Signal Processing 168 (2020) 107343

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Robust adaptive steganography based on generalized dither modulation and expanded embedding domain

Xinzhi Yu, Kejiang Chen, Yaofei Wang, Weixiang Li, Weiming Zhang*, Nenghai Yu

School of Information Science and Technology, University of Science and Technology of China, Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Hefei 230026 China

ARTICLE INFO

Article history:
Received 15 May 2019
Revised 18 September 2019
Accepted 13 October 2019
Available online 14 October 2019

Keywords:
SNPs
Robust steganography
Asymmetric distortion
Generalized dither modulation
Embedding domain

ABSTRACT

Sharing images on social network platforms (SNPs) from mobile intelligent devices is becoming more and more popular and has great potential for covert communication. However, images will be processed by lossy social network channels, such as JPEG compression, which reduces image quality and destroys message extraction. Previous robust steganographic schemes using reverse engineering or anti-compression domain for SNPs suffer from some security flaws or have only small capacity and low security level. The purpose of this paper is to refine the robust steganographic scheme by considering asymmetric costs for different modification polarities and expanding the embedding domain for digital images, aiming to aggregate the modifications on the elements with small costs. Such a new strategy that utilizes asymmetric distortion for dither modulation to implement ternary embedding can be regarded as generalized dither modulation in substantial sense. Compared with the original Dither Modulation-based robust Adaptive Steganography (DMAS), the proposed scheme selects more DCT coefficients as cover elements and we call it Generalized dither Modulation-based robust Adaptive Steganography (GMAS). Extensive experiments demonstrate that the proposed GMAS gains significant performance improvements in terms of robustness and security when compared with DMAS.

1. Introduction

Steganography is a science and art of covert communication that conceals a message within the original digital media without drawing suspicions from steganalysis [1–3]. Currently, the most successful steganographic schemes are based on the framework of minimizing additive distortion, which assigns a modification cost to each cover element and defines the distortion function as the sum of all elements' costs. And Syndrome-Trellis Codes (STCs) [4] provide a general methodology that can asymptotically approach the theoretical bound of average embedding distortion for arbitrary additive distortion function.

Since STCs can reach the payload-distortion bound for additive distortion, the emerging JPEG steganographic schemes all focused on the design of effective distortion function, such as J-UNIWARD (JPEG UNIversal WAvelet Relative Distortion) [5], UERD (Uniform Embedding Revisited Distortion) [6], RBV (Residual Block Value) [7], BET (Block Entropy Transformation) [8], GUED (Generalized Uniform Embedding Distortion) [9], and the aim of whose is to assign low costs to elements within texture areas while high costs to that of smooth areas according to the "Complexity-First Rule" [10].

All the above content-adaptive algorithms allot same cost for ± 1 embedding changes. However, changes with different polarities make different influences on image due to the correlation of natural image. Therefore, the costs for ± 1 embedding changes should not be equivalent. To distinguish the ± 1 embedding costs, Wang *et al.* proposed an asymmetric distortion framework in [11] based on estimated side-information, where an average filter is utilized to compensate the block artifact and then constructs a reference image to adjust the original distortion function so that the stego image can be more similar to the original uncompressed spatial image. They subsequently improved the compensation method by replacing the average filter with Wiener filter in [12], but the time complexity is unacceptable due to the complex process of finding the optimal parameter for adjusting the cost.

Although the aforementioned schemes take the undetectability into account adequately, they do not consider the performance after JPEG compression, which is the main processing method by SNPs due to the limitations of storage and bandwidth. The main

* Corresponding author.
E-mail addresses: xzyu@mail.ustc.edu.cn (X. Yu), chenkj@mail.ustc.edu.cn (K. Chen), yaofei@mail.ustc.edu.cn (Y. Wang), wxli6049@mail.ustc.edu.cn (W. Li), zhangwm@ustc.edu.cn (W. Zhang), ynh@ustc.edu.cn (N. Yu).

https://doi.org/10.1016/j.sigpro.2019.107343
0165-1684/

Table 1
Overall performance of three robust steganographic schemes.

