Multimed Tools Appl
DOI 10.1007/s11042-016-3823-2

Improving side-informed JPEG steganography using two-dimensional decomposition embedding method

Zhenkun Bao[1] · **Xiangyang Luo**[1] · **Weiming Zhang**[2] · **Chunfang Yang**[1,3] · **Fenlin Liu**[1]

Received: 29 February 2016 / Revised: 23 July 2016 / Accepted: 28 July 2016
© Springer Science+Business Media New York 2016

Abstract Side-informed JPEG steganography is a renowned technology of concealing information for the high resistance to blind detection. The existed popular side-informed JPEG steganographic algorithms use binary embedding method with the corresponding binary distortion function. Then, the embedding methods and binary distortion functions of popular side-informed JPEG steganographic algorithms are analyzed and the wasted secure capacity by using the binary embedding operation is pointed out. Thus, the detection resistance of the side-informed JPEG steganographic algorithms can be improved if the embedding operation is changed to ternary mode which causes less changes than binary embedding at same payload. The problem of using ternary embedding is to define a suitable ternary distortion function. To solve this, a two-dimensional decomposition embedding method is proposed in this paper. The proposed ternary distortion function is defined by transforming the problem into two different binary distortion functions of two layers that based on the ternary entropy decomposition.

✉ Xiangyang Luo
luoxy_ieu@sina.com

Zhenkun Bao
bao13213047058@163.com

Weiming Zhang
zhangwm@ustc.edu.cn

Chunfang Yang
chunfangyang@126.com

Fenlin Liu
liufenlin@sina.vip.com

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

[2] CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230026, China

[3] Science and Technology on Information Assurance Laboratory, Beijing 100072, China

Published online: 16 August 2016

Meanwhile, the proposed method ensures the minimal value of the distortion function on each layer can be reached in theory. Several popular side-inform JPEG steganographic algorithms (NPQ, EBS, and SI-UNIWARD) are improved through defining ternary distortion function by the proposed method. The experimental results on parameters, blind detection and processing time show that the proposed method increases the blind detection resistance of side-informed steganographic algorithm with acceptable computation complexity.

Keywords Steganography · Side-informed JPEG steganography · Two-dimensional decomposition · Adaptive steganography · Double-layer embedding

1 Introduction

Steganography is a technology for concealing communication by hiding information in digital media [15, 19]. Among the steganographic technologies, spatial steganography attracts researchers a lot and many algorithms are proposed [26, 27, 30, 32, 33, 35]. Meanwhile, the JPEG steganography is practical for the reason that JPEG format is the most widely used format for digital images. Because the "side-informed" JPEG steganography [14] can use a raw, uncompressed image as "precover" (be used to obtain original data of JPEG image [17]) to decrease the distortion caused by embedding message, it can effectively resist blind detection. Currently, research on this technology is particularly active in the area of steganography.

JPEG steganography can be classified into adaptive and non-adaptive types [28]. Their main difference is that the embedding changes of the former are adaptive with the cover image contents and the changes are constrained to the regions difficult to detect, and the embedding changes of the latter is regardless to the content of cover image. Earlier JPEG steganographic algorithms are almost the non-adaptable type, such as JPEG-JSteg (http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz), OutGuess [2], F5 [31], and no-shrinkage F5 (nsF5) [11] and so on. These algorithms are highly effective and have motivated further research on concealed communication using the JPEG images. However, they are challenged by modern blind detection techniques such as PEV features enhanced by Cartesian Calibration (ccPEV) [21], Cross-Domain Feature (CDF) [23], union of cc-JRM and SRMQ1 (J + SRM) [22] and Discrete Cosine Transform Residual (DCTR) [13].

To improve the resistance to the modern blind detection techniques, researchers proposed many adaptive JPEG steganographic algorithms. They concentrate embedding modifications in suitable areas through a content-adaptive selection method. Popular JPEG steganographic algorithms include: Perturbed Quantization (PQ) algorithm [9] which uses quantization error to define distortion function; Design of Adaptive Steganographic Schemes (DASS-DCT) algorithm [] which defines distortion function by decomposing kernel function of the classifier; New PQ (NPQ) algorithm [16] which improves upon PQ [9] by introducing more parameters into the distortion function; Uniform Embedding Distortion (UED) algorithm [12] which uses correlations of inter-blocks and intra-blocks to define distortion function; and Efficient Block-entropy Steganographic scheme (EBS) algorithm [34] which considers entropy of the JPEG block. Other well-known adaptive JPEG steganographic algorithms include Side-Informed UNIversal WAvelet Relative Distortion (SI-UNIWARD) algorithm [14] and JPEG UNIversal WAvelet Relative Distortion (J-UNIWARD) algorithm [14], which combine the JPEG distortion function with wavelet coefficients of the corresponding spatial image. Notice that, PQ uses wet paper codes [10] and NPQ uses MME codes [20] for embedding, while DASS-DCT,

UED, EBS, SI-UNIWARD and J-UNIWARD use syndrome trellis codes (STCs, proposed by Filler et al. in [6]). STCs owns near optimal coding performance and can extract the embedded message by the parity-check matrix.

Among these adaptive JPEG steganographic algorithms, PQ, NPQ, EBS and SI-UNIWARD are the side-informed type. The side-informed JPEG steganographic algorithm employs the side-information of the unrounded discrete cosine transform (DCT) coefficient from a precover. The detection resistance of the steganographic (stego) image is increased with the help of the side-information. Side-informed JPEG steganography can effectively resist blind detection on a low payload. The average detection error rates of stego images with payload less than 0.3 bits per the non-zero AC coefficient (bpnzAC) from the EBS and SI-UNIWARD algorithms under the modern blind detection method are higher than 45 % (the average detection error rate of randomly guess is 50 %. However, the rate by the latest detection method in high-payload situation (more than 0.8 bpnzAC) is lower than 10 %. Thus, the blind detection resistance is required to be improved in this situation.

It should be noted that the embedding modification patterns of existing side-informed algorithms are binary ±1 on elements of the cover object. This means that the possible modification of each element is determined to either +1 or -1 depending on the rounding errors. This kind of embedding abandons secure capacity on larger distortion modifications. As noted by Ker et al. in [18], secure capacity means that the secret message capacity of the cover object will not have security issues, such as vulnerability to blind detection. From the definition of Kullback-Leibler (KL) divergence between the cover and stego object, it is evident that side-informed JPEG steganography will increase resistance to blind detection if the abandoned secure capacity of each cover element is utilized properly.

As Fridrich elucidated in [29, Ch. 8.6], in embedding coding, ternary ±1 embedding owns more payload capacity than binary ±1 embedding on cover elements. Thus, the side-informed JPEG steganography embedding method is changed from binary to ternary to leverage the abandoned secure capacity. The results of several native trials of defining ternary distortion function indicate that blind resistance performance of side-informed JPEG steganography will be negatively affected by using ternary ±1 embedding with an improper distortion function. Nevertheless, the JPEG image is sensitive to changes in the DCT coefficients; moreover, modification effects differ on different coefficients. Thus, it is difficult to describe distortion by the ternary quantitative function.

To address the problem of defining proper ternary distortion function in side-informed JPEG steganography, in this paper, a two-dimensional decomposition embedding method (2D-DEM) is proposed. The method transforms the ternary problem into two binary distortion definition on relative distortion layer and basic distortion layer based on the decomposition of ternary entropy. Meanwhile, the result of ternary ±1 embedding and the ratio between the payloads carried by relative and basic layer are controlled by the distribution parameter β. Moreover, the optimal probabilities of the embedding result that minimizes both relative and basic distortion is given. The proposed 2D-DEM can be used to improve many existing steganographic algorithms, such as NPQ, EBS and SI-UNIWARD.

The main work of this paper is as follows:

1) The binary embedding used in side-informed JPEG steganographic algorithm is analyzed. We demonstrate that, the resistance to blind detection of side-informed JPEG steganographic algorithm increases if sender utilizes the wasted secure capacities in the condition of independence of each cover element. Meanwhile, ternary embedding that uses improper ternary ±1 distortion function negatively affects the blind detection resistance is presented.

2) A 2D-DEM method is proposed to construct a proper ternary ±1 distortion function. This method converts the problem of defining ternary ±1 distortion function into defining two binary distortion functions on two layers. Meanwhile, the minimal additive distortion values on both layers of 2D-DEM can be reached in theory. Furthermore, the equivalent ternary ±1 distortion of the distribution calculated by 2D-DEM is provided through the proposed ternary flipping lemma. The message can be embedded by steganographic coding method with the equivalent ternary distortion.
3) An image-content tactics named candidates choosing method (CC method) is proposed for the difficulty of setting proper distribution parameter β.
4) An improved JPEG steganographic algorithm is proposed using the proposed ternary ±1 distortion function and parameter setting. The comparative experimental results to the original NPQ, EBS and SI-UNIWARD algorithms show that the improved algorithm can increase the resistance to blind detection, especially in the high embedding payload.

The rest of this paper is organized as follows. An overview of the minimal distortion model and renowned side-informed JPEG steganographic algorithms are introduced in Section 2. In Section 3, the motivations of this research are presented. 2D-DEM method is proposed to address the ternary ±1 distortion function definition problem in Section 4. It is used to improve three well-known side-informed JPEG steganographic algorithms (NPQ, EBS, and SI-UNIWARD) in Section 5. Experimental results are given in Section 6, and the conclusions are presented in Section 7.

2 Preliminaries

In this section, some related preliminaries are given. First, the minimal distortion model, proposed by Filler and Fridrich [8] is introduced. Then, three renowned side-informed JPEG steganographic algorithms are briefly described.

2.1 Minimal distortion model

In the minimal distortion model, the sender embeds an l-bit secret message, $\boldsymbol{m}=\{m_i\}_{1\le i\le l}$, $m_i\in\{0,1\}$, into the cover object with n elements, $\boldsymbol{x}=\{x_i\}_{1\le i\le n}$, $x_i\in \mathrm{I}_c^i$. $\mathrm{I}_c^i=\{0,1,...,255\}$ on a grayscale image and $\mathrm{I}_c^i=[-1024,...,1024)$ on a JPEG image. The embedding rate is defined as $\alpha=l/n\ge 0$. The stego object, $\boldsymbol{y}=\{y_i\}_{1\le i\le n}$, $y_i\in \mathrm{I}_s^i$, is obtained by modifying the cover object elements. I_s^i is determined by the value of x_i and the embedding method. For example, if the embedding modification is the ternary ±1 method, $\mathrm{I}_s^i=\{x_i-1,x_i,x_i+1\}$, $|\mathrm{I}_s^i|=3$, $1\le i\le n$. Note that $\mathrm{I}_s^i\subset \mathrm{I}_c^i$.

The embedding coding method can be regarded as a replacement of cover $\boldsymbol{x}$ by stego $\boldsymbol{y}$. It is assumed that the respective cover and stego objects are obtained as a realization of random variables $\boldsymbol{X}$ and $\boldsymbol{Y}_\alpha$ over variable spaces $\prod_i \mathrm{I}_c^i$ and $\prod_i \mathrm{I}_s^i$, respectively. Moreover, the distributions of $\boldsymbol{X}$ and $\boldsymbol{Y}_\alpha$ are denoted as τ and π, respectively:

$$\tau(\boldsymbol{x})=P(\boldsymbol{X}=\boldsymbol{x}),\quad \pi(\boldsymbol{y})=P(\boldsymbol{Y}_\alpha=\boldsymbol{y}). \tag{1}$$

$\boldsymbol{X}=\boldsymbol{Y}_{\alpha=0}$ when no message is embedded in the cover object.

The symbol of distortion between the cover and stego objects is $D(\boldsymbol{x},\boldsymbol{y})$. The sender can distribute a message of up to $H(\pi)$ bits by causing the average distortion, $E(D(\boldsymbol{x},\boldsymbol{Y}_\alpha))$. $H(x)$ represents the entropy function, and the binary entropy is expressed as $H_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$(bits).

The steganographic coding method aims to cause the least distortion on the cover object by embedding of the secret message. Therefore, a means of minimizing average distortion $E(D(\boldsymbol{x},\boldsymbol{y}))$ subjected to $H(\pi)=l$ bits is important. However, determination of the optimal distribution π with minimal $E(D(\boldsymbol{x},\boldsymbol{y}))$ is a difficult problem. Actually, it has a strong relationship to source coding with the fidelity criterion described in [1]. In [8], Fridrich and Filler applied a proof of maximum entropy distribution to solve the problem of calculating the optimal distribution π. Optimal π was given in Gibbs distribution form:

$$\pi(\boldsymbol{y})=\frac{\exp(-\lambda D(\boldsymbol{x},\boldsymbol{y}))}{\sum_{\boldsymbol{y}}\exp(-\lambda D(\boldsymbol{x},\boldsymbol{y}))}. \tag{2}$$

λ is a parameter that satisfies $H(\pi)=l$.

