symmetry

MDPI

Article

Domain Transformation of Distortion Costs for Efficient JPEG Steganography with Symmetric Embedding

Yuanfeng Pan [1] and Jiangqun Ni [2,3,*]

[1] School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China; panyuanf@mail2.sysu.edu.cn
[2] School of Cyber Science and Technology, Sun Yat-sen University, Shenzhen 518000, China
[3] Department of New Networks, Peng Cheng Laboratory, Shenzhen 518000, China
* Correspondence: issjqni@mail.sysu.edu.cn

Abstract: Nowadays, most image steganographic schemes embed secret messages by minimizing a well-designed distortion cost function for the corresponding domain, i.e., the spatial domain for spatial image steganography or the JPEG (Joint Photographic Experts Group) domain for JPEG image steganography. In this paper, we break the boundary between these two types of schemes by establishing a theoretical link between the distortion costs in the spatial domain and those in the JPEG domain and thus propose a scheme for domain transformations of distortion costs for efficient JPEG steganography with symmetric embedding, which can directly convert the spatial distortion cost into its JPEG counterpart. Specifically, by formulating the distortion cost function for JPEG images in the decompressed spatial domain, a closed-form expression for a distortion cost cross-domain transformation is derived theoretically, which precisely characterizes the conversion from the distortion costs obtained by existing spatial steganographic schemes to those applied in JPEG steganography. Experimental results demonstrate that the proposed method outperforms other advanced JPEG steganographic schemes, e.g., JUNIWARD (JPEG steganography with Universal Wavelet Relative Distortion), JMiPOD (JPEG steganography by Minimizing the Power of the Optimal Detector), and DCDT (Distortion Cost Domain Transformation), in resisting the detection of various advanced steganalyzers.

Keywords: steganography with symmetric embedding; JPEG image; distortion cost function; domain transformation

check for updates

Citation: Pan, Y.; Ni, J. Domain Transformation of Distortion Costs for Efficient JPEG Steganography with Symmetric Embedding. *Symmetry* **2024**, *16*, 575. https://doi.org/10.3390/sym16050575

Academic Editors: Jie Yang and Sergei D. Odintsov

Received: 12 March 2024
Revised: 11 April 2024
Accepted: 26 April 2024
Published: 7 May 2024

1. Introduction

Image steganography is the science and art of covert communication, which embeds secret messages into cover images to generate the corresponding stego images that can be transmitted through open channels without drawing suspicion [1–6]. By using the advantages of steganography, people can achieve secure communication without being detected by network monitors, and it is worth noting that the steganography is not the same as but is supplementary to cryptography, because the former emphasizes the undetectability of communication while the latter emphasizes the secrecy of data. In the past decade, the most common image steganographic scheme has been the distortion minimization framework [7], since the stego image can be statistically indistinguishable from the cover image by minimizing the embedding distortion in this framework.

The distortion minimization framework consists of two components: (1) the design of the distortion cost function and (2) the method of steganographic coding. Steganographic coding aims to minimize the distortion cost function for a given embedding payload, and state-of-the-art coding methods, e.g., STCs (syndrome trellis codes) [8] and SPCs (steganographic polar codes) [9], have already approached the theoretical limit of coding efficiency. Therefore, researchers have focused on improving the design of the distortion cost function, which can properly quantify the distortion cost of modifying each element of the cover image. The following equation demonstrates the general construction of this framework:

$$
\begin{aligned}
Emb(\mathbf{X}, \mathbf{m}) &= \arg\min_{\mathbf{Y} \in \mathbf{C}(\mathbf{m})} D(\mathbf{X}, \mathbf{Y}) \\
\mathbf{H} \cdot \mathbf{Y} &= \mathbf{m}
\end{aligned} \tag{1}
$$

where **X**, **Y** and **m** represent the cover image, stego image and the secret messages, respectively. $Emb(\cdot)$ denotes the embedding conducted by the steganographic codes, $D(\cdot)$ represents the distortion of transferring the cover into a stego image, and **H** refers to the parity-check matrix of code **C**, while $\mathbf{C}(\mathbf{m})$ is the coset corresponding to syndrome **m**.

At present, various steganographic schemes have been proposed for designing distortion cost functions with symmetric embedding, which can be mainly categorized into three groups: (1) **heuristically designed schemes,** such as WOWs (Wavelet-Obtained Weights) [10], UNIWARD (Universal Wavelet Relative Distortion) [11], HiLL (High-pass, Low-pass, and Low-pass) [12], QMP (Quaternion Magnitude-Phase) [13], UERD (Uniform Embedding Revisited Distortion) [14] and GUED (Generalized Uniform Embedding Distortion) [15]; (2) **statistical-model-based schemes**, such as MG (Multivariate Gaussian) [16], MiPOD (Minimizing the Power of the Optimal Detector) [17] and JMiPOD (JPEG steganography by MiPOD) [18]; and (3) **deep-learning-based schemes**, such as UT-GAN (U-net and double-Tanh framework using Generative Adversarial Network) [19], SPAR-RL (Steganographic Pixel-wise Actions and Rewards with Reinforcement Learning) [20], PICO-RL (Payload-Independent Cost learning framework using RL) [21], JS-GAN (JPEG Steganography using a GAN) [22] and JEC-RL (JPEG Embedding Cost with RL) [23]. It is worth noting that each of these designs can only be implemented on a specific type of image format, either spatial or JPEG; e.g., HiLL is specifically designed for spatial images and cannot be used for JPEG images. Furthermore, there are only a limited number of research works that have investigated the relationship between spatial and JPEG steganography, such as BET (Block Entropy Transformation) [24] and DCDT (Distortion Cost Domain Transformation) [25]. BET utilizes the block embedding entropy as the proxy for connecting the spatial and JPEG domains, and achieves a satisfactory security performance of JPEG distortion designed from spatial distortion. However, it suffers from a high computational complexity and lacks a precise theoretical deduction regarding the mapping between embedding entropy in different domains. Although DCDTs could be implemented much faster than BETs, they are still heuristically designed and lack theoretical guarantees.

Considering that JPEG images are more widely used on the internet than spatial images, the development of effective JPEG distortion cost functions is crucial for practical steganographic applications. In this regard, a distortion cost transformation strategy, such as DCDT, has practical significance as it can construct novel JPEG distortion designs by exploiting well-established spatial steganographic schemes. Typically, this strategy offers two key advantages for enhancing the security of JPEG steganography: (1) The availability of diverse and effective JPEG distortion cost functions increases the difficulty of detection for steganalyzers, thereby enhancing steganographic security. (2) The utilization of well-designed spatial steganographic schemes helps to improve security by reducing the spatial artifacts introduced by the embedding modifications in the JPEG domain, considering that the accurate detection of JPEG steganography is mostly achieved with steganalysis features that are extracted from the spatial domain [26–28] rather than from the JPEG domain [29].