Method	Anti-Steganalysis	Capacity	Security Flaw	Reverse Engineering	Computational Complexity
Upward Robust [15]	weak	small	no	no	low
Downward Robust [17]	strong	large	yes	yes	high
Matching Robust [18]	strong	large	yes	yes	high

research issue of steganography is usually restricted in the lab environment, i.e., assuming that stego images will pass through a lossless channel and be accepted by receivers intactly, which fails the covert communication when applied to the real-world. With the rapid development of smart mobile devices, sharing images on SNPs is becoming more and more popular, which will be a useful resource for covert communication. Therefore, it is imperative to propose steganographic schemes that are robust to JPEG compression.

To date, there only exist several attempts for designing such schemes. In [13], Zhang *et al.* first proposed a framework of "Compression-resistant Domain Constructing + RS-STCs Codes", which achieves strong robustness by constructing robust embedding domain and utilizing RS (Reed-Solomon) codes [14]. Thereafter, they proposed a method based on the relative relationship between four DCT coefficients to embed messages under the framework. To take full use of the characteristics of quantization operation, Zhang *et al.* utilized dither modulation to modify the middle frequency AC coefficients according to quantization tables in DMAS [15]. Although these methods can obtain high data extraction accuracy after channel transmission [16] and reasonable undetectability at low relative payload, they can only work when the quality factor of cover images (Q_{cover}) is not larger than that of channel JPEG compression (Q_{channel}). And we call this scheme "Upward Robust".

To solve the problem that Q_{channel} is smaller than Q_{cover}, Tao *et al.* proposed an interesting scheme in [17]. They first obtained the recompressed version of the original JPEG image using Q_{channel}, and got the changes information by embedding messages into it, then modified the original image based on the changes information to get the stego image. This method can reach high security performance through SNP compression, but it can be detected in the stage of uploading images to the SNP. Such a security flaw in uploading stage due to the modification positions of the original image does not meet the requirements of adaptive steganography and the modification strength of which is always bigger than 1. Since it can only work when Q_{channel} is smaller than Q_{cover}, we call this scheme "Downward Robust".

In order to reduce the impact of SNPs, Zhao *et al.* proposed transport channel matching [18] to adjust the cover image to meet the requirements of SNP before embedding. They also utilized BCH (Bose, Ray-chaudhuri and Hocquenghem) codes [19] to further improve the robustness. Although this method can obtain strong robustness and undetectability, it also has security flaws due to the high similarity of DCT coefficients between the uploaded and downloaded stego images, which can be easily detected. And we name this scheme "Matching Robust".

Moreover, the above two methods assume that the JPEG encoder of SNP can be perfectly reverse-engineered so that they can perform the JPEG compression of SNP offline once [17] or more times [18] before embedding. As the reverse engineering [18] is quite difficult to achieve, when conveying secret message, they should upload and download the original cover JPEG image once [17] or more iterations [18] from the specific SNP, which is behavior-suspicious and violates the nature of steganography. Besides, the uploading and downloading operations are time-consuming, resulting in higher computational complexity of both schemes.

As concluded in Table 1, both Downward Robust and Matching Robust have security flaws by which the adversary can design targeted steganalysis. In addition, they need to assume that the JPEG encoder of SNP can be perfectly reverse-engineered. Nowadays, the Upward Robust is the only scheme, which possesses strong robustness, normal behavior, and lower computational complexity, can be applied to SNPs without the above disadvantages. However, DMAS [15] implements binary embedding based on dither modulation and just embeds on the middle frequency regions, which reduces its capacity and weakens its security severely. In this paper, we are trying to perfect it from both embedding method and embedding region. The proposed scheme takes into account the asymmetric distortion for dither modulation to implement ternary embedding and expands the embedding region to cluster as many modifications as possible on the elements with small costs. The performance of the proposed scheme is verified with exhaustive experiments under different channel compression conditions and effective steganalyzers with CCPEV (PEV features [21] enhanced by Cartesian Calibration) [20] and DCTR (Discrete Cosine Transform Residual) [22]. The experimental results show that the proposed scheme achieves higher level of performance in terms of robustness and security than DMAS.