It is very challenging to find a proper π that satisfies $H(\pi)=l$ bits using only formula (2). This is because every possible $\boldsymbol{y}$ need to be traversed in formula (2), whose space size is $\prod_i|\mathbf{I}_s^i|$. Because n is usually greater than 10,000, the space size is catastrophically large for computing technology. However, in steganographic research, it is in common that considering embedding distortion caused by changing the cover element to be independent of each other [3, 29, 34,]. That is due to the fact that the modification amplitude of typical steganographic algorithm is usually slight (often less than two), and the interaction effect of them can be less considered. In this case, an additive distortion function $\rho_i(y_i)\in R$ is defined on the cover object, i.e., when x_i is changed to y_i, and $D(\boldsymbol{x},\boldsymbol{y})$ uses $D(\boldsymbol{y})$ as a shorter expression, the $D(\boldsymbol{y})=\sum_{1\le i\le n}\rho_i(y_i)$ and $E(D(\boldsymbol{y}))$ are obtained, where

$$E(D(\boldsymbol{y}))=\sum_{\boldsymbol{y}}\pi(\boldsymbol{y})D(\boldsymbol{y}). \tag{3}$$

Accordingly, Formula (2) can be simplified to

$$\begin{aligned}\pi(\boldsymbol{y})&=\frac{\exp\left(-\lambda\sum_{1\le i\le n}\rho_i(y_i)\right)}{\sum_{\boldsymbol{y}}\exp\left(-\lambda\sum_{1\le i\le n}\rho_i(y_i)\right)}=\frac{\prod_{1\le i\le n}\exp(-\lambda\rho_i(y_i))}{\sum_{\boldsymbol{y}}\left(\prod_{1\le i\le n}\exp(-\lambda\rho_i(y_i))\right)}=\prod_{1\le i\le n}\frac{\exp(-\lambda\rho_i(y_i))}{\sum_{y_i\in\mathbf{I}_s^i}\exp(-\lambda\rho_i(y_i))}\\&=\prod_{1\le i\le n}\pi_i(y_i)_\lambda.\end{aligned} \tag{4}$$

Formula (4) is computable and $\pi_i(y_i)_\lambda$ denotes the probability of changing x_i to y_i under a specific λ. Parameter λ is obtained through a binary search method in the condition of $H(\pi)=\sum_{1\le i\le n}H\left(\pi_i(y_i)_\lambda\right)=l$ bits. The feasibility of the binary search is based on the monotonicity of $H(\pi_i(y_i)_\lambda)$ on λ in domain $[0,\ +\infty)$. Thus, the sender can reach a minimal additive $E(D(\boldsymbol{y}))$ if π of the stego object satisfies $\pi(\boldsymbol{y})=\prod_{1\le i\le n}\pi_i(y_i)_\lambda$ for any possible $\boldsymbol{y}\in\prod_i\mathbf{I}_s^i$.

After the distribution that minimizes the additive distortion is calculated, simulated optimal embedding can be processed with the help of it. The simulated optimal embedding is a theoretic bound of embedding performance. Actually, difference between simulated optimal

embedding and actual embedding usually exists. However, the STCs can embed message with near optimal embedding performance because STCs uses the idea of Viterbi decoder which a near optimal approach to the maximum likelihood code [3, 6]. For the excellent efficiency of STCs, it is widely used in the recent popular adaptive image JPEG steganographic algorithms, such as DASS-DCT, UED, EBS, SI-UNIWARD and J-UNIWARD.

2.2 Principles of NPQ, EBS and SI-UNIWARD algorithms

The JPEG format stores an image by compressing the raw spatial object through domain transformation, quantization and rounding steps. Before undergoing JPEG compression, the raw uncompressed image is partitioned into consecutive non-overlapping 8×8 blocks after color space conversion (from RGB to YUV) and downsampling. In this paper, we focus on grayscale images which have only intensity information and the influence of color space conversion and downsampling is ignore[1].

The symbols, $\boldsymbol{c}=\{c_{i,j}|1\le i\le h, 1\le j\le w\}$, are always used for a spatial image cover object with a size of $h\times w$. Element $c_{i,j}$ is in a finite set $\mathrm{I}_o=\{0,\ldots,255\}$. $\boldsymbol{c}$ is divided into M blocks of an 8×8 size. Horizontal and vertical DCT are independently applied on each block after minus 128 to each element $c_{i,j}$. Then, the transformed image $\boldsymbol{d}=\{d_{i,j}|1\le i\le h, 1\le j\le w\}$ on the frequency domain is obtained, and DCT coefficient $d_{i,j}$ is in the range of $\mathrm{I}_t=[-1024, 1024)$. The t-th block of frequency image $\boldsymbol{d}$ is denoted as $\boldsymbol{d}_{8\times 8}^{(t)}=\left\{d_{i,j}^{(t)}|1\le i,\ \ j\le 8\right\},\ \ t=1,\ldots,M$.

The quantization table $\boldsymbol{Q}_{8\times 8}^{QF}=\left\{q_{i,j}^{QF}\right\}\in\boldsymbol{Z}$ is calculated from the standard quantization table and quality factor (QF). For example, the 75-quality-valued quantization table, $\boldsymbol{Q}_{8\times 8}^{75}$, obtained from the standard light quantization table is shown as:

$$\boldsymbol{Q}_{8\times 8}^{75}=\begin{bmatrix} 8 & 6 & 5 & 8 & 12 & 20 & 26 & 31\\ 6 & 6 & 7 & 10 & 13 & 29 & 30 & 28\\ 7 & 7 & 8 & 12 & 20 & 29 & 35 & 28\\ 7 & 9 & 11 & 15 & 26 & 44 & 40 & 31\\ 9 & 11 & 19 & 28 & 34 & 55 & 52 & 39\\ 12 & 18 & 28 & 32 & 41 & 52 & 57 & 46\\ 25 & 32 & 39 & 44 & 52 & 61 & 60 & 51\\ 36 & 46 & 48 & 49 & 56 & 50 & 52 & 50 \end{bmatrix} \tag{5}$$

In the quantization step, each quantized block $\boldsymbol{d}_{8\times 8}^{qd(t)}=\left\{d_{i,j}^{qd(t)}|1\le i,\ \ j\le 8\right\},\ \ t=1,\ldots,M$ is obtained by dividing coefficient $d_{i,j}^{(t)}$ by $q_{i,j}^{QF}$. Then, rounding step is applied to modify quantized DCT coefficient $d_{i,j}^{qd(t)}$ to the nearest integer and the rounded DCT block is denoted as $\boldsymbol{d}_{8\times 8}^{\mathrm{qdrd}(t)}=\left\{d_{i,j}^{\mathrm{qdrd}(t)}|1\le i,\ \ j\le 8\right\}$, $t=1,\ldots,M$, $d_{i,j}^{\mathrm{qdrd}(t)}\in\{-1024,-1023,\ldots,1024\}$.

[1] It is easy to extend the steganographic algorithms of grayscale image to color image if considering the three channels of color image is independent to each other, and the databases of the side-informed JPEG steganographic algorithms NPQ, EBS and UNIWARD are grayscale images. Thus, this paper focuses on the grayscale images, and the well-known database BOSSbase ver. 1.01 is used in the experiments.

The side-informed JPEG steganographic algorithm conceals the message on the set of rounded coefficients, $\left\{d_{i,j}^{\mathrm{qdrd}(t)} | 1 \le i,\ \ j \le 8,\ \ t = 1, ..., M\right\}$, of the cover object and produces stego object $\boldsymbol{y} = \left\{y_{i,j}^{(t)} | 1 \le i,\ \ j \le 8,\ \ t = 1, ..., M\right\}$. $\left\{d_{i,j}^{\mathrm{qdrd}(t)} | 1 \le i,\ \ j \le 8,\ \ t = 1, ..., M\right\}$ is loaded in rows from left to right and top to bottom of each block, and starting at the top-left location of the image to obtain $\boldsymbol{x}$. Meanwhile, the side-informed JPEG steganographic algorithm requires unrounded coefficients $\left\{d_{i,j}^{qd(t)} | 1 \le i,\ \ j \le 8,\ \ t = 1, ..., M\right\}$ to be the "precover", which is utilized by calculating the rounding error, $\boldsymbol{e} = \left\{e_{i,j}^{(t)} = d_{i,j}^{\mathrm{qdrd}(t)} - d_{i,j}^{qd(t)} | 1 \le i, j \le 8, t = 1, ..., M\right\}$.

The well-known side-informed JPEG steganographic algorithms use a framework comprised of the distortion function and steganographic code. The distortion functions of NPQ, EBS and SI-UNIWARD are respectively defined as

$$\rho_{i,j}^{(t)1} = \frac{{q_{i,j}}^{\alpha_1}\left(1 - 2\left(\left|e_{i,j}^{(t)}\right|\right)\right)}{\left(\mu + \left|d_{i,j}^{\mathrm{qdrd}(t)}\right|\right)^{\alpha_2}} \tag{6}$$

$$\rho_{i,j}^{(t)2} = \left(\frac{q_{i,j}\left(0.5 - \left|e_{i,j}^{(t)}\right|\right)}{\mathrm{H}\left(\boldsymbol{d}^{(t)}|_{i,j}\right)}\right) \tag{7}$$

$$\rho_{i,j}^{(t)3} = \sum_{k,u,v} \frac{\left|W_{u,v}^{(k)}(\boldsymbol{c}) - W_{u,v}^{(k)}(A)\right| - \left|W_{u,v}^{(k)}(\boldsymbol{c}) - W_{u,v}^{(k)}(B)\right|}{\varepsilon + \left|W_{u,v}^{(k)}(\boldsymbol{c})\right|}. \tag{8}$$

The symbols $\rho_{i,j}^{(t)1}$, $\rho_{i,j}^{(t)2}$ and $\rho_{i,j}^{(t)3}$ imply the distortion value of changed element caused by the embedding process. They are binary distortion functions with a default definition that the distortion of no change element equals 0. μ, α_1 and α_2 of the NPQ distortion function are parameters defined to modify the distortion function in [16]. In the distortion function $\rho_{i,j}^{(t)2}$ of EBS, $\boldsymbol{d}^{(t)}|_{i,j}$ is the t-th block where element $d_{i,j}^{\mathrm{qdrd}(t)}$ is located, and $\mathrm{H}(\boldsymbol{d}^{(t)}{}_{i,j})$ is the block entropy, which is defined as $\mathrm{H}\left(\boldsymbol{d}^{(t)}{}_{i,j}\right) = -\sum_i h_i^{(t)} \log h_i^{(t)}$, where $h_i^{(t)}$ is the normalized histogram of all non-zero DCT coefficients in t-th block $\boldsymbol{d}^{(t)}$. In the distortion function of SI-UNIWARD, symbol A denotes $J^{-1}(\boldsymbol{y}_{i,j})$ and B denotes $J^{-1}(\boldsymbol{d})$ in the SI-UNIWARD algorithm. $W_{u,v}^{(k)}(x)$ is the uv-th wavelet coefficient in the k-th subband of the first decomposition level and $J^{-1}(x)$ is the JPEG decompression process. Meanwhile, $\boldsymbol{c}$ represents the spatial image as the "precover".

The parameters of the NPQ method are suggested to be set as μ=0, α_1=α_2=0.5, which are presented in [16]. In the [14], the NPQ, EBS, and SI-UNIWARD can be increased the blind detection resistance if the element in each of the 1/2 coefficients $d_{i,j}^{\mathrm{qdrd}(t)}$ (whose $e_{i,j}^{(t)}$ is equal to 1/2) is rejected to change when $(i,j) \in \{(0,0),(0,4),(4,0),(4,4)\}$ on account of the 1/2 coefficient phenomenon (highlighted in [14]). Thus, the implementations of these three algorithms consider the phenomenon in the experiments.

3 Motivations

In this section, the motivations of this paper is described. First, some analyses of the binary embedding method used in side-informed JPEG steganography are given. Then, some simple trials and security experiments using ternary ±1 embedding in SI-UNIWARD are presented.