In order to establish the relationship between the spatial and JPEG steganography, this paper conducts a theoretical investigation into the transformation of distortion costs from the spatial to the JPEG domain. Specifically, via the design of the distortion cost function for JPEG steganography in the decompressed spatial domain, a closed-form expression for the distortion cost cross-domain transformation is derived theoretically through simple yet efficient arithmetic operations. This expression allows for the direct conversion of the distortion costs computed by existing spatial steganographic schemes, e.g., HiLL, MiPOD, and SUNIWARD [11], into the distortion costs for the JPEG domain. Furthermore, the transformation expression is executed in a block-wise manner, ensuring computational efficiency. Finally, experiments are carried out to validate the effectiveness of the proposed method in terms of both security and computational complexity using the BOSSBase [30] dataset. The results demonstrate that the proposed JPEG steganographic scheme is computationally efficient and outperforms the competing one, i.e., DCDT, and other advanced JPEG approaches, i.e., JMiPOD and JUNIWARD [11], for resisting the detection of various modern steganalyzers.

The contributions of this paper are summarized as follows:

- A deep investigation into the transformation of distortion costs from the spatial to the JPEG domain is conducted.
- A simple yet efficient closed-form expression for the distortion cost cross-domain transformation is developed.
- The transformation expression is executed in a block-wise manner, ensuring computational efficiency.
- Comprehensive experiments validate the effectiveness of the proposed scheme in terms of both steganographic security and computational complexity.

The rest of this paper is organized as follows. In Section 2, the common notations and preliminaries on JPEG steganography are introduced. Then, the proposed distortion cost cross-domain transformation method for JPEG steganography is elaborated in Section 3. Subsequently, we present the experimental results and analysis in Section 4. Finally, the paper is concluded in Section 5.

2. Preliminaries

2.1. Notations and Basic Concepts

Throughout this paper, boldface symbols are used to represent matrices and italic font with indices denotes the elements within a matrix. The notation [Z] is reserved for the Iverson bracket, where [Z] = 1 when Z is true and otherwise [Z] = 0.

Specifically, JPEG grayscale cover and stego images are denoted as $\mathbf{X} = \left(x_{k,l}^{m,n}\right)^{n_1 \times n_2}$ and $\mathbf{Y} = \left(y_{k,l}^{m,n}\right)^{n_1 \times n_2}$, respectively, where n_1 and n_2 are the height and width of the image and are both assumed to be multiples of eight for a simpler technical description. In addition, the range of indices is $1 \leq m \leq n_1/8$, $1 \leq n \leq n_2/8$, $0 \leq k, l \leq 7$. Note that $x_{k,l}^{m,n}$ (or $y_{k,l}^{m,n}$) is the $(8 \times (m-1) + k + 1, 8 \times (n-1) + l + 1)$-th element in **X** (or **Y**), which corresponds to the DCT (Discrete Cosine Transform) coefficient in the (k, l)-th DCT mode of the (m, n)-th DCT block.

The (k, l)-th DCT basis [31], $0 \leq k, l \leq 7$, is an 8×8 matrix $\mathbf{f}^{k,l} = \left(f_{i,j}^{k,l}\right)^{8\times 8}$, $0 \leq i, j \leq 7$, and defined as

$$f_{i,j}^{k,l} = \frac{w_k w_l}{4} \cos \frac{\pi k(2i+1)}{16} \cos \frac{\pi l(2j+1)}{16}, \tag{2}$$

where $w_0 = 1/\sqrt{2}$, $w_k = 1$ for $k > 0$.

By decompressing the DCT coefficients in the (m, n)-th block of **X**, a corresponding spatial block of 8×8 pixels is obtained [31], in which pixel $\hat{x}_{i,j}^{m,n}$ is calculated by

$$\hat{x}_{i,j}^{m,n} = \sum_{k=0}^{7} \sum_{l=0}^{7} f_{i,j}^{k,l} \, q_{k,l} \, x_{k,l}^{m,n}, \tag{3}$$

where $q_{k,l}$ is the quantization step in the JPEG luminance quantization matrix. After decompressing all DCT blocks in **X**, we can obtain a spatial (decompressed JPEG) image, denoted as $\hat{\mathbf{X}} = \left(\hat{x}_{i,j}^{m,n}\right)^{n_1 \times n_2}$.

2.2. Distortion Measure

Under the distortion minimization framework [32], the primary objective of JPEG image steganography is to design a distortion cost function, which is denoted as $D(\mathbf{X},\mathbf{Y})$ and can be calculated as

$$D(\mathbf{X},\mathbf{Y}) = \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{k=0}^{7}\sum_{l=0}^{7}\rho\left(t_{k,l}^{m,n}\right)\left[x_{k,l}^{m,n} \neq y_{k,l}^{m,n}\right], \tag{4}$$

where $\rho\left(t_{k,l}^{m,n}\right)$ is the additive distortion cost that evaluates the impact of modifying the DCT coefficient $x_{k,l}^{m,n}$ to $y_{k,l}^{m,n} = x_{k,l}^{m,n} + t_{k,l}^{m,n}$, and the modification $t_{k,l}^{m,n}$ attains values in $\{-1,0,+1\}$ for ternary embedding. Generally, the modification impacts are considered to exhibit symmetry, i.e., $\rho\left(t_{k,l}^{m,n} = +1\right) = \rho\left(t_{k,l}^{m,n} = -1\right) = \rho_{k,l}^{m,n}$, and $\rho\left(t_{k,l}^{m,n} = 0\right) = 0$ signifies that no distortion cost is incurred when the DCT coefficient remains unmodified. We note that ternary symmetric embedding is adopted in this paper for its universality. Therefore, $D(\mathbf{X},\mathbf{Y})$ in Equation (4) can also be expressed as

$$D(\mathbf{X},\mathbf{Y}) = \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{k=0}^{7}\sum_{l=0}^{7}\rho_{k,l}^{m,n}\left|y_{k,l}^{m,n} - x_{k,l}^{m,n}\right|. \tag{5}$$

For a given message with length L, minimizing the average embedding distortion can be formulated as the following optimization problem with a payload constraint [7]:

$$\min_{\boldsymbol{\beta}} E_{\boldsymbol{\beta}}(D) = \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{k=0}^{7}\sum_{l=0}^{7}\rho_{k,l}^{m,n}\beta_{k,l}^{m,n}, \tag{6}$$

$$\text{subject to} \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{k=0}^{7}\sum_{l=0}^{7}H\left(\beta_{k,l}^{m,n}\right) = L, \tag{7}$$

where $\beta_{k,l}^{m,n} \in \boldsymbol{\beta}$ is the embedding modification probability of modifying $x_{k,l}^{m,n}$ to $y_{k,l}^{m,n} = x_{k,l}^{m,n} + 1$ or $y_{k,l}^{m,n} = x_{k,l}^{m,n} - 1$, and $H(x) = -2x\log x - (1-2x)\log(1-2x)$ is the entropy function for ternary symmetric embedding. Following the maximum entropy criterion, when $\beta_{k,l}^{m,n} = \frac{1}{3}$, $H(\beta_{k,l}^{m,n})$ reaches its maximum value, i.e., $\log_2 3$ bits. Consequently, for a JPEG image of size $n_1 \times n_2$, the maximum embedding capacity is $n_1 \times n_2 \times \log_2 3$ bits. With the optimal $\boldsymbol{\beta}$ derived by Equations (6) and (7), an optimal embedding simulator [33] can be exploited to execute embedding and test the security of a steganographic method.