The contributions of this work are summarized as follows.

1) We present a more effective and lower time-consuming asymmetric distortion scheme by improving the compensation method in [11].
2) The generalized dither modulation based on asymmetric distortion is proposed and utilized to implement ternary embedding, which can enhance the robustness and security significantly.
3) We construct a model and conduct extensive experiments to pursue the trade-off between robustness and security, which can guide us to expand the embedding domain reasonably and further improve the undetectability evidently.

The rest of this paper is organized as follows. We introduce the notations and prior works in Section 2. The proposed scheme is described in Section 3. Results of comparative experiments are elaborated in Section 4. Conclusion and future work are given in Section 5.

2. Preliminaries and prior work

2.1. Notations

Throughout the paper, matrices, vectors and sets are written in bold face. The cover image (of size $n_1 \times n_2$) is denoted by $\mathbf{X} = (x_{ij})^{n_1 \times n_2}$, where the signal x_{ij} is an integer and represents the quantized JPEG DCT coefficients, $x_{ij} \in \{-1024, \dots, 1023\}$. $\mathbf{Y} = (y_{ij})^{n_1 \times n_2}$ denotes the stego image. Without loss of generality, we will assume that n_1 and n_2 are multiples of 8.

For simplicity, the quantization table will be denoted as $\mathbf{Q} = (q_{kl}),\ (k, l \in \{1, \dots, 8\})$. Then we use the symbols $\mathbf{D}$ and $\mathbf{X}$ to denote the matrices of de-quantized and quantized DCT coefficients, respectively. The symbol $J^{-1}(\mathbf{X})$ for the JPEG image represents the spatial image decompressed from $\mathbf{X}$. If no otherwise specified, ρ_{ij} (or ρ) and ζ_{ij} (or ζ) will denote the embedding costs of quantized DCT coefficients x_{ij} and de-quantized DCT coefficients d_{ij}, respectively.

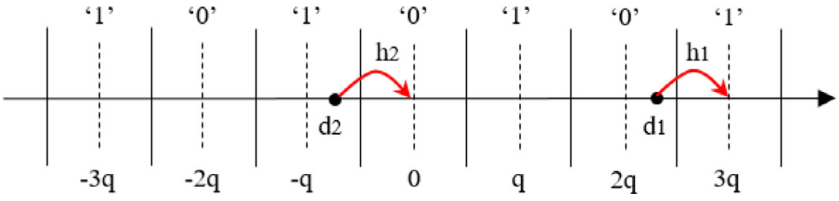


Fig. 1. Embedding schematic of the watermarking algorithm [25].

2.2. Dither modulation

Dither modulation is an extension of the original uniform quantized index modulation (QIM) algorithm proposed in [23,24]. As dither modulation can reduce quantization artifacts and generate a perceptually superior quantized content, it has become one of the most popular methods for robust watermarking algorithms [25,26]. Now, we will briefly introduce the embedding process of the watermarking algorithm [25] for frequency domain.

The embedding schematic of the algorithm [25] is shown in Fig. 1. It is obvious that the coordinate axes of de-quantized DCT coefficient values are divided into intervals according to the quantization step q, and the odd class intervals represent message bit '1' while the even class intervals represent message bit '0'. In order to embed the message bit w with minimum modification distance h, we should reasonably quantize the de-quantized DCT coefficient d so that the embedding message bit w can be expressed by the interval in which the quantization result $\hat{d}$ locates. For instance, if we embed message bit '1' into d_1, then $\hat{d}_1$ should be equal to $3q$ instead of q. Similarly, if we embed message bit '0' into d_2, then $\hat{d}_2$ should be equal to 0 instead of $-2q$.

As we can see, the coefficient d is always quantized as the middle coordinate of the nearest interval which can express the carried binary message. Therefore, the binary dither modulation can reduce the interference caused by random errors and guarantee the perceptual quality effectively.