3.1 Binary embedding in side-informed steganography

The embedding method in existing side-informed JPEG steganographic techniques is binary ±1. This means that only two possible values exist for each of the changeable cover elements (the cover value after +1/−1 and original cover value). For this method, the +1 or −1 modification on each cover element must be determined before executing the embedding process. The principle of this approach is based on the causes of minor distortion in side-informed JPEG steganography. For example, we suppose changeable element with an integer value of 2 and rounded from 2.4. The distance between the original value, is 2.4, and the +1 modification result, 3, is 0.6, while the same distance on the −1 modification result is 1.4. It is obvious that less distance between the original value and embedding result implies less distortion. Thus, in this example, the distortion caused by the +1 modification is less than that of the −1 modification; Moreover, the changed value on this element is determined to be 3. After executing the determination on each changeable cover element, the coding method can be implemented to embed the message.

Binary ±1 embedding has abandoned the use of modifications that causes greater distortion. In the steganographic region, a secret messages is embedded in we are interested in the KL divergence [25] between cover object $\boldsymbol{x}$ and stego object $\boldsymbol{y}$, which we will denote $D_{KL}(\boldsymbol{Y}_0||\boldsymbol{Y}_\alpha)$. Smaller value of $D_{KL}(\boldsymbol{Y}_0||\boldsymbol{Y}_\alpha)$ means lower level of detectability of the stego object.

As long as the distribution of $\boldsymbol{Y}_\alpha$ satisfies specific smoothness assumptions [5], Taylor expansion to the right of $\alpha=0$ with fixed cover parameter θ is

$$D_{KL}(\boldsymbol{Y}_0||\boldsymbol{Y}_\alpha)=\sum_{\boldsymbol{y}}\left[\tau(\boldsymbol{y})\ln\frac{\tau(\boldsymbol{y})}{\pi(\boldsymbol{y})}\right]\sim\frac{n}{2}\alpha^2\,\mathrm{F}^\theta(0) \tag{9}$$

where $\mathrm{F}^\theta(0)$ is so-called Fisher information. The above equation above relays the square root law of imperfect steganography. It means the sender must adjust the embedding rate α to maintain the same statistical detectability over the increase of cover length n, so that $n\alpha^2$ remains constant. It means that the embedding payload, $n\alpha$, must be proportional to $\sqrt{n}$, and the proper measure of the secure payload (*SP*) is the proportionality constant, $\mathrm{F}^\theta(0)$, which is the Fisher information [18, 19].

Under the independence assumption of cover and stego object given in the first part of Section 2, and sometimes function τ of an image in transform domain image is often independent to each cover element for the DCT process eliminates the correlation between every two DCT coefficients in a same DCT block. Thus, in side-informed JPEG steganographic algorithm, each elements of the cover object can be considered as a single independent image on variable $\boldsymbol{X}_{(i)}$ over I_c^i, which contains only one pixel and cover parameter θ_i. We define the KL divergence, D_{KL}^i, between $\boldsymbol{X}_{(i)}$ and $\boldsymbol{Y}_{(i)}$ on each single image. They obey the relationship of Formula (9):

$$D_{KL}^i\left(\boldsymbol{Y}_{0(i)}\middle\|\boldsymbol{Y}_{\alpha(i)}\right)=\sum_{y_i\in\mathrm{I}_s^i}\left[\tau_i(y_i)\ln\frac{\tau_i(y_i)}{\pi_i(y_i)}\right]\sim\frac{1}{2}{\alpha_i}^2\,\mathrm{F}^\theta(0) \tag{10}$$

The embedding rate on cover element x_i is α_i. Because the size of each single image is 1, α_i is equal to the embedding payload. Furthermore, the distributions π and τ can be presented as

$$\pi(\boldsymbol{y}) = P(\boldsymbol{Y}_\alpha = \boldsymbol{y}) = \prod_{1\le i\le n} P\left(\boldsymbol{Y}_{\alpha(i)} = y_i\right) \tag{11}$$

$$\tau(\boldsymbol{y}) = P(\boldsymbol{X} = \boldsymbol{x}) = \prod_{1\le i\le n} P\left(\boldsymbol{X}_{(i)} = x_i\right) \tag{12}$$

Meanwhile, we use symbols $\pi_i(y_i)$ and $\tau_i(x_i)$ to denote $P(\boldsymbol{Y}_{\alpha(i)}=y_i)$ over I_c^i and $P(\boldsymbol{X}_{(i)}=x_i)$ over I_s^i, respectively. According to the definition of KL divergence in [25], D_{KL} between $\boldsymbol{x}$ and $\boldsymbol{y}$ can be expressed as

$$\begin{aligned} D_{KL}(\boldsymbol{Y}_0 \| \boldsymbol{Y}_\alpha) &= \sum_{\boldsymbol{y}} \left[\prod_{i=1}^{n} \tau_i(y_i)\left(\sum_{i=1}^{n} \ln\frac{\tau_i(y_i)}{\pi_i(y_i)}\right)\right] = \sum_{\boldsymbol{y}} \sum_{i=1}^{n} \left[\prod_{i=1}^{n} \tau_i(y_i)\left(\ln\frac{\tau_i(y_i)}{\pi_i(y_i)}\right)\right] \\ &= \sum_{j=1}^{n} \left[a_j \sum_{y_j\in \mathrm{I}_s^j} \left(\tau_j\left(y_j\right)\ln\frac{\tau_j\left(y_j\right)}{\pi_j\left(y_j\right)}\right)\right] = \sum_{j=1}^{n} a_j D_{KL}^{j}\left(\boldsymbol{Y}_{0(j)} \middle\| \boldsymbol{Y}_{\alpha(j)}\right) \\ &\sim \sum_{j=1}^{n} a_j \frac{1}{2}\alpha_j^2 \mathrm{F}^{\theta_j}(0) \end{aligned} \tag{13}$$

The symbol a_j denotes $\prod_{1\le i\le n,\ i\ne j}\tau_i(y_i)$, which is a constant to y_j. It means that the total secure payload, SP_{total}, of the cover object can be expressed as a sum of the secure payload, $SP_{\mathrm{single}(i)}$, of each single image. If we can employ the secure capacity of the abandoned modification in binary embedding, a larger payload will be embedded at the same level of the KL divergence.

As Fridrich explained about embedding coding in [[7], Ch. 8.6], the capacity of each cover element in ternary ±1 embedding (up to $\log_2 3$ bits per element) is higher than binary ±1 embedding (up to 1 bit per element). That is, using ternary ±1 embedding may cause a lower level of detectability than binary ±1 embedding, and the problem is focus on how to define a proper ternary ±1 distortion function in side-informed JPEG steganographic algorithm. This is the first motivation of this paper.

3.2 Initial attempts of defining ternary ±1 distortion function

A natural approach of defining ternary ±1 distortion function is introducing the binary ±1 distortion function in the renowned side-informed JPEG steganographic algorithm. Thus, several native ternary ±1 distortion functions on the distortion function $\left\{\rho_{i,j}^{(t)}\right\}$ of the SI-UNIWARD algorithm are tested as follows:

$$\rho_{tr1}^{(t)}\left(y_{i,j}\right) = \begin{cases} \rho_{i,j}^{(t)3}, & \text{closer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)}, \\ \rho_{i,j}^{(t)3}, & \text{longer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)}, \\ 0 & , \text{ no change.} \end{cases} \tag{14}$$

$$\rho_{tr2}^{(t)}\left(y_{i,j}\right) = \begin{cases} \rho_{i,j}^{(t)3} & , \text{closer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)}, \\ 2\rho_{i,j}^{(t)3}, & \text{longer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)}, \\ 0 & , \text{ no change,} \end{cases} \tag{15}$$

$$\rho_{tr3}^{(t)}\left(y_{i,j}\right)=\begin{cases}\rho_{i,j}^{(t)3} & , \text{ closer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)},\\ 10\rho_{i,j}^{(t)3} & , \text{ longer distance between } y_{i,j}^{(t)} \text{ and } d_{i,j}^{qd(t)},\\ 0 & , \text{ no change.}\end{cases} \tag{16}$$

The detection experiments were executed through blind detection method composed by DCTR [13] feature library and ensemble classifier [24] on 10,000 images of Bossbase 1.01 database.[2] The comparative experimental results are showed in Fig. 1. The experimental results show that these native definitions negatively affect the blind detection resistance. It is due to the sensitivity of the DCT coefficients in the JPEG image, and the above distortion functions can hardly express the ternary distortion of +1 and −1 modification. Thus, we attempt to define a proper ternary ±1 distortion function in another way.

First, We start from the rounding error $\boldsymbol{e}$ which is used in the existing side-informed JPEG steganographic algorithms. Because the rounding error is related to the distortion introduced by the rounding process in JPEG compression, we define +1 and −1 modification errors $\boldsymbol{me}^{+1}=\left\{me_{i,j}^{+1(t)}|i,j,t\right\}$ and $\boldsymbol{me}^{-1}=\left\{me_{i,j}^{-1(t)}|i,j,t\right\}$ as

$$me_{i,j}^{+1(t)}=\left|d_{i,j}^{\mathrm{qdrd}(t)}+1-d_{i,j}^{qd(t)}\right|,\quad 1\le i,j\le 8,\quad t=1,...,M, \tag{17}$$

$$me_{i,j}^{-1(t)}=\left|d_{i,j}^{\mathrm{qdrd}(t)}-1-d_{i,j}^{qd(t)}\right|,\quad 1\le i,j\le 8,\quad t=1,...,M. \tag{18}$$

They are related to the distortion caused by +1 or −1 modification on DCT coefficients. Because the quantized DCT coefficient $d_{i,j}^{qd(t)}$ is divided by the corresponding element $q_{i,j}^{QF}$ in quantization table $\boldsymbol{Q}_{8\times 8}^{QF}$, we believe that the proper ternary distortion function need to take account of the effect of the divisor $q_{i,j}^{QF}$.

Moreover, a proper distortion function requires considering the difference of secure capacity on different cover elements when sharing the embedding payload on each cover elements. A clever way is to learn from the binary distortion function $\rho_{i,j(\mathrm{binary})}^{(t)}$ in the renowned side-informed JPEG steganographic algorithm. Thus, we propose a ternary ±1 distortion function in such construction:

$$\rho_{\mathrm{proper}}^{(t)}\left(y_{i,j}^{(t)}\right)=\begin{cases}\rho_{i,j(\mathrm{binary})}^{(t)}\times q_{i,j}^{QF}\times me_{i,j}^{+1(t)}, & y_{i,j}^{(t)}=x_{i,j}^{(t)}+1,\\ \rho_{i,j(\mathrm{binary})}^{(t)}\times q_{i,j}^{QF}\times me_{i,j}^{-1(t)}, & y_{i,j}^{(t)}=x_{i,j}^{(t)}-1,\\ 0 & , \quad y_{i,j}^{(t)}=x_{i,j}^{(t)}.\end{cases} \tag{19}$$

Thus, this distortion function is used on SI-UNIWARD algorithm and the comparative experimental results are shown in Fig. 1 which are obtained on 10,000 random chosen images with quality factor 85 from BOSSbase 1.01 database and DCTR [13] feature library. From the results, the ternary ±1 distortion function (19) cannot increase the resistance. The reason may be due to the immaturity of the distortion function definition. Thus, how to define proper ternary ±1 distortion function is the most important problem to increase the blind detection resistance of side-informed JPEG steganographic algorithm. This is the second motivation of this paper.

[2] Proposed by Patrick Bas, Tomas Filler, Tomas Pevny in ICASSP 2013, contains 10,000 512×512 grayscale images, available: http://agents.fel.cvut.cz/stegodata/

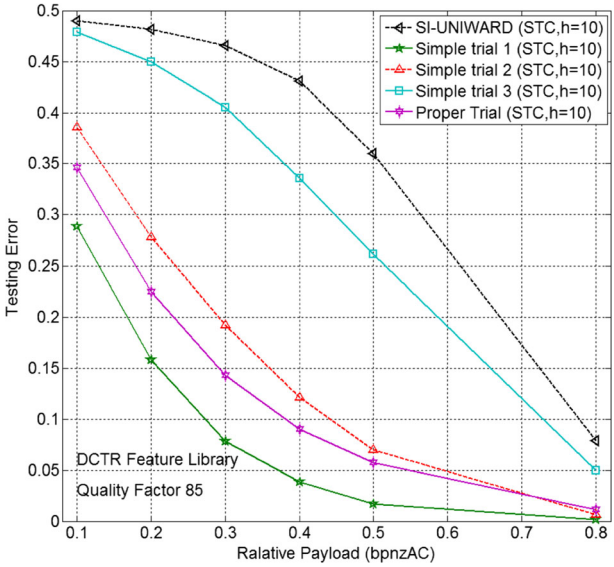

Fig. 1 Experimental results of trials on SI-UNIWARD [14] (quality factor 85)

4 Two-dimensional decomposition embedding method

In this section, a novel method named two-dimensional decomposition embedding method is proposed to define ternary ±1 distortion function in a refined way. The proposed method is based on the decomposition of ternary entropy. Through the 2D-DEM, the problem of defining ternary ±1 distortion function is transformed into defining two binary distortion functions on two layers. The distribution forms of minimal distortion on each layer, proofs and an example are presented as follows.