3. The Proposed Distortion Cost Cross-Domain Transformation Method

For JPEG image steganography, this paper proposes an efficient distortion cost cross-domain transformation method, which is designed to directly convert the distortion costs obtained by spatial steganographic schemes to those used in the JPEG domain. In this section, the motivation and feasibility of the proposed method are first presented. Then, by formulating the distortion cost function for JPEG images in the decompressed spatial domain, a closed-form expression can be derived accordingly, which is the core of the distortion cost cross-domain transformation and will be described in detail.

3.1. Motivation and Feasibility

Currently, most steganographic schemes for digital images are content-adaptive, whether established in the spatial domain or in the JPEG domain. They are essentially designed to restrict the embedding modifications to regions of the cover image with complex content by assigning low distortion costs to these complex regions, which are difficult for steganalyzers to model accurately. This content-adaptive property inspires us to explore the underlying relationship between the spatial distortion costs and the JPEG ones for expanding the applicability of existing steganographic schemes and simultaneously improving the steganographic security. As mentioned in Section 1, considering that the JPEG distortion cost functions have more practical value in steganographic applications than the spatial ones, this paper focuses on the transformation of distortion cost from the spatial to the JPEG domain. Unlike the heuristic design of DCDT, this paper concentrates on the construction of the distortion cost cross-domain transformation in a theoretical derivation.

As we know, the DCT transform in the JPEG compression is performed in non-overlapping 8×8 image blocks, meaning that each DCT block contains the same content information as its corresponding decompressed block. Based on the content adaptivity of the distortion cost, it should be feasible to convert the distortion cost in the decompressed spatial domain into its JPEG counterpart and efficient to implement the conversion in a block-wise manner. To derive the cross-domain transformation of the distortion cost, it is natural to investigate the distortion cost function in different domains as a starting point. In accordance with Section 2.2, the objective of image steganography within the minimal distortion paradigm [7] is to minimize the average embedding distortion under a given payload size constraint, so it is important to properly design the distortion cost function. Referring to Equation (5), the distortion cost function for JPEG images is composed of the distortion costs for the DCT coefficients and the absolute value of the embedding modifications in the JPEG domain. Note that the corresponding embedding changes in the decompressed spatial domain incurred by the embedding modifications in the JPEG domain can easily be obtained due to the linearity of the inverse DCT. Accordingly, the spatial distortion cost for each pixel of the decompressed JPEG image can be evaluated with existing spatial steganographic schemes. By combining the spatial embedding changes and the spatial distortion costs, the distortion cost function for JPEG images can be formulated in the decompressed spatial domain, which enables the possibility of establishing a distortion cost transformation from the spatial to the JPEG domain.

3.2. Expression for the Distortion Cost Cross-Domain Transformation

As mentioned in the above subsection, in order to derive the cross-domain transformation from the spatial distortion cost to the JPEG distortion cost, we propose formulating a JPEG distortion cost function in the decompressed spatial domain. Following the distortion cost function paradigm in Equation (5), the distortion cost function for JPEG images in the decompressed spatial domain, namely $\hat{D}(\mathbf{X}, \mathbf{Y})$, can be defined as follows:

$$\hat{D}(\mathbf{X}, \mathbf{Y}) = \sum_{m=1}^{n_1/8} \sum_{n=1}^{n_2/8} \sum_{i=0}^{7} \sum_{j=0}^{7} \hat{\rho}_{i,j}^{m,n} \left| \hat{y}_{i,j}^{m,n} - \hat{x}_{i,j}^{m,n} \right|, \tag{8}$$

where $\hat{\boldsymbol{\rho}} = \left(\hat{\rho}_{i,j}^{m,n} \right)^{n_1 \times n_2}$ are the spatial distortion costs and can be obtained by applying existing efficient spatial steganographic schemes to the decompressed JPEG image $\hat{\mathbf{X}}$, e.g., SUNIWARD, HiLL, MiPOD, etc. $\left| \hat{y}_{i,j}^{m,n} - \hat{x}_{i,j}^{m,n} \right|$ represents the absolute value of the difference between the pixel values in the decompressed stego and cover images, which is incurred by the embedding modifications $t_{k,l}^{m,n}$ in the JPEG domain. Referring to Equation (3), we have:

$$\begin{aligned} d_{i,j}^{m,n} = \hat{y}_{i,j}^{m,n} - \hat{x}_{i,j}^{m,n} &= \sum_{k=0}^{7} \sum_{l=0}^{7} f_{i,j}^{k,l} \, q_{k,l} \, y_{k,l}^{m,n} - \sum_{k=0}^{7} \sum_{l=0}^{7} f_{i,j}^{k,l} \, q_{k,l} \, x_{k,l}^{m,n} \\ &= \sum_{k=0}^{7} \sum_{l=0}^{7} f_{i,j}^{k,l} \, q_{k,l} \, t_{k,l}^{m,n}. \end{aligned} \tag{9}$$

after substituting Equation (9) into (8). Therefore, the average embedding distortion $E(\hat{D})$ corresponding to $E_{\boldsymbol{\beta}}(D)$ in Equation (6) can be given by

$$E(\hat{D}) = \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{i=0}^{7}\sum_{j=0}^{7}\hat{\rho}_{i,j}^{m,n}\, E\left(\left|d_{i,j}^{m,n}\right|\right). \tag{10}$$

It is obvious to observe that from Equation (10), to tackle $E(\hat{D})$, we need to calculate the expected value of $\left|d_{i,j}^{m,n}\right|$. Unfortunately, $E\left(\left|d_{i,j}^{m,n}\right|\right)$ cannot be computed analytically. To significantly reduce the complexity of computing $E\left(\left|d_{i,j}^{m,n}\right|\right)$, we switch to an upper bound of $\left|d_{i,j}^{m,n}\right|$:

$$\left|d_{i,j}^{m,n}\right| \leq \sum_{k=0}^{7}\sum_{l=0}^{7}\left|f_{i,j}^{k,l}\right| \cdot q_{k,l} \cdot \left|t_{k,l}^{m,n}\right|. \tag{11}$$

Recalling that the embedding modifications $t_{k,l}^{m,n}$ attain values in $\{-1, 0, +1\}$ with probabilities $\{\beta_{k,l}^{m,n}, 1-2\beta_{k,l}^{m,n}, \beta_{k,l}^{m,n}\}$ for ternary symmetric embedding, we thus have:

$$E\left(\left|t_{k,l}^{m,n}\right|\right) = \beta_{k,l}^{m,n}\cdot|-1| + \beta_{k,l}^{m,n}\cdot|+1| = 2\beta_{k,l}^{m,n}. \tag{12}$$

