalty factor  $v$  in Eq. (8) as 10, and the results are summarized in Table 12. It is observed that the performance of the proposed DCDT-HiLL is indeed improved by incorporating the mutually dependent embedding strategy.

Table 12: Classification error probability  $P_E$  (in %) of DCDT-HiLL and DCDT-HiLL<sub>ud</sub> for CC-JRM, GFR and SCA-GFR on BOSSBaseJ75 at 0.2 bpnzAC.

Scheme	Steganalyzer		
	CC-JRM	GFR	SCA-GFR
DCDT-HiLL	40.10	29.95	24.51
DCDT-HiLL <sub>ud</sub>	<b>40.46</b>	<b>30.69</b>	<b>25.30</b>

## 4. Conclusion

In this paper, a novel Distortion Cost Domain Transformation (DCDT) based JPEG steganographic scheme is proposed, which formulates the JPEG steganography as the optimization problem of minimizing the overall distortion cost in its decompressed spatial domain, aiming to maintain the statistical undetectability in both spatial and DCT domains. The proposed DCDT scheme transforms the decompressed  $8 \times 8$  spatial pixel block distortion costs into DCT domain by incorporating a generalized domain distortion cost transformation function in terms of the embedding changes in decompressed

$8 \times 8$  pixel block and the adopted distortion cost function in spatial domain. The domain distortion cost transformation function is developed with an exponential model to further maintain the statistical undetectability in both spatial and JPEG domains. Extensive experiments have been carried out, which demonstrates that the proposed DCDT-HiLL outperforms other existing SOTA JPEG steganographic schemes, including UERD, J-UNIWARD, and GUED, in resisting the detection of newly emerged phase-aware JPEG steganalyzers, e.g., GFR and SCA-GFR. In addition, the proposed DCDT-HiLL can rival the SOTA BET-HiLL with one order of magnitude lower computational complexity as well. The experimental results also show that our proposed DCDT-HiLL has strong applicability, and its security performance can be further improved by incorporating the mutually dependent embedding strategy. Overall, the proposed DCDT-HiLL can not only improve the performance against JPEG phase-aware feature-based steganalyzers but also broaden the applications of existing image steganographic schemes in spatial domain.

### **Acknowledgement**

This work was supported in part by the National Natural Science Foundation of China under Grant U1736215, Grant U1936212, and Grant 61772573.

### **References**

### **References**

- [1] K. D, The history of steganography, in: Anderson R. (eds) Information Hiding. IH 1996. LNCS 1174, Springer, Berlin, Heidelberg, 1996, pp. 1 – 5. doi:10.1007/3-540-61996-8\_27.
- [2] T. Pevný, J. Fridrich, Benchmarking for steganography, in: Solanki K., Sullivan K., Madhow U. (eds) Information Hiding. IH 2008. LNCS 5284, Springer, Berlin, Heidelberg, 2008, pp. 251 – 267. doi:10.1007/978-3-540-88961-8\_18.

- [3] L. Li, W. Zhang, C. Qin, K. Chen, W. Zhou, N. Yu, Adversarial batch image steganography against cnn-based pooled steganalysis, *Signal Processing* 181 (2021) 107920. doi:10.1016/j.sigpro.2020.107920.
- [4] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, N. Yu, Robust adaptive steganography based on generalized dither modulation and expanded embedding domain, *Signal Processing* 168 (2020) 107343. doi:10.1016/j.sigpro.2019.107343.
- [5] T. Qiao, S. Wang, X. Luo, Z. Zhu, Robust steganography resisting jpeg compression by improving selection of cover element, *Signal Processing* 183 (2021) 108048. doi:10.1016/j.sigpro.2021.108048.
- [6] Y. Zhang, C. Qin, W. Zhang, F. Liu, X. Luo, On the fault-tolerant performance for a class of robust image steganography, *Signal Processing* 146 (2018) 99 – 111. doi:10.1016/j.sigpro.2018.01.011.
- [7] Y. Su, C. Zhang, C. Zhang, A video steganalytic algorithm against motion-vector-based steganography, *Signal Processing* 91 (8) (2011) 1901 – 1909. doi:10.1016/j.sigpro.2011.02.012.
- [8] Y. Wang, Y. Cao, X. Zhao, Minimizing embedding impact for h.264 steganography by progressive trellis coding, *IEEE Transactions on Information Forensics and Security* 16 (2021) 333 – 345. doi:10.1109/TIFS.2020.3013523.
- [9] X. Yi, K. Yang, X. Zhao, Y. Wang, H. Yu, Ahcm: Adaptive huffman code mapping for audio steganography based on psychoacoustic model, *IEEE Transactions on Information Forensics and Security* 14 (8) (2019) 2217 – 2231. doi:10.1109/TIFS.2019.2895200.
- [10] Y. Huang, S. Tang, J. Yuan, Steganography in inactive frames of voip streams encoded by source codec, *IEEE Transactions on Information Forensics and Security* 6 (2) (2011) 296 – 306. doi:10.1109/TIFS.2011.2108649.
- [11] B. Li, M. Wang, J. Huang, X. Li, A new cost function for spatial image steganography, in: *2014 IEEE International Conference on Image Processing (ICIP), 2014*, pp. 4206 – 4210. doi:10.1109/ICIP.2014.7025854.