4.1 Double-layered decomposition of ternary ±1 embedding

Based on the definitions given in Section 2, additional symbolic definition of ternary ±1 embedding under additive distortion are provided to elucidate the proposed method:

Suppose the sender embeds secret message $\boldsymbol{m}$ of l bits in length into n-bit length cover object $\boldsymbol{x}$ through ternary ±1 embedding. As a result, stego object $\boldsymbol{y} = \{y_i\}_{1\le i\le n}$, $y_i \in \mathrm{I}_s^i$ is obtained. Because cover object elements are changed in a ± 1 manner, $\mathrm{I}_s^i = \{y_i^0,\ y_i^1,\ y_i^2\}$ with $y_i^0 = x_i - 1,\ y_i^1 = x_i,\ y_i^2 = x_i + 1$. We consider all cover object elements as independent of each other in an additive distortion situation. Thus, we use symbols $p_i^- = \pi_i(y_i^0),\ p_i^0 = \pi_i(y_i^1),\ p_i^+ = \pi_i(y_i^2)$ to denote probabilities of changing x_i to $y_0^i,\ y_1^i,\ y_2^i$ which means $p_i^- + p_i^0 + p_i^+ = 1$. If the sender modifies x_i under $\{p_i^-, p_i^0, p_i^+\}$, the maximal information payload of x_i is $\mathrm{H}(\pi_{ij}(\mathrm{I}_s^{ij})) = -\left(p_{ij0}\log_2 p_{ij0} + p_{ij-}\log_2 p_{ij-} + p_{ij+}\log_2 p_{ij+}\right)$ bits. Thus, the maximal payload of $\boldsymbol{x}$ in this situation is $P = \sum_{1\le i\le n}\mathrm{H}(\pi(\mathrm{I}_s^i))$ bits.

Then, based on the ternary entropy definition, $\mathrm{H}\left(\pi\left(\mathrm{I}_s^i\right)\right)$ is decomposed into a sum of two binary entropies as

$$\begin{aligned}\mathrm{H}\left(\pi\left(\mathrm{I}_s^i\right)\right) &= -\left(p_i^0\log_2 p_i^0 + p_i^-\log_2 p_i^- + p_i^+\log_2 p_i^+\right)\\ &= \mathrm{H}_2\left(p_i^0\right) - \left(1-p_i^0\right)\left(\tilde{p}_i^-\log_2 p_i^- + \tilde{p}_i^+\log_2 p_i^+ - \log_2\left(1-p_i^0\right)\right)\\ &= \mathrm{H}_2\left(p_i^0\right) - \left(1-p_i^0\right)\left(\tilde{p}_i^-\log_2 \tilde{p}_i^- + \tilde{p}_i^+\log_2 \tilde{p}_i^+\right)\\ &= \mathrm{H}_2\left(p_i^0\right) + \left(1-p_i^0\right)\mathrm{H}_2\left(\tilde{p}_i^-\right)\end{aligned} \tag{20}$$

Symbols $\tilde{p}_i^-$ and $\tilde{p}_i^+$ denote $p_i^-/\left(p_i^- + p_i^+\right)$ and $p_i^+/\left(p_i^- + p_i^+\right)$, respectively with $\tilde{p}_i^- + \tilde{p}_i^+ = 1$. $\tilde{p}_i^-$ and $\tilde{p}_i^+$ are conditional probabilities of +1 and −1 modifications under the situation of a changing x_i. Note that the probabilities of changing x_i are $1-p_i^0$ and p_i^0 with $1-p_i^0 = p_i^- + p_i^+$. We decompose ternary ±1 embedding into double-layer binary embedding as outlined below:

First, the sender embeds l' ($l' < l$) bits of $\boldsymbol{m}$ in the first layer, the conditional probabilities of $\tilde{p}_i^-$, $\tilde{p}_i^+$ on each cover element are calculated. ($\left\{\tilde{p}_i^-,\ \tilde{p}_i^+\right\}_{1\le i\le n}$ are conditional probabilities; thus, it is difficult to unify l' on different images. Accordingly, we use distribution parameter β which is introduced in the second part of Section 4 to control l' in general expressions.) Second, the remainder of $\boldsymbol{m}$ is embedded in the second layer, $1-p_i^0$, p_i^0on each of the cover elements, which are given after embedding the first layer. Meanwhile, we define a corresponding additive two-dimensional distortion profile on these two layers as relative distortion (RD) $\{\rho_{RD}(y_i)\}_{1\le i\le n}$ and basic distortion (BD) $\{\rho_{BD}(y_i)\}_{1\le i\le n}$. (Henceforth, we refer to the first and second layer as the RD layer and BD layer, respectively.) $\{\rho_{RD}(y_i)\}_{1\le i\le n}$ implies the distortion between the +1 and −1 modification on x_i, while $\{\rho_{BD}(y_i)\}_{1\le i\le n}$ are distortion values of changing x_i

$$\rho_{RD}(y_i) = \begin{cases} \rho_i^{RD-}, y_i = x_i - 1, \\ \rho_i^{RD+}, y_i \neq x_i + 1. \end{cases} \tag{21}$$

$$\rho_{BD}(y_i) = \begin{cases} 0, & y_i = x_i, \\ \rho_i^{BD}, & y_i \neq x_i. \end{cases} \tag{22}$$

Then, $D_R(\boldsymbol{y}) = \sum_{1\le i\le n}\rho_{RD}(y_i)$ and $D_B(\boldsymbol{y}) = \sum_{1\le i\le n}\rho_{BD}(y_i)$ on account of the assumption that $D_R(\boldsymbol{y})$ and $D_B(\boldsymbol{y})$ are both additive. The average values $E(D_B)$ and $E(D_R)$ on random variable $\boldsymbol{Y}$ are

$$E(D_R) = \sum_{\boldsymbol{y}} \pi(\boldsymbol{y}) D_R(\boldsymbol{y}) = \sum\nolimits_{1\le i\le n}\sum\nolimits_{y_i\in\{x_i-1, x_i+1\}} \pi_i(y_i)\rho_{RD}(y_i), \tag{23}$$

$$E(D_B) = \sum_{\boldsymbol{y}} \pi(\boldsymbol{y}) D_B(\boldsymbol{y}) = \sum\nolimits_{1\le i\le n}\sum\nolimits_{y_i\in\{x_i, x_i\pm 1\}} \pi_i(y_i)\rho_{RD}(y_i). \tag{24}$$

And, the distribution probabilities $\left\{\tilde{p}_i^-,\ \tilde{p}_i^+\right\}_{1\le i\le n}$ which minimize $E(D_R)$, and $\left\{1-p_i^0,\ p_i^0\right\}_{1\le i\le n}$, which minimize $E(D_B)$, should be calculated. The calculation processes on these two layers differ; therefore, we respectively introduce the processes in the following parts.

4.2 Calculation of distribution with minimal RD on the first layer

Because $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$ are conditional probabilities, and probabilities $\{p_i^0\}_{1\le i\le n}$ are not certain, it is inconvenient for the sender to set the payload length, $l' = \sum_{1\le i\le n}(1-p_i^0)\mathrm{H}_2(\tilde{p}_i^-)$, on different images. Thus, we introduce β (named as distribution parameter) to control l' on the RD layer in another manner. β relates to information entropy of $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$, which are denoted as objective relative payload (ORP) $\mathrm{ORP} = \sum_{1\le i\le n}\mathrm{H}_2(\tilde{p}_i^-) = \beta\times n$ bits. β is a real number in range [0, 1]. Note that ORP is not the final payload on the RD layer after completing 2D-DEM embedding because $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$ are conditional probabilities.

Different values of β result in different $\boldsymbol{y}$. By setting β over [0, 1], an embedding result is obtained which is equal to binary embedding, typical ternary ±1 embedding (probabilities of +1 and −1 are equal) and ternary ±1 embedding that the probabilities of +1 and −1 are not equal all the time. If we set β=0, the embedding result is equal to the binary ±1 embedding method used in PQ, MME-DCT, NPQ, EBS and SI-UNIWARD algorithms. It reaches the one bit payload on each cover element. When we set $\beta\neq 0$, a larger value of β implies more information is concealed in this layer. When β=1, the maximum value, it means that the probabilities of the +1 and −1 modification are equal on each element, and the capacity on x_i can reach up to $\log_2 3$ in the condition of $p_i^0 = 1/3$. This case is often used in JPEG steganographic algorithm without a precover, such as DASS-DCT [], UED [12] and J-UNIWARD [14].

After β is set, ORP is determined and $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$ corresponding to the average minimal relative distortion can be calculated. It is obvious that $\{\rho_{RD}(y_i)\}_{1\le i\le n}$ and ORP obey the conditions in the first part of Section 2. The probabilities $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$ result in minimal $E(D_R)$ can be determined as follows:

$$\tilde{p}_i^- = \frac{\exp\left(-\lambda_1\rho_i^{RD-}\right)}{\exp(-\lambda_1\rho_i^{RD-}) + \exp\left(-\lambda_1\rho_i^{RD+}\right)}, \tag{25}$$

$$\tilde{p}_i^+ = \frac{\exp\left(-\lambda_1\rho_i^{RD+}\right)}{\exp(-\lambda_1\rho_i^{RD-}) + \exp\left(-\lambda_1\rho_i^{RD+}\right)}.$$

Moreover, λ_1 satisfies $\sum_{1\le i\le n}\mathrm{H}_2(p'_{i-}) = \beta\times n$ bits and can be determined through a binary search method.

4.3 Calculation of distribution with minimal BD on the second layer

In this section, probabilities $\{1-p_i^0,\ p_i^0\}_{1\le i\le n}$, which minimize $E(D_B)$ with a payload of $l-l'$ bits, is calculated. Because conditional probabilities $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$ are determined in the second part of Section 4, information entropies $\{\mathrm{H}_2(\tilde{p}_i^-)\}_{1\le i\le n}$ are constant in the remainder of this section.

The payload on the second layer, denoted as objective basic payload (OBP), is information entropy expressed as $OBP = \sum_{1\le i\le n}\mathrm{H}_2(p_i^0)$. The optimal probabilities $\{1-p_i^0,\ p_i^0\}_{1\le i\le n}$ that cause minimal $E(D_B)$ are in the following forms:

$$\begin{aligned} p_i^0 &= \frac{1}{1+\exp\left(-\lambda_2\rho_i^{BD}+\mathrm{H}_2\left(\tilde{p}_i^-\right)\right)} \quad , \\ 1-p_i^0 &= \frac{\exp\left(-\lambda_2\rho_i^{BD}+\mathrm{H}_2\left(\tilde{p}_i^-\right)\right)}{1+\exp\left(-\lambda_2\rho_i^{BD}+\mathrm{H}_2\left(\tilde{p}_i^-\right)\right)}. \end{aligned} \tag{26}$$

To determine the proper value of λ_2 in Formula (26), a binary search method is employed under constraint $OBP = l(\text{bits}) - \sum_{1\le i\le n}\left(1-p_i^0\right)\mathrm{H}_2\left(\tilde{p}_i^-\right)$. The validity of Formula (26) is demonstrated as follows.

4.3.1 Proof of optimal distribution

Before proving Formula (26), we list the corresponding conditions and problem.