According to Equations (11) and (12), $E\left(\left|d_{i,j}^{m,n}\right|\right)$ can be bounded by

$$E\left(\left|d_{i,j}^{m,n}\right|\right) \leq \sum_{k=0}^{7}\sum_{l=0}^{7}\left|f_{i,j}^{k,l}\right| q_{k,l}\, E\left(\left|t_{k,l}^{m,n}\right|\right) = \sum_{k=0}^{7}\sum_{l=0}^{7} 2\left|f_{i,j}^{k,l}\right| q_{k,l}\, \beta_{k,l}^{m,n}. \tag{13}$$

Hence, using Equation (13), $E(\hat{D})$ in Equation (10) can be bounded as follows:

$$E(\hat{D}) \leq \sum_{m=1}^{n_1/8}\sum_{n=1}^{n_2/8}\sum_{i=0}^{7}\sum_{j=0}^{7}\sum_{k=0}^{7}\sum_{l=0}^{7} 2\left|f_{i,j}^{k,l}\right| q_{k,l}\, \hat{\rho}_{i,j}^{m,n}\, \beta_{k,l}^{m,n} = S_{\boldsymbol{\beta}}(\hat{D}), \tag{14}$$

where $S_{\boldsymbol{\beta}}(\hat{D})$ is used for convenience to denote the upper bound of the average embedding distortion of JPEG steganography in the decompressed spatial domain.

Obviously, by comparing $E_{\boldsymbol{\beta}}(D)$ in Equation (6) and $S_{\boldsymbol{\beta}}(\hat{D})$ in Equation (14), a closed-form expression for converting the spatial distortion costs $\hat{\boldsymbol{\rho}} = \left(\hat{\rho}_{i,j}^{m,n}\right)^{n_1 \times n_2}$ to the JPEG distortion costs $\boldsymbol{\rho} = \left(\rho_{k,l}^{m,n}\right)^{n_1 \times n_2}$ can be derived as

$$\rho_{k,l}^{m,n} = \sum_{i=0}^{7}\sum_{j=0}^{7} 2\left|f_{i,j}^{k,l}\right| q_{k,l}\, \hat{\rho}_{i,j}^{m,n}, \tag{15}$$

where $f_{i,j}^{k,l}$ is obtained by Equation (2), $q_{k,l}$ is the quantization step of (k,l)-th DCT mode, and $\hat{\boldsymbol{\rho}}$ can be directly acquired by using spatial steganographic schemes. It can be observed that Equation (15) has a similar form to Equation (3), which indicates that the proposed transformation method can be efficiently executed in a block-wise manner (this is the same computational demand as decompressing a JPEG image). Once the JPEG distortion costs $\boldsymbol{\rho}$ are computed by Equation (15), the message embedding process can be executed with the near-optimal steganographic codes STCs [33] or SPCs [9]. In summary, the procedure of the proposed distortion cost cross-domain transformation method is presented in Algorithm 1.

Algorithm 1: Distortion cost cross-domain transformation

```
Input: A JPEG image $\mathbf{X} = \left(x_{k,l}^{m,n}\right)^{n_1 \times n_2}$
Output: The JPEG distortion costs $\boldsymbol{\rho} = \left(\rho_{k,l}^{m,n}\right)^{n_1 \times n_2}$ for $\mathbf{X}$
Decompress the JPEG image $\mathbf{X}$ into the spatial domain using Equation (3), and
  denote the spatial (decompressed JPEG) image by $\hat{\mathbf{X}} = \left(\hat{x}_{i,j}^{m,n}\right)^{n_1 \times n_2}$;
Apply an existing spatial steganographic scheme to $\hat{\mathbf{X}}$, e.g., SUNIWARD or HiLL,
  and denote the obtained spatial distortion costs by $\hat{\boldsymbol{\rho}} = \left(\hat{\rho}_{i,j}^{m,n}\right)^{n_1 \times n_2}$;
Compute the JPEG distortion costs $\boldsymbol{\rho}$ using Equation (15),
$\rho_{k,l}^{m,n} = \sum_{i=0}^{7} \sum_{j=0}^{7} 2\left|f_{i,j}^{k,l}\right| q_{k,l}\, \hat{\rho}_{i,j}^{m,n}$ for all non-overlapping $8 \times 8$ blocks $(m,n)$.
```

Additionally, the process of applying the proposed distortion cost cross-domain transformation method in JPEG steganography is shown in Figure 1. In the following sections of this paper, the JPEG steganographic scheme realized by Equation (15) is referred to as JC-A (JPEG distortion costs converted from the spatial distortion costs that are calculated by the spatial steganographic scheme "A"). In specific, JC-SUNI, JC-HiLL, and JC-MiPOD adopt the spatial steganographic schemes SUNIWARD, HiLL, and MiPOD, respectively.

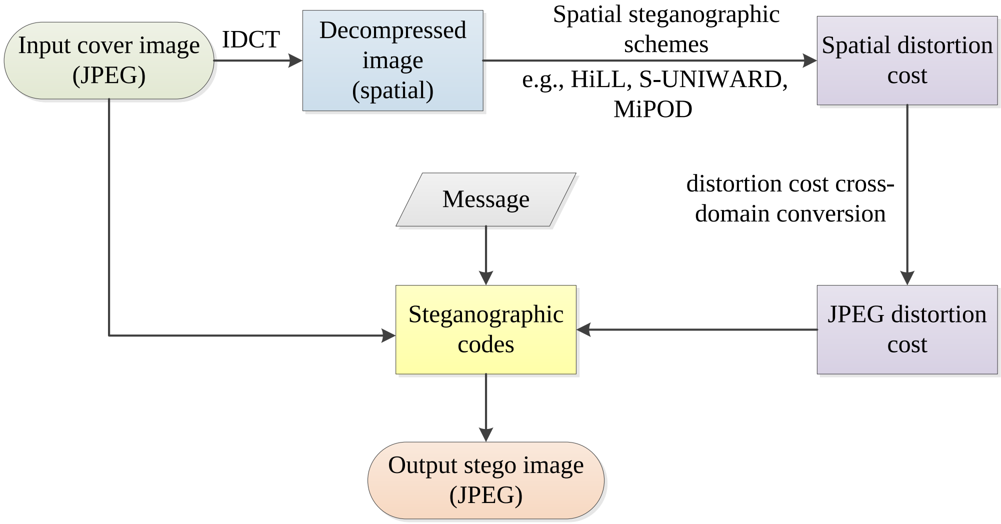

Input cover image (JPEG)
IDCT
Decompressed image (spatial)
Spatial steganographic schemes
e.g., HiLL, S-UNIWARD, MiPOD
Spatial distortion cost
Message
distortion cost cross-domain conversion
Steganographic codes
JPEG distortion cost
Output stego image (JPEG)

Figure 1. The diagram of the proposed JPEG steganographic scheme (IDCT is the Inverse Discrete Cosine Transform).