2.3. Review of the original method DMAS

Dither Modulation-based robust Adaptive Steganography (DMAS) [15] is the current optimal Upward Robust embedding method and follows the framework of "Compression-resistant Domain Constructing + RS-STCs Codes". It utilizes the construction of robust embedding domain and RS codes [14] to achieve strong resistant ability for JPEG compression. In addition, dither modulation along with single-layered STCs is adopted to possess a relatively satisfactory undetectability. Since the image format adopted by SNPs is mostly JPEG, we will only concern JPEG image. The details are described as follows:

1) Process Cover Image. Given a JPEG image $\mathbf{X}$, the corresponding de-quantized DCT coefficients $\mathbf{D}$ and quantization table $\mathbf{Q}$ can be easily obtained.
2) Extract Cover Elements. Denote the coefficients of each 8×8 DCT block as d_{kl}, $(k,l\in\{1,\ldots,8\})$, extract elements from the middle frequency domain $(k+l=8,9)$ that is robust to JPEG compression and calculate their modifying magnitudes according to dither modulation in Section 2.2 when modified to neighboring intervals.
3) Calculate Modifying Costs. The embedding costs for quantized DCT coefficients x_{ij} can be calculated by the distortion function of J-UNIWARD [5]:

$$\rho_{ij}^{(JUNI)}=\sum_{k=1}^{3}\sum_{\mu=1}^{n_1}\sum_{\nu=1}^{n_2}\frac{|W_{\mu\nu}^{(k)}(J^{-1}(\mathbf{X}))-W_{\mu\nu}^{(k)}(J^{-1}(\mathbf{Y}_{x_{ij}}))|}{|W_{\mu\nu}^{(k)}(J^{-1}(\mathbf{X}))|+\sigma},\tag{1}$$

where $W_{\mu\nu}^{(k)}$ represents the $\mu\nu$th wavelet coefficient in the kth subband of the first level decomposition and $\mathbf{Y}_{x_{ij}}$ represents the corresponding stego images when changing x_{ij} by 1, $\sigma=2^{-6}$ is a constant stabilizing numerical calculations. Then the embedding costs for de-quantized DCT coefficients d_{ij} are defined as Eq. (2):

$$\zeta_{ij}^{(JUNI)}=\rho_{ij}^{(JUNI)}/q_{ij},\tag{2}$$

and the final modifying costs are calculated as:

$$\xi_{ij}^{(JUNI)}=\zeta_{ij}^{(JUNI)}\times h_{ij},\tag{3}$$

where q_{ij} and h_{ij} represent the corresponding quantization step and modifying magnitude of d_{ij}, respectively.
4) RS Encoding. Before embedding, the RS codes are adopted to encode the messages to improve the accuracy of extracted messages after JPEG compression.
5) STCs Embedding. The single-layered STCs are implemented to embed the encoded messages with minimum embedding distortion and the stego images $\mathbf{Y}$ can be obtained through quantization and Huffman coding, which saves the storage space by lossless compression.

After receiving the JPEG compressed stego images, receivers should first calculate the de-quantized DCT coefficients and quantize them with the same quantization tables used by senders. Then perform STCs decoding to extract the messages encoded by RS codes, and finally get the secret messages through RS decoding.

3. Proposed method

3.1. Motivation

The above subsection has reviewed that DMAS [15] mainly use binary STCs along with dither modulation to strive for "minimum modification distance" during embedding, as shorter modification distance means lower embedding cost for symmetric distortion. However, the coding efficiency of binary STCs is poorer than that of ternary STCs, which will cause fewer modifications and smaller distortion when embedding the same message. In addition, the opinion in [11,12] has shown that different modification polarities will cause different influences on image, i.e., shorter modification distance may lead to higher cost. Therefore, a ternary embedding method based on improved dither modulation that takes full use of asymmetric distortion will be an advisable improvement for DMAS to achieve "minimum modification cost".