Condition 1: Probabilities $\left\{\tilde{p}_i^-,\ \tilde{p}_i^+\right\}_{1\le i\le n}$ are constant. Symbol ent_i is used to denote entropy $\mathrm{H}_2\left(\tilde{p}_i^-\right)$ which is in the range [0, 1] bits.
Condition 2: Probabilities $\left\{1-p_i^0,\ p_i^0\right\}_{1\le i\le n}$ contain OBP bits information.
Condition 3: $D_B(\boldsymbol{y})$ is additive ($D_B(\boldsymbol{y}) = \sum_{1\le i\le n}\rho_{BD}(y_i)$ and $\{\rho_{BD}(y_i)\}_{1\le i\le n}$ are positive.
Problem: How to find probabilities $\left\{1-p_i^0,\ p_i^0\right\}_{1\le i\le n}$ that cause minimal average distortion $E(D_B)$:

$$E(D_B) = \sum\nolimits_{1\le i\le n}\left(p_i^0\times 0 + \left(1-p_i^0\right)\times\rho_i^{BD}\right) = \sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)\rho_i^{BD} \tag{27}$$

which is subjected to constraints

$$0\le p_i^0\le 1\ \ ,\ \ n\in\boldsymbol{Z}, \tag{28}$$

$$\rho_{BD}(y_i) = \begin{cases} 0, & y_i = x_i \\ \rho_i^{BD}, & y_i\ne x_i \end{cases},\ \ i = 1,2,...,n \tag{29}$$

$$OBP + \sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)e_i = \sum\nolimits_{1\le i\le n}\mathrm{H}_2\left(p_i^0\right) + \sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)ent_i = l\ \text{bits}, \tag{30}$$

For the derivation process of Formula (26), on *Condition 3*, the problem can be solved by the *Lagrange multiplier method* by introducing parameter μ and multivariate function $F\left(p_1^0,p_2^0,...,p_i^0,..,p_n^0\right)$. Let

$$F\left(p_1^0,p_2^0,...,p_i^0,..,p_n^0\right) = \sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)\rho_i^{BD} + \mu\left[l-\sum\nolimits_{1\le i\le n}\mathrm{H}_2\left(p_i^0\right)-\sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)ent_i\right] \tag{31}$$

Then, the partial derivative of F on variate p_i^0, $1 \le i \le n$,

$$\frac{\partial F\left(p_1^0, p_2^0, ..., p_i^0, .., p_n^0\right)}{\partial p_i^0} = -\rho_i^{BD} + \mu\left[\log_2 p_i^0 - \log_2\left(1-p_i^0\right) + e_i\right] = 0, \tag{32}$$

if and only if $\left\{p_i^0 = 1/\left(1+\exp\left(-\rho_i^{BD}/\mu + e_i\right)\right)\right\}_{1\le i\le n}$. Owing to Constraint (29), function F reaches a minimum, which is minimal $E(D_B)$ under Constraint (30) at this point. After denoting symbol $\lambda_2 = 1/\mu$ and replacing ent_i by $\mathrm{H}_2\left(\tilde{p}_i^-\right)$, Formula (26) is obtained. Then, the feasibility of the binary search method on λ_2 is due to monotonicity of $\left\{OBP + \sum_{1\le i\le n}\left(1-p_i^0\right)\mathrm{H}_2\left(\tilde{p}_i^-\right)\right\}_{\lambda_2}$ on λ_2, which is proved as follows.

4.3.2 Proof of feasibility on the binary search method

Functions $G(\lambda_2)$ and $G_i(\lambda_2)$ are defined on variate λ_2 as

$$G(\lambda_2) = \sum\nolimits_{1\le i\le n}\left(p_i^0\log_2 p_i^0 + \left(1-p_i^0\right)\log_2\left(1-p_i^0\right)\right) + \sum\nolimits_{1\le i\le n}\left(1-p_i^0\right)ent_i \tag{33}$$

and

$$G_i(\lambda_2) = -\left(p_i^0\log_2 p_i^0 + \left(1-p_i^0\right)\log_2\left(1-p_i^0\right)\right) + \left(1-p_i^0\right)ent_i \tag{34}$$

It is obvious that $G(\lambda_2) = \sum_{1\le i\le n} G_i(\lambda_2)$. Then, we substitute $\left\{\ p_i^0\right\}_{1\le i\le n}$ in (34) using Formula (26):

$$\begin{aligned} G_i(\lambda_2) = {} & \frac{\log_2\left(1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)\right)}{1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)} \\ & + \frac{\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}{1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}\left(ent_i - \log_2\left(\frac{\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}{1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}\right)\right) \end{aligned} \tag{35}$$

The first order derivatives of $G_i(\lambda_2)$ and $G(\lambda_2)$ are

$$G_i'(\lambda_2) = -\frac{\rho_i^{BD}\left(ent_i\ln 2 + \lambda_2\rho_i^{BD} - ent_i\right)\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}{\left(1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)\right)^2\ln 2} \tag{36}$$

and

$$\begin{aligned} G'(\lambda_2) &= \sum\nolimits_{1\le i\le n} G_i'(\lambda_2) \\ &= -\sum\nolimits_{1\le i\le n}\frac{\rho_i^{BD}\left(ent_i\ln 2 + \lambda_2\rho_i^{BD} - ent_i\right)\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)}{\left(1+\exp\left(-\lambda_2\rho_i^{BD} + ent_i\right)\right)^2\ln 2} \end{aligned} \tag{37}$$

Distortion values $\{\rho_{BD}(y_i)\ge 0\}_{1\le i\le n}$ are positive, $G_i'(\lambda_2)>0$ in domain $(-\infty, (1-\ln 2)\ ent_i/\rho_i^{BD})$, and $G_i'(\lambda_2)<0$ in domain $((1-\ln 2)\ ent_i/\rho_i^{BD},\ +\infty)$. Thus, $G_i(\lambda_2)$ reaches a maximum on $\lambda_2 = (1-\ln 2)\ ent_i/\rho_i^{BD}$ with the fact that $G_i(\lambda_2) \to^{\lambda_2\to+\infty} 0$, which guarantees that the binary search method on λ_2 is feasible.

After the calculation on the BD layer, the corresponding ternary ±1 modification probabilities $\{p_i^-, p_i^0, p_i^+\}_{1\le i\le n}$ are obtained by combining probabilities $\{1-p_i^0,\ p_i^0\}_{1\le i\le n}$ and $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le n}$:

$$\begin{cases} p_i^- = (1-p_i^0)\times \tilde{p}_i^-, \\ p_i^0 = 0 \\ p_i^+ = (1-p_i^0)\times \tilde{p}_i^+. \end{cases} \tag{38}$$

4.4 Example

Although the proposed method is somewhat complex in the theoretical proofs, the procedure of calculations is clear in the actual embedding procedure. Therefore, a simple example is provided.

Suppose a sender owns a cover object of integer DCT coefficients $\boldsymbol{a}$=(2,3,4,5), which is rounded from $\boldsymbol{a}$'=(1.8,3.1,4.4,5.3). The sender intend to embed two bits message into the cover object $\boldsymbol{a}$ and a stego object $\boldsymbol{b}$is obtained. The RD and BD functions can be defined as

$$\rho_{RD}(b_i) = \begin{cases} |a_i - 1 - a'_i|, & b_i = a_i - 1, \\ |a_i + 1 - a'_i|, & b_i = a_i + 1, \end{cases} \tag{39}$$

$$\rho_{BD}(b_i) = \begin{cases} 0, & b_i = a_i, \\ |a_i - a'_i|, & b_i \neq a_i. \end{cases} \tag{40}$$

Then, the calculations of the optimal probabilities that cause the minimal values of RD and BD functions is processed as follows. First, distribution β=0.75 is set, and the probabilities $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le 4}$ that can minimize RD is calculated through Formula (25). The λ_1 of Formula (25) is determined as λ_1=2.5139 which satisfies the equation $ORP = \sum_{1\le i\le 4} \mathrm{H}_2(\tilde{p}_i^-) = 0.75\times 4 = 3$. Thus, $\{\tilde{p}_i^-,\ \tilde{p}_i^+\}_{1\le i\le 4}$ is $\{0.7321, 0.2679\}_1$, $\{0.3769, 0.6231\}_2$, $\{0.1180, 0.8820\}_3$, and $\{0.1812, 0.8188\}_4$.

Then, probabilities $\{1-p_i^0,\ p_i^0\}_{1\le i\le 4}$, which cause the minimal value of BD are calculated through Formula (26). The λ_2 of Formula (26) is determined as λ_2=2.8124 which satisfies $OBP = 2(\text{bits}) - \sum_{1\le i\le 4}(1-p_i^0)\mathrm{H}_2(\tilde{p}_i^-)$. Thus, $\{1-p_i^0,\ p_i^0\}_{1\le i\le 4}$ is $\{0.1960, 0.8040\}_1$, $\{0.1055, 0.8945\}_2$, $\{0.0319, 0.9681\}_3$, and $\{0.0486, 0.9514\}_4$.

Last, the ternary probabilities $\{p_i^-,\ p_i^0,\ p_i^+\}_{1\le i\le 4}$, which cause minimal values of RD and BD functions, are obtained by Formula (38):

$$\begin{cases} p_1^- = 0.1435, \\ p_1^0 = 0.8040, \\ p_1^+ = 0.0525, \end{cases}, \begin{cases} p_2^- = 0.0398, \\ p_2^0 = 0.8945, \\ p_2^+ = 0.0657, \end{cases}, \begin{cases} p_3^- = 0.0038, \\ p_3^0 = 0.9681, \\ p_3^+ = 0.0281, \end{cases}, \begin{cases} p_4^- = 0.0088, \\ p_4^0 = 0.9514, \\ p_4^+ = 0.0398, \end{cases}. \tag{41}$$

Furthermore, how to embed the message using the optimal probabilities $\{p_i^-,\ p_i^0,\ p_i^+\}_{1\le i\le n}$ calculated by the 2D-DEM? Because the steganographic embedding code, such as STCs or BCH, needs a distortion function in the process, we can convert

the probabilities into an equivalent ternary ±1 distortion function through by inversing the formula (4). It means that the equivalent ternary ±1 distortion function $\left\{\rho_i^-, \rho_i^0, \rho_i^+\right\}_{1\le i\le n}$is calculated by:

$$\begin{cases} \rho_i^- = -\log\left(p_i^-/p_i^0\right), \\ \rho_i^0 = 0 \\ \rho_i^+ = -\log\left(p_i^+/p_i^0\right). \end{cases}, \tag{42}$$

5 Procedure of improving side-informed JPEG steganography by 2D-DEM

In this section, the proposed 2D-DEM is applied to improve the well-known side-informed JPEG steganographic algorithms, NPQ, EBS, and SI-UNIWARD. First, the improvement procedure and definitions are presented. Then, discussion about setting proper parameter values is provided.

5.1 Improvement procedure

Under the framework of NPQ, EBS and SI-UNIWARD methods, an improvement method based on 2D-DEM is proposed. In Fig. 2, the procedure of the improved side-informed JPEG steganographic algorithm based on the proposed 2D-DEM method is presented. In the side of sender, first, the side-information and the DCT coefficients are respectively extracted from the precover and JPEG cover object. Then, based on the proposed method (2D-DEM), the sender defines a ternary ±1 distortion function after setting the values of β and T. In the next step, steganographic coder, STCs is applied embed the secret messages into the DCT coefficients with the ternary distortion corresponding (multi-layer STCs is used for ternary distortion function). Last, the DCT coefficients are packed into JPEG format, and transmitted to receiver through a public channel. In the side of receiver, the DCT coefficients that contains the secret

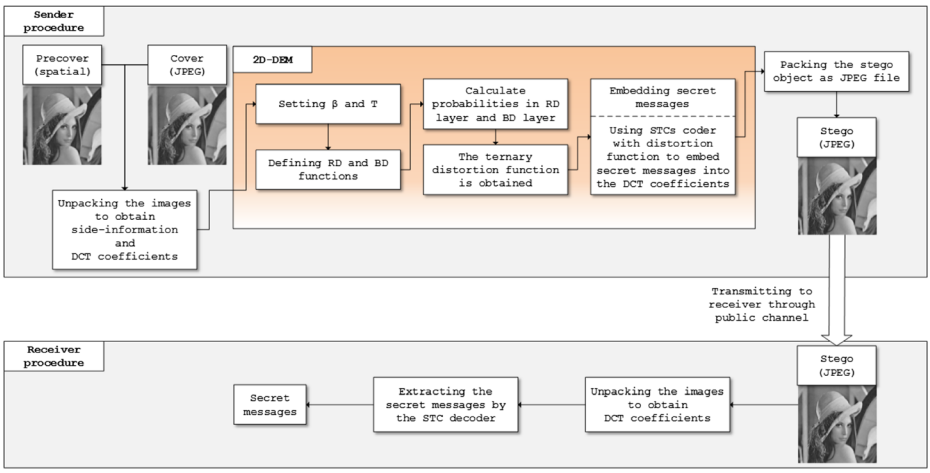

Fig. 2 Procedure of side-informed JPEG steganography based on 2D-DEM

messages are obtained by unpacking the stego images first. Then, the messages are extracted from the coefficients based on the STCs decoding algorithm.

In the following lines, the details of applying the proposed 2D-DEM to the NPQ, EBS and SI-UNIWARD are presented. First, in the BD layer of 2D-DEM, the basic distortion function $\left\{\rho_{BD}\left(y_{i,j}^{(t)}\right)|1\leq i,\ \ j\leq 8,\ \ t=1,...,M\right\}$ is defined based on the original distortion function of the side-informed JPEG steganographic algorithm.