4. Experimental Results

4.1. Experimental Settings

4.1.1. Image Datasets

In this paper, experiments were conducted on the widely used image database *BOSSBase* v1.01 [30] for image steganography, which consists of 10,000 512 × 512 × 8-bit grayscale images. To facilitate the evaluation and comparison of algorithm performance, we first resized the images in BOSSBase to a size of 256 × 256 using the Matlab function "imresize" with the *Bicubic* Kernel and then compressed them into the JPEG domain with *QF* (Quality Factor) = 75 and *QF* = 95. After that, two JPEG image datasets were available, namely BOSSQ75 and BOSSQ95, which will be used in the following tests.

4.1.2. Steganographic Schemes

To evaluate the security performance of the proposed JC-A scheme, advanced JPEG steganographic schemes, e.g., UERD [14], JUNIWARD [11] and JMiPOD [18], were included in a comparison. In addition, the heuristically designed Distortion Cost Domain Transformation scheme, DCDT, is also involved. Since all tested schemes are only different in the distortion cost function, the experiments were simulated at the corresponding payload–distortion bound [33] under a given relative payload $\alpha \in \{0.1, 0.2, 0.3, 0.4, 0.5\}$ bpnzAC (bits per non-zero alternating current DCT coefficient).

4.1.3. Steganalyzers

Four advanced steganalysis feature sets were adopted to evaluate the security of involved steganographic schemes at different relative payloads and QFs, namely the CC-JRM (Cartesian-Calibrated JPEG-Rich Model) [29], the PHARM (Phase Aware Projection Model) [27], GFRs (Gabor Filter Residuals) [28], and SCA-GFRs (Selection Channel Aware GFRs) [34]. The CC-JRM is derived from DCT coefficients to detect steganographic embedding modifications in the JPEG domain, PHARM and GFR are constructed based on noise residuals in the decompressed spatial domain, and SCA-GFRs are the selection-channel-aware version of GFRs that incorporate the knowledge of the embedding modification probabilities to provide a substantial detection gain. After extracting the feature sets from both cover and stego images, the detectors were trained as binary classifiers implemented by using the FLD (Fisher Linear Discriminant) ensemble [35] with default settings. The security performance is quantified by the average classification error probability $\overline{P}_E$ of the FLD ensemble classifier over ten iterations of random testing, where a larger $\overline{P}_E$ means a higher steganographic security. The split ratio of cover/stego pairs for training and testing is 1:1.

4.2. Comparison with Prior Work

After determining the experimental setup, we then proceeded to compare the security performance of the proposed scheme, JC-A, with the competing approach, DCDT, in which the widely acknowledged spatial steganographic schemes SUNIWARD, HiLL, and MiPOD were used for the acquisition of spatial distortion costs. Additionally, the advanced JPEG schemes UERD, JUNIWARD and JMiPOD were also included for comparison. The average classification error probability $\overline{P}_E$ (in %) of the tested steganographic schemes for various relative payloads under the detection of CC-JRM, PHARM, GFR and SCA-GFR on both datasets BOSSQ75 and BOSSQ95 is summarized in Tables 1–4, respectively. Bold numbers in the tables indicate the best security performance for the given settings. Overall, it can be observed that the proposed scheme is effective in resisting the detection of involved steganalysis features, as described in the following analysis.

Table 1. Average classification error probability $\overline{P}_E$ (in %) of the involved JPEG steganographic schemes under the detection of **CC-JRM** versus different relative payloads on BOSSQ75 and BOSSQ95.

Scheme	**QF = 75**					**QF = 95**				
	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
UERD	48.14	44.41	39.77	34.46	28.78	49.73	48.57	46.08	42.84	38.76
JUNIWARD	48.51	45.65	41.47	36.61	31.43	49.55	49.08	48.11	45.83	42.75
JMiPOD	48.21	45.13	41.09	36.02	30.85	49.72	49.31	48.14	45.94	43.08
DCDT-SUNI	48.31	44.28	39.32	33.23	27.18	49.72	49.19	47.82	45.43	41.57
DCDT-MiPOD	48.01	44.32	38.15	32.61	25.43	49.67	49.11	47.13	44.26	40.35
DCDT-HiLL	48.13	44.54	40.02	34.52	28.71	49.74	49.25	48.03	45.91	42.21
JC-SUNI	**48.63**	**45.74**	**41.63**	**37.26**	**31.59**	**49.86**	**49.62**	**48.31**	**46.63**	**43.15**
JC-MiPOD	48.55	45.46	41.51	36.31	30.52	49.83	49.41	48.06	45.57	41.78
JC-HiLL	48.57	45.21	40.48	35.12	28.14	49.84	49.58	48.15	46.31	42.36

Table 2. Average classification error probability $\overline{P}_E$ (in %) of the involved JPEG steganographic schemes under the detection of **PHARM** versus different relative payloads on BOSSQ75 and BOSSQ95.

Scheme	**QF = 75**					**QF = 95**				
	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
UERD	45.63	38.68	31.16	24.02	18.28	48.61	45.35	41.13	35.74	30.52
JUNIWARD	46.39	39.75	32.16	24.37	17.59	49.15	47.16	43.84	39.42	33.86
JMiPOD	45.91	40.21	33.39	26.45	20.34	49.16	47.35	44.91	41.43	36.94
DCDT-SUNI	45.55	38.92	30.42	23.33	16.83	49.31	47.48	44.63	40.25	35.82
DCDT-MiPOD	45.42	38.51	30.52	23.13	17.32	49.44	47.36	44.51	40.13	35.17
DCDT-HiLL	45.73	38.77	31.27	24.05	17.69	49.32	47.51	44.83	41.12	36.86
JC-SUNI	**46.95**	**41.23**	**34.62**	**28.57**	**22.13**	49.38	**47.73**	45.18	41.74	37.51
JC-MiPOD	46.71	41.04	34.47	27.88	22.06	49.48	47.51	44.98	41.04	36.05
JC-HiLL	46.71	41.12	34.29	28.15	22.04	**49.55**	47.66	**45.19**	**41.84**	**38.08**

Table 3. Average classification error probability $\overline{P}_E$ (in %) of the involved JPEG steganographic schemes under the detection of **GFR** versus different relative payloads on BOSSQ75 and BOSSQ95.