Currently, the adaptive steganographic methods have demonstrated that modifying the low frequency AC coefficients will cause small impact on image, while the embedding domain of DMAS are only restricted in the middle frequency domain, resulting in small capacity and poor security performance. From Fig. 2 we can see that the lower the frequencies, the weaker the robustness of DCT modes, i.e., robustness and security contradict each other. To further improve the security of DMAS, we will try to find the equilibrium point between security and robustness in the following subsection.

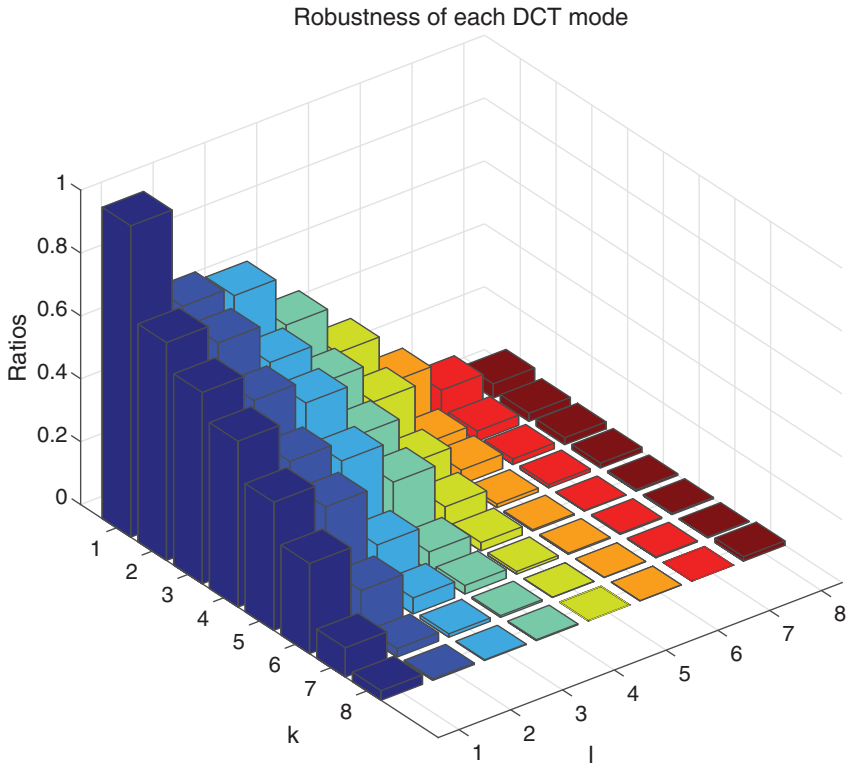


Fig. 2. The robustness of each DCT mode against JPEG compression. Randomly select 1000 images (denoted as C_{65}) from BOSSbase 1.01 [28] with $QF = 65$ and get their compressed version (denoted as C_{85}) with $QF = 85$, then recompress C_{85} with $QF = 65$ to obtain S_{65}. Let N_{65} represent the number of non-zero DCT coefficients of C_{65}, and D_{65} represent the number of different DCT coefficients between C_{65} and S_{65}. The average ratio of D_{65} to N_{65} is shown in the above figure.

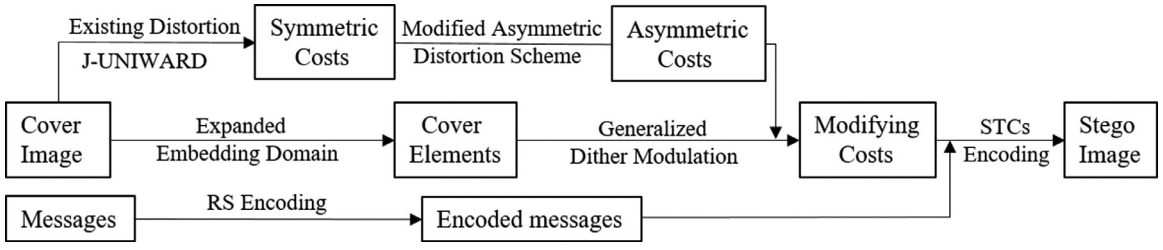


Fig. 3. The flowchart of the proposed scheme (GMAS).