Then, in the RD layer of 2D-DEM, RD function $\left\{\rho_{RD}\left(y_{i,j}^{(t)}\right)|1\leq i,j\leq 8,t=1,...,M\right\}$ is defined to describe the relative distortion between +1 and -1 based on the Equation (19) in Section 3.2. Meanwhile, because the JPEG image is sensitive to modification on the DCT coefficient, some DCT coefficients with large difference between distortions caused by +1 and −1 modification on them are unsuitable for using ternary ±1 embedding. And, the larger value of $|e_{i,j}^{(t)}|$ implies a greater difference. Thus, we introduce a threshold, $0\leq T\leq 0.5$, on rounding error $|e_{i,j}^{(t)}|$ to control the number of the DCT coefficients used ternary ±1 embedding.

Last, we use $x_{i,j}^{(t)}$ to denote $d_{i,j}^{\mathrm{qdrd}(t)}$ and $me_{i,j}^{+1(t)}$, $me_{i,j}^{-1(t)}$ of Formula (17,18) to denote the modification error in the side-informed JPEG steganographic algorithm, and the BD function $\left\{\rho_{BD}\left(y_{i,j}^{(t)}\right)|1\leq i,j\leq 8,t=1,...,M\right\}$ and RD function $\left\{\rho_{RD}\left(y_{i,j}^{(t)}\right)|1\leq i,j\leq 8,t=1,...,M\right\}$ for improving NPQ, EBS and SI-UNIWARD algorithms based on the 2D-DEM are defined as

$$\begin{aligned}\rho_{BD}^{NPQ}\left(y_{i,j}^{(t)}\right)&=\rho_{i,j}^{1},\\ \rho_{BD}^{EBS}\left(y_{i,j}^{(t)}\right)&=\rho_{i,j}^{2},\\ \rho_{BD}^{SI-\mathrm{UNIWARD}}\left(y_{i,j}^{(t)}\right)&=\rho_{i,j}^{3},\end{aligned}\tag{43}$$

and

$$\rho_{RD}\left(y_{i,j}^{(t)}\right)=\begin{cases}q_{i,j}\times me_{i,j}^{-1(t)}, & y_{i,j}^{(t)}=y_{i,j}^{(t)}-1,\ \ \left|e_{i,j}^{(t)}\right|<T,\\ q_{i,j}\times me_{i,j}^{+1(t)}, & y_{i,j}^{(t)}=y_{i,j}^{(t)}+1,\ \ \left|e_{i,j}^{(t)}\right|<T,\\ q_{i,j}\times me_{i,j}^{-1(t)}, & y_{i,j}^{(t)}=y_{i,j}^{(t)}-1,\ \ \left|e_{i,j}^{(t)}\right|<-T,\\ +\infty\quad\quad\quad, & y_{i,j}^{(t)}=y_{i,j}^{(t)}+1,\ \ \left|e_{i,j}^{(t)}\right|<-T,\\ +\infty\quad\quad\quad, & y_{i,j}^{(t)}=y_{i,j}^{(t)}-1,\ \ \left|e_{i,j}^{(t)}\right|\geq T,\\ q_{i,j}\times me_{i,j}^{+1(t)}, & y_{i,j}^{(t)}=y_{i,j}^{(t)}+1,\ \ \left|e_{i,j}^{(t)}\right|\geq T.\end{cases}\tag{44}$$

And then, Fig. 3 shows an example of applying 2D-DEM on SI-UNIWARD algorithm after setting β and T. The cover image is chosen from the BOSSbase 1.01 database, and the stego image is obtained after embedding 0.2 bpnzAC secret messages by the improved steganographic algorithm. The changes in the DCT domain and spatial domain are respectively shown in the Fig. 3.

Actually, the threshold T and distribution parameter β are determined by the sender. After sender uses them to define ternary distortion function, STCs is implemented in the embedding process for its near-optimal performance. Because STCs uses a parity-check matrix shared by

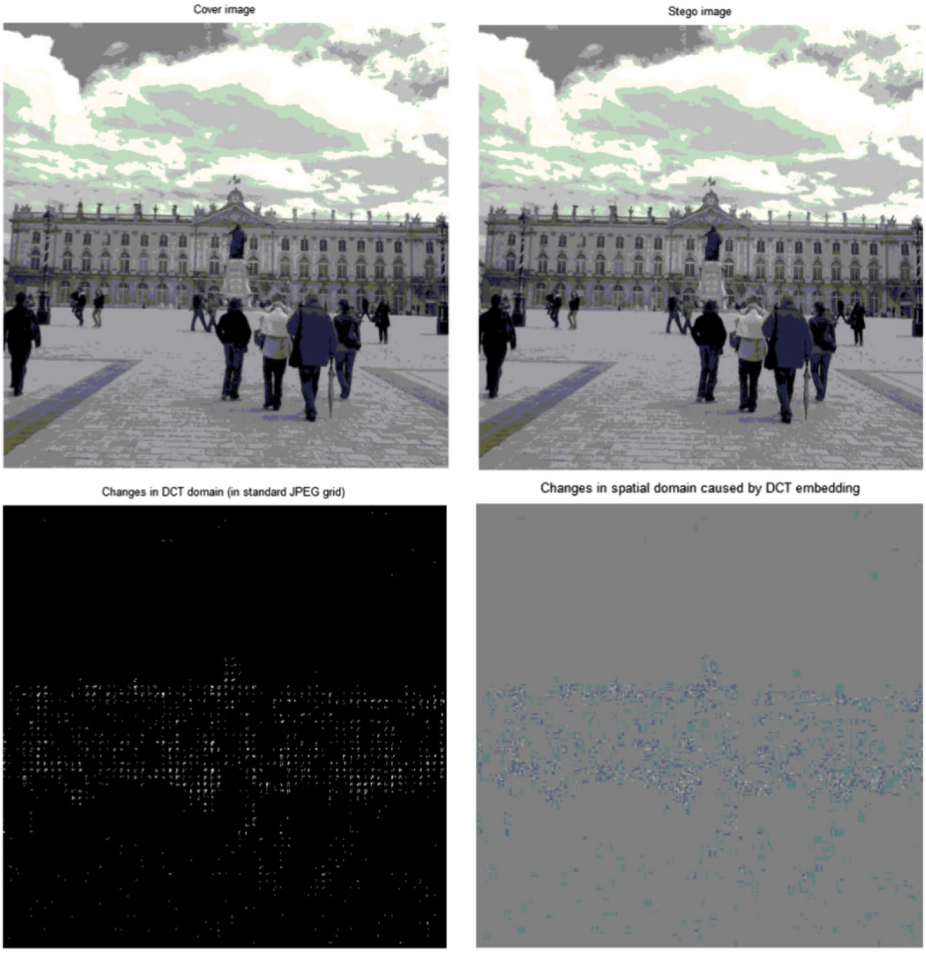

Fig. 3 Example of cover (*upper-left*) and stego(*upper-right*) images (0.2bpnzAC payload) produced by the proposed method on SI-UNIWARD. The bottom-left figure shows the changes in the DCT domain, and the bottom-right figure shows the changes in the spatial domain

the sender and receiver in embedding and extraction processes, the receiver can extract the secret message through the STCs extraction process without knowing information of T and β (multiple the bit-vector of stego object by the matrix). In the next, the method of setting proper values of T and β is described.

5.2 Setting parameter values

Two parameters T and β, exist in the proposed improvement method for defining proper ternary ±1 distortion function. Different values considerably affect the detection resistance of side-informed JPEG steganographic algorithm. Parameter T controls the size of the cover elements that use ternary ±1 embedding. If we set T to a maximum value of 0.5, ternary ±1 embedding is used on each cover element. In this situation, 2D-DEM will become too sensitive to the value of β because too many.

unsuitable cover elements are included. High-level sensitivity will make it difficult to find proper value of β by empirical approaches.

To determine the value of T, a test on 1000 512×512 grayscale images with different quality factors (75, 85 and 95) is conducted. The images are chosen randomly from the BOSSbase 1.01 database. First, the average number of coefficients satisfying $|e_{i,j}^{(t)}| < T$ with different T values is presented in Fig. 4. From the figure, the average rates between cover elements satisfying T and whole elements are increasing on the value of T. Meanwhile, based on the experimental result in the second part of Section 6, $T = 0.1$ is suggested.

After parameter T is determined, we focus on the value of β. We use an empirical approach that chooses a proper image among a set of candidates (denoted as the candidates choosing method, brief as CC method) to find the proper value of β. The CC method is simple: First, a set of candidate stego objects for a cover object is created by embedding the same message in the cover object with different values of β.[3] Then, a stego object with the highest relationship to the cover object is chosen. We use spatial Euclidean distance to measure the relationship between the cover object and stego object (he JPEG object is decomposed to the spatial domain).

Then, we make tests of counting the β value of the chosen object based on the SI-UNIWARD algorithm with the improvement method outlined in the first part of Section 5. 1000 512×512 grayscale images from the BOSSbase 1.01 database were used with different quality factors (75, 85 and 95). In the experiment, $T = 0.1$ is fixed and β changed from 0 to 1 with 0.05 intervals. The results of mean β values were 0.5133 (qf75), 0.5349 (qf85) and 0.6432(qf95). In Section 6, additional experiments substantiate this result in several aspects.

6 Experiments

In this section, experiments on 2D-DEM parameters, blind detection resistance and computation complexity are presented. First, their environments and setups are described as follows.

6.1 Experimental setups

The experiments were conducted on a personal computer with an Intel Core i7-4700MQ CPU at 2.4G Hz and the Windows 7 operating system. In the blind detection resistance experiment, we randomly selected images to be the "precover" from the BOSSbase 1.01 database (containing 10,000 512×512 grayscale images obtained from eight different cameras). Then, JPEG cover images under quality factors of 75, 85, and 95 were respectively obtained through JPEG compression. The steganographic codes focuses on reducing the difference between optimal embedding and practical results (This difference is called coding loss [3]). As STCs and multilayered STCs [3] (proposed by Filler, Judas and Fridrich) can embed the message with nearly optimal coding performance, multilayered STCs coding method was applied with the recommended value parameter of $h = 10$ in the experiments.

[3] Actually, the value of T can also be changed in the CC method, but this will significantly increase the number of the candidate images, and the experimental results showed in the Fig. 5 implies that the effect of T-value stay steady in [0.1,0.3], thus, the CC method just changes the values of β.

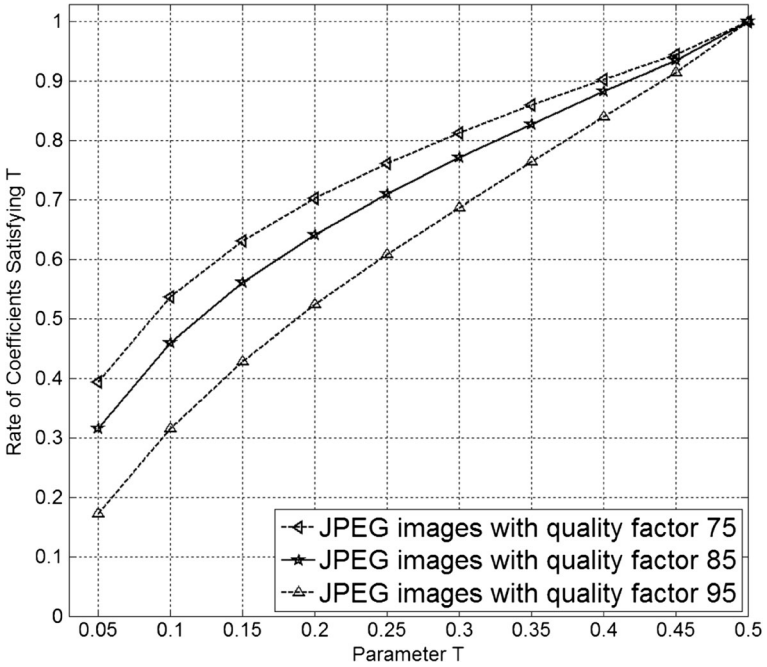

Fig. 4 Experimental results of counting rates of coefficients satisfying parameter T on images

The blind detection experiments were comprised of blind detection features and a classifier. To train the ensemble classifier, 3 detection feature libraries were chosen: ccPEV274 [21] (548 dimensions), J + SRM [22] (35,263 dimensions) and DCRT [13] (8000 dimensions).