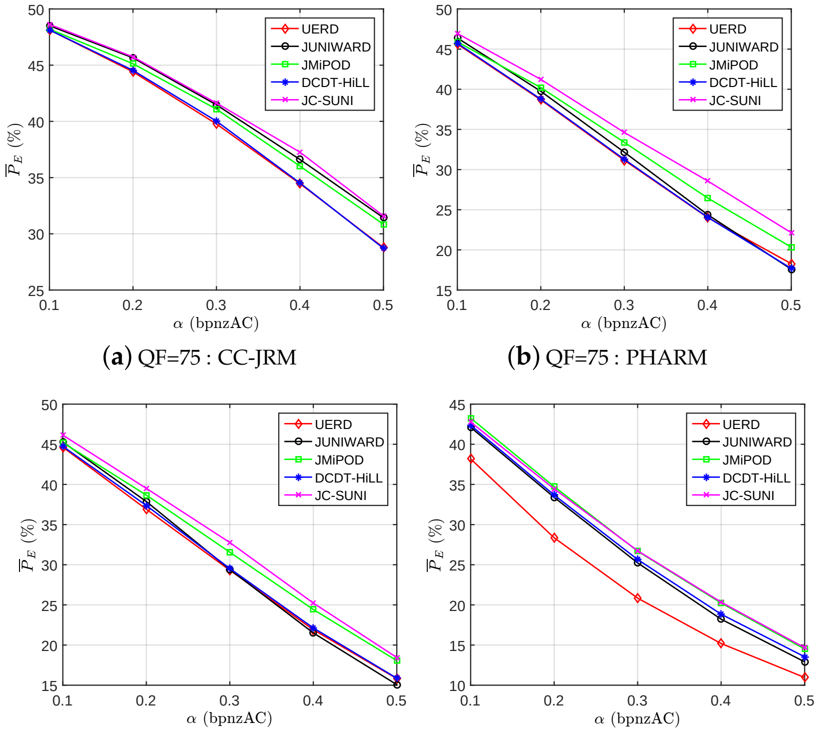
Scheme	**QF = 75**					**QF = 95**				
	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
UERD	44.64	36.91	29.32	21.91	15.82	47.74	44.12	39.11	33.61	27.63
JUNIWARD	45.29	37.87	29.41	21.51	15.07	48.98	46.14	41.89	36.55	30.62
JMiPOD	45.21	38.67	31.56	24.43	18.06	48.86	46.52	43.16	38.78	34.03
DCDT-SUNI	44.56	36.69	28.55	20.72	14.83	48.85	46.27	42.75	37.68	32.39
DCDT-MiPOD	44.21	35.87	27.02	19.63	13.71	48.77	46.23	42.01	37.44	31.86
DCDT-HiLL	44.74	37.38	29.53	22.13	15.87	48.94	46.49	43.02	38.47	33.39
JC-SUNI	**46.14**	**39.51**	**32.77**	**25.23**	**18.45**	**49.14**	**46.87**	43.38	**39.22**	34.14
JC-MiPOD	45.53	39.23	31.58	24.16	17.63	48.91	46.64	43.08	38.93	33.09
JC-HiLL	45.96	38.95	31.26	24.08	17.47	49.11	46.73	**43.45**	39.15	**34.33**

Table 4. Average classification error probability $\overline{P}_E$ (in %) of the involved JPEG steganographic schemes under the detection of **SCA-GFR** versus different relative payloads on BOSSQ75 and BOSSQ95.

Scheme	**QF = 75**					**QF = 95**				
	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
UERD	38.18	28.36	20.84	15.19	10.96	44.73	38.81	33.23	27.62	22.49
JUNIWARD	42.11	33.39	25.23	18.22	12.91	48.28	44.82	40.42	35.36	29.74
JMiPOD	**43.26**	**34.73**	26.69	20.23	14.51	48.06	44.87	41.02	36.37	31.51
DCDT-SUNI	41.67	32.87	24.69	17.99	12.94	47.73	44.43	40.35	35.68	30.91
DCDT-MiPOD	40.39	31.22	23.96	17.59	12.91	47.51	43.97	39.75	35.32	30.79
DCDT-HiLL	42.37	33.68	25.65	18.84	13.54	48.05	44.81	40.96	36.25	31.18
JC-SUNI	42.76	34.45	**26.74**	**20.34**	**14.67**	48.42	45.06	41.15	36.87	31.68
JC-MiPOD	41.74	33.91	26.23	20.18	14.63	48.36	**45.43**	**41.37**	**37.06**	**31.96**
JC-HiLL	40.89	31.81	23.83	17.74	11.76	**48.56**	45.18	40.94	36.21	31.07

Referring to the results in Tables 1–4, we can observe that compared with DCDT, our scheme achieves an overall superior security performance in resisting the detection of CC-JRM, PHARM, and GFR, especially on the BOSSQ75 dataset. Specifically, in Table 1, the proposed scheme slightly outperforms other JPEG schemes in resisting the detection of the CC-JRM, which is attributed to the fact that our scheme is designed from the perspective of minimizing the impact of the embedding in the spatial domain, whereas the CC-JRM specifically captures the statistical variations in the JPEG domain. In the cases of resisting the detection of PHARM and GFR, as shown in Tables 2 and 3, the proposed scheme can outperform DCDT by a clear margin when using the same spatial steganographic scheme, which reflects that the JPEG distortion costs computed by our theoretically derived scheme are more accurate and effective than those computed by the heuristically designed DCDT. For example, compared with DCDT-SUNI, the maximal security improvements for JC-SUNI in resisting the detection of PHARM and GFR on the BOSSQ75 dataset are 5.30% and 4.51%, respectively, and the maximal improvements for JC-SUNI in resisting the detection of PHARM and GFR on the BOSSQ95 dataset are 1.69% and 1.54%, respectively. The security performance gains of our scheme degrade when resisting the detection of SCA-GFR, which is assumed to have the knowledge of the selection channel (i.e., the embedding modification probabilities) from the steganographic scheme. Nevertheless, identifying the selection channel is too difficult to achieve, because this knowledge is usually unavailable to steganalyzers in practical scenarios.