- [12] W. Su, J. Ni, X. Hu, J. Fridrich, Image steganography with symmetric embedding using gaussian markov random field model, *IEEE Transactions on Circuits and Systems for Video Technology* 31 (3) (2021) 1001 – 1015. doi:10.1109/TCSVT.2020.3001122.
- [13] L. Guo, J. Ni, Y. Q. Shi, Uniform embedding for efficient JPEG steganography, *IEEE Transactions on Information Forensics and Security* 9 (5) (2014) 814 – 825. doi:10.1109/TIFS.2014.2312817.
- [14] L. Guo, J. Ni, W. Su, C. Tang, Y. Q. Shi, Using statistical image model for JPEG steganography: Uniform embedding revisited, *IEEE Transactions on Information Forensics and Security* 10 (12) (2015) 2669 – 2680. doi:10.1109/TIFS.2015.2473815.
- [15] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, *EURASIP Journal on Information Security* 2014 (1) (2014) 1 – 13. doi:10.1186/1687-417X-2014-1.
- [16] W. Su, J. Ni, X. Li, Y. Q. Shi, A new distortion function design for jpeg steganography using the generalized uniform embedding strategy, *IEEE Transactions on Circuits and Systems for Video Technology* 28 (12) (2018) 3545 – 3549. doi:10.1109/TCSVT.2018.2865537.
- [17] X. Hu, J. Ni, Y. Q. Shi, Efficient jpeg steganography using domain transformation of embedding entropy, *IEEE Signal Processing Letters* 25 (6) (2018) 773 – 777. doi:10.1109/LSP.2018.2818674.
- [18] Y. Pan, J. Ni, W. Su, Improved uniform embedding for efficient jpeg steganography, in: Sun X., Liu A., Chao HC., Bertino E. (eds) *Cloud Computing and Security. ICCCS 2016. LNCS 10039*, Springer, Cham, 2016, pp. 125 – 133. doi:10.1007/978-3-319-48671-0\_12.
- [19] T. Filler, J. Judas, J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, *IEEE Transactions on Information Forensics and Security* 6 (3) (2011) 920 – 935. doi:10.1109/TIFS.2011.2134094.

- [20] X. Song, F. Liu, C. Yang, X. Luo, Y. Zhang, Steganalysis of adaptive JPEG steganography using 2D Gabor filters, in: Proc. of the 3rd ACM Workshop on Information Hiding and Multimedia Security, 2015, pp. 15 – 23. doi:10.1145/2756601.2756608.
- [21] T. Denemark, M. Boroumand, J. Fridrich, Steganalysis features for content-adaptive JPEG steganography, IEEE Transactions on Information Forensics and Security 11 (8) (2016) 1736 – 1746. doi:10.1109/TIFS.2016.2555281.
- [22] V. Holub, J. Fridrich, Designing steganographic distortion using directional filters, in: 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012, pp. 234 – 239. doi:10.1109/WIFS.2012.6412655.
- [23] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security 11 (2) (2016) 221 – 234. doi:10.1109/TIFS.2015.2486744.
- [24] P. Bas, T. Filler, T. Pevný, Break our steganographic system: the ins and outs of organizing BOSS, in: Filler T., Pevný T., Craver S., Ker A. (eds) Information Hiding. IH 2011. LNCS 6958, Springer, Berlin, Heidelberg, 2011, pp. 59 – 70. doi:10.1007/978-3-642-24178-9\_5.
- [25] J. L. Myers, A. D. Well, Research Design and Statistical Analysis, 2nd Edition, Lawrence Erlbaum Associates, 2003.
- [26] B. Li, M. Wang, X. Li, S. Tan, J. Huang, A strategy of clustering modification directions in spatial image steganography, IEEE Transactions on Information Forensics and Security 10 (9) (2015) 1905 – 1917. doi:10.1109/TIFS.2015.2434600.
- [27] T. Denemark, J. Fridrich, Improving steganographic security by synchronizing the selection channel, in: Proc. of the 3rd ACM Workshop on Information Hiding and Multimedia Security, 2015, pp. 5 – 14. doi:10.1145/2756601.2756620.

- [28] X. Hu, J. Ni, W. Su, J. Huang, Model-based image steganography using asymmetric embedding scheme, *Journal of Electronic Imaging* 27 (4). doi:10.1117/1.JEI.27.4.043023.
- [29] W. Zhang, Z. Zhang, L. Zhang, H. Li, N. Yu, Decomposing joint distortion for adaptive steganography, *IEEE Transactions on Circuits and Systems for Video Technology* 27 (10) (2017) 2274 – 2280. doi:10.1109/TCSVT.2016.2587388.
- [30] W. Li, W. Zhang, K. Chen, W. Zhou, N. Yu, Defining joint distortion for jpeg steganography, in: *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018, pp. 5 – 16. doi:10.1145/3206004.3206008.
- [31] T. P. Bas, Furon, Bows-2 (july 2007).  
URL <http://bows2.gipsa-lab.inpg.fr>
- [32] Phil sallee's matlab jpeg toolbox.  
URL <http://dde.binghamton.edu/download/stegoalgorithms/>
- [33] J. Kodovský, J. Fridrich, Steganalysis of JPEG images using rich models, in: *Proc. SPIE 8303, Media Watermarking, Security, and Forensics 2012*, 83030A, 2012, pp. 0A 1 – 13. doi:10.1117/12.907495.
- [34] J. Kodovský, J. Fridrich, V. Holub, Ensemble classifiers for steganalysis of digital media, *IEEE Transactions on Information Forensics and Security* 7 (2) (2012) 432 – 444. doi:10.1109/TIFS.2011.2175919.