The ensemble classifier with the Fisher linear discriminant base learner [24] was implemented with default parameters (The number of cover objects was equal to that of stego objects on both training and testing set). It is an automatic framework with an efficient utilization of 'out-of-bag' error estimates for the stopping criterion. In the training step, the decision threshold of each base learner was adjusted to minimize the total detection error under equal priors on the training set:

$$P_E = \min_{P_{FA}} \frac{1}{2}\left(P_{FA} + P_{MD}(P_{FA})\right) \tag{45}$$

where P_{FA} and P_{MD} are the false alarm rate and missed detection rate, respectively. In the testing step, we used Detection Error Rates (*DER*), which are average values of $(P_{FA}+P_{MD}(P_{FA}))/2$ over 20 random training/testing splits to express the detection results. (On each split, half randomly chosen images were used to train classifier and the other half images were used to test the detection ability of classifier, and the ratio of cover and stego object numbers is 1:1).

6.2 Experiments of parameters

T and β are two important parameters of the proposed ternary ±1 distortion function. As the proper parameter values were demonstrated in the second part of Section 5, the experimental results that substantiate them are presented below. In this section, *DER* results that express the blind detection resistance were obtained by using ensemble classifier and ccPEV feature library

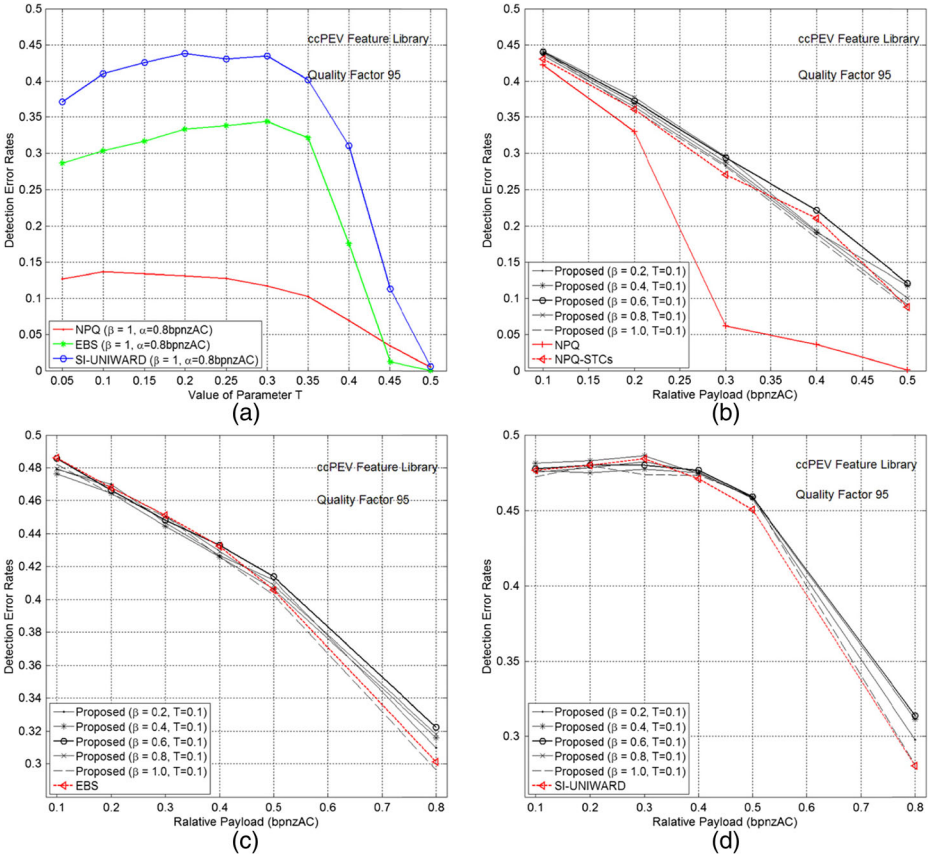

Fig. 5 Experimental results under ccPEV [21] feature library (JPEG images with quality factor 95). **a** is the comparison results on parameter T, and the (**b**, **c**, **d**) are the comparison result on parameter β when use the 2D-DEM method on NPQ, EBS and SI-UNIWARD respectively

on 3000 randomly chosen images (compressed from the corresponding spatial images of BOSSbase database with quality factor 95), and the embedding processes were STCs with $h = 10$.

First, β=1, and T was changed from 0.05 to 0.5 with 0.05 intervals in the proposed method. The DER results, of improvement method on NPQ (0.5 bpnzAC payload), EBS (0.8 bpnzAC payload) and SI-UNIWARD (0.8 bpnzAC payload) algorithms are shown in Fig. 5(a). From the results, the resistances of improvement method on NPQ, EBS and SI-UNIWARD stayed steady while $T \in [0.05,\ 3]$. Thus, we suggest the sender set $T = 0.1$ as an empirical value.

Then, experiments on distribution parameter β were conducted. $T = 0.1$, and β was changed from 0 to 1 with 0.2 intervals. Note that β=0 means the original side-informed JPEG steganographic algorithm. The payload was changed from 0.1 to 0.5 bpnzAC with 0.1 intervals and additional experiments on payload 0.8 bpnzAC were conducted on EBS and SI-UNIWARD. The *DER* results of improvement method on NPQ, EBS and SI-UNIWARD algorithms are respectively shown in Fig. 5(b,c,d).

In Fig. 5(b), the proposed method (β=0.6, T=0.1 improves DERs of NPQ and NPQ-STCs algorithms from 6.16 % and 26.88 % to 29.44 % on 0.3 bpnzAC payload. From the figures, it is clear that the proposed method with β=0.6, T=0.1 improves the blind detection resistance a lot when comparing to the original NPQ, especially in the high-payload situation: the stego

images of original NPQ on 0.5 bpnzAC payload can be detected with $DER \approx 0$ when the NPQ improved by the proposed method increases the detection resistance to $DER \approx 30\%$.

In Fig. 5(c,d), the improvements on EBS and SI-UNIWARD are slight on the payload less than 0.4 npnzAC. That is because these two algorithms can resist the ccPEV feature library well on the low-payload situation, and the experimental results show that EBS and SI-UNIWARD algorithms owned high blind detection resistances on payload less than 0.4 bpnzAC ($DER >$ 45%, the 50 %-valued DERs means the detection is randomly guess). It implies that the improvements of the proposed method are not significant in the low-payload situation of ccPEV detection, while they are more impressive on the high-payload situation. The improved algorithm ($\beta=0.6$, $T=0.1$) improves DERs of EBS and SI-UNIWARD algorithms from 30.11 % and 28.06 % to 32.24 % and 31.37 % on 0.8 bpnzAC payload, respectively.

In conclusions of above experimental results, the best setting of parameters T and β is $\beta=0.6$, $T=0.1$ which substantiate the result in the Section 5.2. Actually, the suitable set of β varies from cover images, and the proposed CC method can set different value of β on different cover images. Together with the result that the EBS and SI-UNIWARD algorithms can resist ccPEV well on the low-payload situation, comparative experiments of high-dimensional detection algorithms are conducted on EBS and SI-UNIWARD in the next section.

6.3 Experiments of high-dimensional detection algorithms

In this section, experiments on blind detection resistance are conducted with high-dimension feature libraries. The J + SRM [22] and DCTR [13] feature libraries are two well-known blind detection feature libraries.

First, because the proposed method with setting $\beta=0.6$, $T=0.1$ has best improvement on EBS and SI-UNIWARD in the second part of Section 6, the *DER* results of improvement method ($\beta=0.6$, $T=0.1$) on EBS and SI-UNIWARD algorithms, obtained on 10,000 randomly chosen images with quality factors 75, 85 and 95 from the BOSSbase and classified by ensemble classifier and J + SRM feature library, are shown in Table 1 on 0.8 bpnzAC payload. From Table 1, it is clear that the proposed method can improve the detection resistance of EBS and SI-UNIWARD in most quality factors.

Then, to verify the feasibility of the proposed method, more experiments of DCTR feature library are conducted on SI-UNIWARD algorithm (the latest side-informed JPEG steganographic algorithm). Meanwhile, the CC method proposed in the second part of Section 5 can be implemented into the improvement method: choose a proper β value through CC method, and

Table 1 Experimental results on EBS (http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz) and SI-UNIWARD [32] algorithms on 0.8 bpnzAC payload under J + SRM [28] feature library (quality factors is 75, 85 and 95). The values in the table denote the DERs of the experiments and the bold values indicate the highest value of a set of experiments with same original algorithm and same image quality factor

Algorithms	Quality Factor		
	75	85	95
EBS [34]	6.39 %	**10.42 %**	17.35 %
Improved EBS based on 2D-DEM	**6.83 %**	10.27 %	**19.31 %**
SI-UNIWARD [14]	9.09 %	08.29 %	6.90 %
Improved SI-UNIWARD based on 2D-DEM	**9.66 %**	**09.29 %**	**09.11 %**

Table 2 Experimental results on SI-UNIWARD [32] algorithm under DCTR (http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz) feature library (quality factor is 75). The values in the table denote the DERs of the experiments and the bold values indicate the highest value of a set of experiments with same original algorithm and same embedding algorithm

Algorithms	Relative Payload					
	0.1	0.2	0.3	0.4	0.5	0.8
SI-UNIWARD [14]	49.01 %	48.17 %	46.28 %	42.52 %	35.53 %	9.09 %
Improved SI-UNIWARD based on 2D-DEM	48.89 %	48.01 %	46.33 %	42.81 %	36.02 %	9.85 %
Improved SI-UNIWARD based on 2D-DEM with CC method	**49.29 %**	**48.51 %**	**47.03 %**	**43.31 %**	**37.12 %**	**11.32 %**
SI-UNIWARD [14] (SE)	**49.85 %**	49.38 %	48.07 %	45.44 %	41.46 %	22.48 %
Improved SI-UNIWARD based on 2D-DEM (SE)	49.82 %	49.33 %	48.17 %	45.60 %	41.71 %	23.28 %
Improved SI-UNIWARD based on 2D-DEM with CC method (SE)	49.38 %	**49.60 %**	**48.50 %**	**46.03 %**	**42.51 %**	**25.38 %**

output a stego object with the chosen value of β. Thus, values of β are different based on the image-content. Based on this, the DER results of the comparative blind detection experiments on different payloads, obtained by using ensemble classifier and DCTR feature library on 10,000 images (compressed from the corresponding spatial images of BOSSbase database with quality factors of 75, 85, and 95), are respectively shown in Table 2, Table 3 and Table 4. In the table, both simulated embedding (SE) and actual embedding by ±1 STCs (h = 10) are presented. The results imply that the proposed algorithm using CC method owned better performance than the original binary embedding SI-UNIWARD on JPEG images of different quality factors and the high payload situations which are larger than 0.3 bpnzAC. The most significant improvement is from 0.0581 to 0.0990 at images with quality factor 95 and actual embedding method STCs (h = 10). Meanwhile, it can be concluded from the Tables 2,3 and 4 that the proposed method

Table 3 Experimental results on SI-UNIWARD [32] algorithm under DCTR (http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz) feature library (quality factor is 85). The values in the table denote the DERs of the experiments and the bold values indicate the highest value of a set of experiments with same original algorithm and same embedding algorithm

Algorithms	Relative Payload					
	0.1	0.2	0.3	0.4	0.5	0.8
SI-UNIWARD [14]	48.91 %	47.97 %	46.52 %	43.12 %	36.03 %	7.89 %
Improved SI-UNIWARD based on 2D-DEM	48.64 %	48.01 %	46.70 %	43.11 %	36.52 %	8.92 %
Improved SI-UNIWARD based on 2D-DEM with CC method	**49.05 %**	**48.67 %**	**47.26 %**	**43.89 %**	**37.52 %**	**10.11 %**
SI-UNIWARD [14] (SE)	49.27 %	49.02 %	47.65 %	44.96 %	40.64 %	19.37 %
Improved SI-UNIWARD based on 2D-DEM (SE)	49.44 %	49.14 %	47.97 %	45.35 %	41.00 %	20.30 %
Improved SI-UNIWARD based on 2D-DEM with CC method (SE)	**49.91 %**	**49.60 %**	**48.50 %**	**46.03 %**	**42.01 %**	**22.38 %**

Table 4 Experimental results on SI-UNIWARD [32] algorithm under DCTR (http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz) feature library (quality factor is 95). The values in the table denote the DERs of the experiments and the bold values indicate the highest value of a set of experiments with same original algorithm and same embedding algorithm

Algorithms	Relative Payload					
	0.1	0.2	0.3	0.4	0.5	0.8
SI-UNIWARD [14]	48.05 %	48.07 %	46.88 %	43.62 %	35.07 %	05.81 %
Improved SI-UNIWARD based on 2D-DEM	47.88 %	47.95 %	47.03 %	44.12 %	36.13 %	07.60 %
Improved SI-UNIWARD based on 2D-DEM with CC method	**48.29 %**	**48.51 %**	**47.23 %**	**44.11 %**	**37.52 %**	**09.90 %**
SI-UNIWARD [14] (SE)	47.98 %	47.99 %	47.14 %	44.96 %	41.00 %	17.51 %
Improved SI-UNIWARD based on 2D-DEM (SE)	**48.11 %**	47.92 %	47.20 %	45.60 %	41.58 %	18.75 %
Improved SI-UNIWARD based on 2D-DEM with CC method (SE)	48.00 %	**48.03 %**	**47.50 %**	**46.33 %**	**43.01 %**	**21.38 %**

works better on the JPEG images of higher quality factor. The reason would be that the DCT coefficients are distributed steadier on the high quality factor images than low quality factor ones. The values are much more concentrated to 0 when the quality factor of JPEG format is low. In conclusions, the proposed method proposed method improves the blind detection resistance of EBS and SI-UNIWARD, especially in the high payload situations.