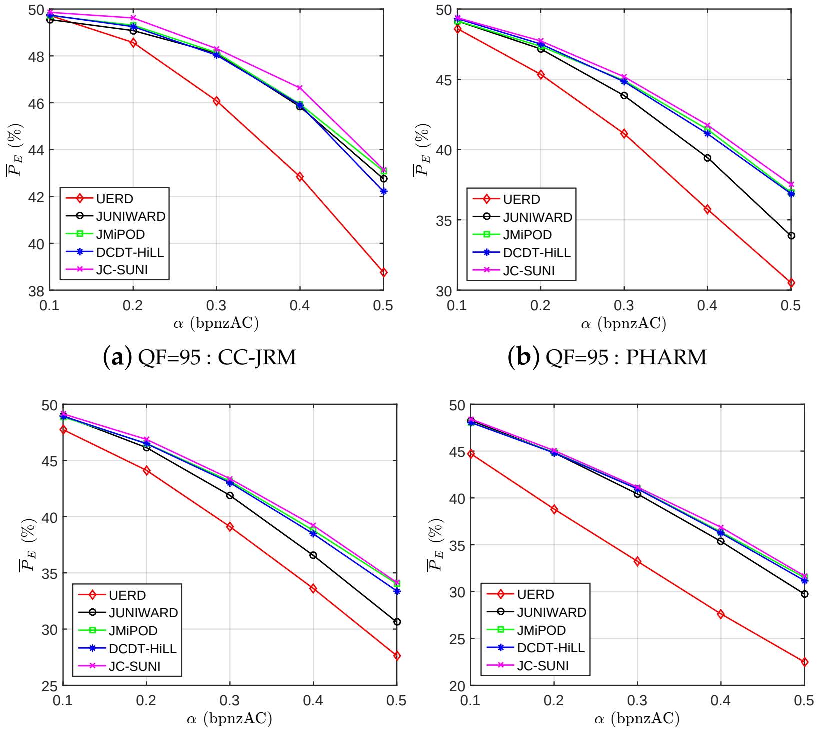
In contrast to the advanced JPEG steganographic schemes on security performance, according to the results in Tables 1–4, it can be observed that our schemes JC-SUNI, JC-HiLL, and JC-MiPOD not only outperform the heuristic-based schemes UERD and JUNIWARD, but also rival the state-of-the-art statistical model-based scheme JMiPOD. In order to clearly demonstrate that the security performance has been improved, some representative results are selected from Tables 1–4, and shown in Figures 2 and 3. Overall, the proposed JC-SUNI exhibits the best security performance among the schemes involved. For instance, compared with UERD, the maximal security improvements of JC-SUNI in resisting the detection of CC-JRM, PHARM, GFR, and SCA-GFR on the BOSSQ75 dataset can reach 2.81%, 4.55%, 3.45%, and 6.09%, respectively, and the maximal improvements of JC-SUNI in resisting the detection of CC-JRM, PHARM, GFR, and SCA-GFR on the BOSSQ95 dataset can even reach 4.39%, 6.99%, 6.51% and 9.25%, respectively. When compared with the state-of-the-art scheme JMiPOD, our JC-SUNI demonstrates maximal security improvements of 1.24%, 2.12%, 1.21% and 0.16% in resisting the detection of CC-JRM, PHARM, GFR, and SCA-GFR on the BOSSQ75 dataset, respectively, and maximal improvements of 0.69%, 0.57%, 0.44% and 0.50% in resisting the detection of CC-JRM, PHARM, GFR, and SCA-GFR on the BOSSQ95 dataset, respectively. The observed security improvements in the proposed scheme validate the effectiveness of our theoretically derived expression for converting the distortion costs computed by existing spatial steganographic schemes to those applied in JPEG steganography. Furthermore, as shown in Tables 1–4, our JC-SUNI, JC-HiLL, and JC-MiPOD schemes exhibit a similar level of security in most cases, indicating the applicability of the proposed distortion cost cross-domain transformation method to different spatial steganographic schemes. In practical applications, there is a general consensus that any steganographic scheme with $\overline{P}_E \geq 40\%$ is considered to be secure. The experimental results show that compared with other competitors, our scheme has an overall superior security performance, and $\overline{P}_E$ can be larger than 40% under a certain embedding payload. In this regard, we can more flexibly adjust the embedding payload in the proposed scheme to achieve secure steganography.



(**a**) QF=75 : CC-JRM (**b**) QF=75 : PHARM

(**c**) QF=75 : GFR (**d**) QF=75 : SCA-GFR

Figure 2. Average classification error probability $\overline{P}_E$ (in %) for different JPEG steganographic schemes when steganalyzing with (**a**) CC-JRM, (**b**) PHARM, (**c**) GFR, and (**d**) SCA-GFR on BOSSQ75. The curves correspond to the results given in Tables 1–4.



(**a**) QF=95 : CC-JRM (**b**) QF=95 : PHARM

(**c**) QF=95 : GFR (**d**) QF=95 : SCA-GFR

Figure 3. Average classification error probability $\overline{P}_E$ (in %) for different JPEG steganographic schemes when steganalyzing with (**a**) CC-JRM, (**b**) PHARM, (**c**) GFR, and (**d**) SCA-GFR on BOSSQ95. The curves correspond to the results given in Tables 1–4.

4.3. Practical Evaluation of Computational Complexity

In this part, we further evaluate the computational complexity of our proposed schemes JC-SUNI, JC-HiLL, and JC-MiPOD compared with other advanced steganographic schemes, e.g., UERD, JUNIWARD, JMiPOD, and DCDT, in terms of time consumption. Considering that the involved schemes are mainly different in the distortion cost function, it is reasonable to evaluate their computational complexity by comparing the practical time consumption in the calculation of distortion costs. In specific, we compare the average time consumption in calculating the distortion costs for the involved schemes over 1000 JPEG images randomly selected from the BOSSQ75 and BOSSQ95 datasets, respectively. This experiment was implemented in Matlab 2015b on a 3.2 GHz Intel CPU Xeon E-2836 with 64 GB memory under a computer running a 64-bit Windows 10 system. The numerical results are summarized in Table 5. It can be observed that: (1) The average time consumption of the proposed scheme is consistently less than that of DCDT when using the same spatial steganographic scheme for distortion cost cross-domain transformations. (2) The proposed JC-HiLL and JC-SUNI are computationally efficient, at about 75 and 43 times faster, respectively, than JUNIWARD in the calculation of distortion costs. (3) For practical steganographic applications, both JC-HiLL and JC-SUNI can be implemented in an acceptable time for UERD.

Table 5. Average time consumption over 1000 JPEG images of 256 × 256 × 8 bits under QF = 75 and QF = 95 in the calculation of distortion costs for UERD, JUNIWARD, JMiPOD, DCDT-HiLL, DCDT-MiPOD, DCDT-SUNI, JC-HiLL, JC-MiPOD, and JC-SUNI. The unit of time is milliseconds (ms).

QF	**Average Time Consumption (ms)**		
	UERD	**JUNIWARD**	**JMiPOD**
75	9.8	1848.3	159.8
95	10.3	1881.4	144.3
QF	**Average Time Consumption (ms)**		
	DCDT-HiLL	**DCDT-MiPOD**	**DCDT-SUNI**
75	26.2	240.6	49.6
95	29.5	243.8	45.8
QF	**Average Time Consumption (ms)**		
	JC-HiLL	**JC-MiPOD**	**JC-SUNI**
75	24.1	236.4	42.6
95	25.4	234.3	43.2

5. Conclusions

In this paper, we propose an efficient distortion cost cross-domain transformation method for JPEG steganography, the core of which is a closed-form expression for converting the distortion costs obtained by existing spatial steganographic schemes to those used in the JPEG images. This transformation method not only guarantees computational efficiency, but also improves the security performance of JPEG steganography in resisting the mainstream steganalysis features which are extracted in the spatial domain. Moreover, a variety of effective JPEG distortion costs can be generated by taking advantage of the well-designed spatial steganographic schemes, providing more options for practical steganographic applications. Finally, experimental results show that the proposed scheme, when adopting different spatial steganographic schemes for the distortion cost transformation, can achieve comparable or superior security performances compared to other advanced JPEG steganographic schemes in resisting the detection of various steganalysis features.

Author Contributions: Y.P.: conceptualization, methodology, investigation, software and writing—original draft. J.N.: conceptualization, supervision, validation and writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by National Natural Science Foundation of China under Grants U1936212 and U22A2030, in part by the Key-Area Research and Development Program of Guangdong Province under Grant 2020B0101360001, and in part by the Peng Cheng Laboratory Project under Grant PCL2021A02.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Khalifa, A.; Guzman, A. Imperceptible image steganography using symmetry-adapted deep learning techniques. *Symmetry* **2022**, *14*, 1325. [CrossRef]
2. Li, X.; Guo, D.; Qin, C. Diversified cover selection for image steganography. *Symmetry* **2023**, *15*, 2024. [CrossRef]
3. Muralidharan, T.; Cohen, A.; Cohen, A.; Nissim, N. The infinite race between steganography and steganalysis in images. *Signal Process* **2022**, *201*, 108711. [CrossRef]
4. Shehab, D.A.; Alhaddad, M.J. Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research. *Symmetry* **2022**, *14*, 117. [CrossRef]
5. Setiadi, D.R.I.M.; Rustad, S.; Andono, P.N.; Shidik, G.F. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Process.* **2023**, *206*, 108908. [CrossRef]
6. Milosav, P.; Milosavljević, M.; Banjac, Z. Steganographic method in selected areas of the stego-carrier in the spatial domain. *Symmetry* **2023**, *15*, 1015. [CrossRef]
7. Filler, T.; Fridrich, J. Gibbs construction in steganography. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 705–720. [CrossRef]
8. Filler, T.; Judas, J.; Fridrich, J. Minimizing embedding impact in steganography using trellis-coded quantization. In Proceedings of the Media Forensics and Security II, San Jose, CA, USA, 18–20 January 2010; Volume 7541, pp. 38–51. [CrossRef]
9. Li, W.; Zhang, W.; Li, L.; Zhou, H.; Yu, N. Designing near-optimal steganographic codes in practice based on polar codes. *IEEE Trans. Commun.* **2020**, *68*, 3948–3962. [CrossRef]
10. Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security, Tenerife, Spain, 2–5 December 2012; pp. 234–239. [CrossRef]
11. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain. *EURASIP J. Inf. Secur.* **2014**, *2014*, 1–13. [CrossRef]
12. Li, B.; Wang, M.; Huang, J.; Li, X. A new cost function for spatial image steganography. In Proceedings of the 2014 IEEE International Conference on Image Processing, Paris, France, 27–30 October 2014; pp. 4206–4210. [CrossRef]
13. Liu, Q.; Su, W.; Ni, J.; Hu, X.; Huang, J. An efficient distortion cost function design for image steganography in spatial domain using quaternion representation. *Signal Process.* **2023**, *219*, 109370. [CrossRef]
14. Guo, L.; Ni, J.; Su, W.; Tang, C.; Shi, Y.Q. Using statistical image model for JPEG steganography: Uniform embedding revisited. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2669–2680. [CrossRef]
15. Su, W.; Ni, J.; Li, X.; Shi, Y.Q. A new distortion function design for JPEG steganography using the generalized uniform embedding strategy. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 3545–3549. [CrossRef]
16. Fridrich, J.; Kodovský, J. Multivariate gaussian model for designing additive distortion for steganography. In Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 2949–2953. [CrossRef]
17. Sedighi, V.; Cogranne, R.; Fridrich, J. Content-adaptive steganography by minimizing statistical detectability. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 221–234. [CrossRef]
18. Cogranne, R.; Giboulot, Q.; Bas, P. Efficient steganography in JPEG images by minimizing performance of optimal detector. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1328–1343. [CrossRef]
19. Yang, J.; Ruan, D.; Huang, J.; Kang, X.; Shi, Y.Q. An embedding cost learning framework using GAN. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 839–851. [CrossRef]
20. Tang, W.; Li, B.; Barni, M.; Li, J.; Huang, J. An automatic cost learning framework for image steganography using deep reinforcement learning. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 952–967. [CrossRef]
21. Li, W.; Wu, S.; Li, B.; Tang, W.; Zhang, X. Payload-independent direct cost learning for image steganography. *IEEE Trans. Circuits Syst. Video Technol.* **2024**, *34*, 1970–1975. [CrossRef]
22. Yang, J.; Ruan, D.; Kang, X.; Shi, Y.Q. Towards automatic embedding cost learning for JPEG steganography. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 37–46. [CrossRef]
23. Tang, W.; Li, B.; Barni, M.; Li, J.; Huang, J. Improving cost learning for JPEG steganography by exploiting JPEG domain knowledge. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 4081–4095. [CrossRef]

24. Hu, X.; Ni, J.; Shi, Y.Q. Efficient JPEG steganography using domain transformation of embedding entropy. *IEEE Signal Process. Lett.* **2018**, *25*, 773–777. [CrossRef]
25. Su, W.; Ni, J.; Hu, X.; Huang, J. New design paradigm of distortion cost function for efficient JPEG steganography. *Signal Process.* **2022**, *190*, 108319. [CrossRef]
26. Holub, V.; Fridrich, J. Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 219–228. [CrossRef]
27. Holub, V.; Fridrich, J. Phase-aware projection model for steganalysis of JPEG images. In Proceedings of the Media Watermarking, Security, and Forensics 2015, San Francisco, CA, USA, 9–11 February 2015; Volume 9409, p. 94090T. [CrossRef]
28. Song, X.; Liu, F.; Yang, C.; Luo, X.; Zhang, Y. Steganalysis of adaptive JPEG steganography using 2D Gabor filters. In Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, Portland, OR, USA, 17–19 June 2015; pp. 15–23. [CrossRef]
29. Kodovský, J.; Fridrich, J. Steganalysis of JPEG images using rich models. In Proceedings of the Media Watermarking, Security, and Forensics 2012, Burlingame, CA, USA, 23–25 January 2012; Volume 8303, p. 83030A. [CrossRef]
30. Bas, P.; Filler, T.; Pevný, T. "Break Our Steganographic System": The ins and outs of organizing BOSS. In Proceedings of the 13th International Conference on Information Hiding, Prague, Czech Republic, 18–20 May 2011; Springer: Berlin/Heidelberg, Germany, pp. 59–70. [CrossRef]
31. Wallace, G. The JPEG still picture compression standard. *IEEE Trans. Consum. Electron.* **1992**, *38*, xviii–xxxiv. [CrossRef]
32. Filler, T.; Fridrich, J. Minimizing additive distortion functions with non-binary embedding operation in steganography. In Proceedings of the 2010 IEEE International Workshop on Information Forensics and Security, Seattle, WA, USA, 12–15 December 2010; pp. 1–6. [CrossRef]
33. Filler, T.; Judas, J.; Fridrich, J. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 920–935. [CrossRef]
34. Denemark, T.; Boroumand, M.; Fridrich, J. Steganalysis features for content-adaptive JPEG steganography. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1736–1746. [CrossRef]
35. Kodovský, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 432–444. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.