6.4 Experiments of processing time

Computation complexity is an essential element in the practical use of steganographic algorithms. The computation complexity experiment that we conducted is described below; the results are shown in Table 5.

We used the average processing time of algorithm on 1000 images from the BOSSbase database to express the complexity. The results show that the computation complexity engendered by the proposed method (β=0.6, T=0.1) is insignificant, and the proposed method with CC approach (using 21 candidate stego images) increases acceptable multiple computation complexity.

Table 5 Algorithm processing time of NPQ [16], EBS [34] and SI-UNIWARD [14] on quality factor 95 JPEG images with STCs (/sec)

Algorithms	Relative Payload				
	0.1	0.2	0.3	0.4	0.5
NPQ-STCs [16]	1.004	1.000	0.993	1.028	0.9868
Improved NPQ based on 2D-DEM	1.021	1.029	1.045	1.054	1.098
EBS [34]	1.018	1.008	1.006	1.014	1.021
Improved EBS based on 2D-DEM	1.043	1.041	1.045	1.041	1.043
SI-UNIWARD [14]	2.835	2.878	2.868	2.932	3.021
Improved SI-UNIWARD based on 2D-DEM	3.007	3.044	3.074	3.066	3.096
Improved SI-UNIWARD based on 2D-DEM with CC method	31.16	31.02	31.13	31.2	31.26

7 Conclusions

In this paper, we analyzed the binary embedding method used in renowned side-informed JPEG steganographic algorithms and demonstrated that in the condition of independence of each cover element, the resistance to blind detection of side-informed JPEG steganographic algorithm increases when a ternary embedding that uses proper ternary ±1 distortion function utilizes the secure capacities abandoned by binary embedding. As simple ternary ±1 distortion function negatively affects detection resistance, a method to define proper ternary ±1 distortion function is proposed. The proposed method transforms the problem of defining ternary distortion function into defining two binary distortion functions on two layers. Furthermore, the distribution of stego object is controlled by the distribution parameter, and minimal values of distortion functions are reached on both RD and BD layers through the given formulas. Meanwhile, the actual embedding is conducted by the given ternary flipping lemma. Three well-known side-informed JPEG steganographic algorithms, NPQ, EBS, and SI-UNIWARD are improved by defining proper ternary ±1 distortion function through the method.

The experimental results show that the proposed method is efficient at improving blind detection resistance with proper parameter values. Thus, it is concluded that it is better to use ternary embedding on the side-informed JPEG steganography if a suitable ternary distortion function is defined. The proposed method can be applied to any side-informed JPEG steganography that uses binary ±1 embedding. The possible further studies would be:

1) Steganalysis of stego objects of color images;
2) Side-informed JPEG steganographic algorithm of color images that considering the correlationship of different channels of color images;
3) Researching the influence of parameters β and T of 2D-DEM method;
4) Giving a more suitable ternary or pentary distortion function of side-informed JPEG steganography.

Acknowledgments This work was supported by the National Natural Science Foundation of China (No. 61379151, 61272489, 61572452 and 61572052), the National Natural Science Youth Foundation of China (No. 61302159, 61401512), the Excellent Youth Foundation of Henan Province of China (No. 144100510001), and the Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-14-108).

References

1. Cover TM, Thomas JA (2012) Elements of information theory. John Wiley & Sons Press, Hoboken
2. Crandall R (1998) Some Notes on Steganography. Steganography Mailing List. http://os.inf.tu-dresden.de/west-feld/crandall.pdf
3. Filler T, Fridrich J (2010) Minimizing Additive Distortion Functions with Non-binary Embedding Operation in Steganography. In: Proc of the 2th IEEE International Workshop on Information Forensics and Security, IEEE, Seattle, 1–6
4. Filler T, Fridrich J (2011) Design of Adaptive Steganographic Schemes for Digital Images. In: Proc. of the 13th IS&T/SPIE Electronic Imaging, Media Watermarking, Security, and Forensics, vol. 7880, no. 0F, 1–14
5. Filler T, Ker AD, Fridrich J (2009) The Square Root Law of Steganographic Capacity for Markov Covers. In: Proc. of the 11th. IS&T/SPIE Electronic Imaging, Media Forensics and Security 7254(08):1–11
6. Filler T, Judas J, Fridrich J (2010) Minimizing Embedding Impact in Steganography Using Trellis-coded Quantization. In: Proc. of the 12th IS&T/SPIE Electronic Imaging, Media Forensics and Security, vol. 7541, no. 05, 1–14

7. Fridrich J (2009) Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge
8. Fridrich J, Filler T (2007) Practical Methods for Minimizing Embedding Impact in Steganography. In: Proc. of the 9th IS&T/SPIE Electronic Imaging, Photonics West, vol. 6505, no. 02, 01–15
9. Fridrich J, Goljan M, Soukal D (2004) Perturbed Quantization Steganography with Wet Paper Codes. In: Proc. of the 6th ACM Workshop on Multimedia & Security, 4–15, ACM, New York
10. Fridrich J, Goljan M, Lisonek P, Soukal D (2005) Writing on wet paper. IEEE Trans Signal Process 53(10): 3923–3935
11. Fridrich J, Pevny T, Kodovshy J (2007) Statistically Undetectable Jpeg Steganography: Dead Ends Challenges, and Opportunities. In: Proc. of the 9th ACM Workshop on Multimedia & Security, ACM, New York, 3–14
12. Guo L, Ni J, and Shi YQ (2012) An Efficient Jpeg Steganographic Scheme Using Uniform Embedding. In: Proc of the 4th IEEE International Workshop on Information Forensics and Security, 169–174, IEEE, Tenerife
13. Holub V, Fridrich J (2015) Low-complexity features for jpeg steganalysis using Undecimated DCT. IEEE Trans. Inf. Forensics Secur. 10(2):219–228
14. Holub V, Fridrich J, Denemark T (2014) Universal distortion function for steganography in an arbitrary domain. EURASIP J Inf Secur 2014(1):1–13
15. Huang J, Shi YQ (2002) Reliable information bit hiding. IEEE transactions on circuits and Systems for Video. Technology 12(10):916–920
16. Huang F, Huang J, Shi YQ (2012) New Channel selection rule for jpeg steganography. IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, 1181–1191
17. Ker AD (2007). A Fusion of Maximum Likelihood and Structural Steganalysis. In: Proc of the 9th International Workshop on Information Hiding, 4567, 204–219
18. Ker AD, Pevny T, Kodovsky J, Fridrich J (2008) The Square Root Law of Steganographic Capacity. In: Proc. of the 10th ACM Workshop on Multimedia & Security, ACM, New York, 107–116
19. Ker AD, Bas P, Böhme R, Cogranne R, Craver S, Filler T, Fridrich J, Pevny T (2013) Moving Steganography and Steganalysis from the Laboratory into the Real World. In: Proc of the first ACM Workshop on Information Hiding and Multimedia Security, ACM, New York, 45-58
20. Kim Y, Duric Z, Richards D (2007) Modified Matrix Encoding Technique for Minimal Distortion Steganography. In: Proc of the 9th International Workshop on Information Hiding, 4437, 314-327
21. Kodovsky J, Fridrich J (2009) Calibration revisited. In: Proc. of the 11th ACM Workshop on Multimedia & Security, ACM, New York, 63-74
22. Kodovsky J, Fridrich J (2012) Steganalysis of Jpeg Images Using Rich Models. In: Proc. of the 14th IS&T/SPIE Electronic Imaging, Media Watermarking, Security, and Forensics, vol. 8303, no. 0 A, 01–13
23. Kodovsky J, Pevny T, Fridrich J (2010) Modern Steganalysis can Detect YASS. In: Proc. of the 12th IS&T/SPIE Electronic Imaging,. Media Forensic Secur 7541(02):1–11
24. Kodovsky J, Fridrich J, Holub V (2012) Ensemble classifiers for steganalysis of digital media. IEEE Transactions on Information Forensics and Security 7(2):432–444
25. Kullback S (1968) Information Theory and Statistics. Courier Corporation Press, Mineola
26. Lin CC, Liu XL, Tai WL, et al. (2013) A novel reversible data hiding scheme based on AMBTC compression technique. Multimed Tool Appl 74(11):1–20
27. Lin CC, Liu XL, Yuan SM (2015) Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping. Inf Sci 293:314–326
28. Liu Q (2011) Steganalysis of DCT-embedding based adaptive steganography and YASS. In: Proc. of the 13th ACM Workshop on Multimedia & Security. ACM, New York 2011;77-86
29. Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on lsb matching revisited. IEEE Trans Inf Forensics Secur 5(2):201–2014
30. Muhammad K, Sajjad M, Mehmood I, et al. (2015) A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multi-level Encryption and Achromatic Component of An Image. Multimed Tool Appl 93(5):1–27
31. Provos N (2001) Defending against statistical steganalysis. In: Proc of Usenix Security Symposium, vol. 10, 323–336
32. Sedighi V, Fridrich J, Cogranne R (2015) Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model. In: Proc of the SPIE - The International Society for Optical Engineering, vol 9409, no 94090H, 1–13
33. Sedighi V, Cogranne R, Fridrich J (2016) Content-adaptive steganography by minimizing statistical detectability[J. IEEE Trans Inf Forensics Secur 11(2):221–234
34. Wang C, Ni J (2012) An Efficient Jpeg Steganographic Scheme Based on the Block Entropy of DCT Coefficients. In: Proc of the 37th IEEE International Conference on Acoustics, Speech and Signal Processing, 1785–1788, IEEE, Kyoto
35. Yang Y, Zhang W, Liang D, et al. (2016) Reversible data hiding in medical images with enhanced contrast in texture area. Digital Signal Process, 2016 52(C):13–24

Zhenkun Bao received his B.S. and M.S. from the Zhengzhou Information Science and Technology Institute, in 2011 and 2014, respectively. Now, he is a doctoral candidate of Computer Applications of Zhengzhou Information Science and Technology Institute. His current research interests include image steganography and steganalysis technique.

Xiangyang Luo received his B.S., M.S. and Ph. D. from Zhengzhou Information Science and Technology Institute, in 2001, 2004 and 2010, respectively. He has been with Zhengzhou Information Science and Technology Institute since July 2004. From 2006 to 2007, he was a visiting scholar of the Department of Computer Science and Technology of Tsinghua University. From 2011, he is a postdoctoral of Institute of China Electronic System Equipment Engineering Co., Ltd. He is the author or co-author of more than 50 refereed international journal and conference papers. His research interest includes image steganography and steganalysis. He obtained the support of the National Natural Science Foundation of China and the Basic and Frontier Technology Research Program of Henan Province.

Weiming Zhang received the M.S. and Ph.D. degrees from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2002 and 2005, respectively. He is currently an Associate Professor with the School of Information Science and Technology, University of Science and Technology of China, Hefei, China. His research interests include multimedia security, information hiding, and cryptography.

Chunfang Yang received his B.S. and M.S. from the Zhengzhou Information Science and Technology Institute, in 2005 and 2008, respectively. Now, he is a doctoral candidate of Computer Applications of Zhengzhou Information Science and Technology Institute. His current research interests include image steganography and steganalysis technique.

Fenlin Liu received his B.S. from Zhengzhou Information Science and Technology Institute in 1986, M.S. from Harbin Institute of Technology in 1992, and Ph.D. from the Northeast University in 1998. Now, he is a professor of Zhengzhou Information Science and Technology Institute. His research interests include information hiding and security theory. He is the author or co-author of more than 90 refereed international journal and conference papers. He obtained the support of the National Natural Science Foundation of China and the Found of Innovation Scientists and Technicians Outstanding Talents of Henan Province of China.