The flowchart of our proposed scheme is presented in Fig. 3. Compared with DMAS [15], we first extract cover elements from the expanded embedding domain which contains middle and several mid-low AC coefficients. Secondly, the symmetric costs measured by any of the existing JPEG distortion functions are adjusted via the modified asymmetric distortion scheme to get different costs for ± 1 embedding changes. Then the modifying costs of cover elements can be calculated through generalized dither modulation and asymmetric costs. To enhance robustness, the secret messages will be encoded by RS codes in advance, and stego image can be finally obtained via double-layered STCs. Similar to DMAS, we call our proposed scheme Generalized dither Modulation-based robust Adaptive Steganography (abbreviated to GMAS) in the subsequent section.

3.2. Modified asymmetric distortion scheme

Wang *et al.* proposed two asymmetric distortion schemes in [11,12] to reduce the impact of block artifact. Although the scheme in [12] can obtain higher security performance, it is too time-consuming to be suitable for real-world application. As the compensation method of Wang et al. [12] are more effective than that of Wang et al. [11], we will modify the scheme in [11] to get a reasonable trade-off between security and time complexity, and the details of which are as follows.

1. Given a JPEG image $\mathbf{X}$, decompress it into spatial domain to get the generated spatial image $J^{-1}(\mathbf{X})$.
2. Obtain the filtered spatial image $\mathbf{S}$ by filtering $J^{-1}(\mathbf{X})$ with the average filter $\mathbf{F}$ as Eqs. (4) and (5). The reasons why we adopt Eq. (5) are that the pixels of eight neighborhoods are the most correlated in a natural image, and a 3×3 filter is appropriate for smoothing the border pixels of each block and increasing the correlation of pixels within different blocks. The smaller sized filter cannot take full use of the pixel correlation, and the larger sized filters may introduce misleading information from the farther pixels. Thus $\mathbf{S}$ is similar to a normal spatial image and can be used as side-information directly like [12], instead of using its border pixels of each block to replace that of $J^{-1}(\mathbf{X})$ like [11], to guide the adjustment of the given distortion function.

$$\mathbf{S} = J^{-1}(\mathbf{X}) \otimes \mathbf{F}, \tag{4}$$

$$\mathbf{F}=\begin{bmatrix}1/9 & 1/9 & 1/9\\ 1/9 & 1/9 & 1/9\\ 1/9 & 1/9 & 1/9\end{bmatrix}. \tag{5}$$

3. Transform **S** into DCT domain through DCT transformation to get the de-quantized DCT coefficients $\overline{\mathbf{X}}$. To consider the distortion adjustment method more meticulously, we use the result of dividing $\overline{\mathbf{X}}$ by their corresponding quantization steps directly in Eq. (6) and Eq. (7) to avoid the rounding error that can invalidate some weak side-information.
4. Utilize the existing distortion functions, such as J-UNIWARD [5] and UERD [6], to calculate the symmetric costs ρ_{ij}, then the final asymmetric embedding costs can be obtained as follows:

$$\rho_{ij}^{+}=\begin{cases}\alpha\cdot\rho_{ij}, & x_{ij}<\bar{x}_{ij}/q_{ij}\\ \rho_{ij}, & x_{ij}\geq\bar{x}_{ij}/q_{ij}\end{cases}, \tag{6}$$

$$\rho_{ij}^{-}=\begin{cases}\alpha\cdot\rho_{ij}, & x_{ij}>\bar{x}_{ij}/q_{ij}\\ \rho_{ij}, & x_{ij}\leqslant\bar{x}_{ij}/q_{ij}\end{cases}, \tag{7}$$

where $\bar{x}_{ij}$ denotes the de-quantized DCT elements of $\overline{\mathbf{X}}$ and $\alpha\in[0,1]$ controls the degree of adjustment on ρ_{ij}.

3.3. Generalized dither modulation

Dither modulation can effectively take advantage of the side-information to reduce quantization noise when applied to data hiding, such as watermarking in [25,26] and steganography in [15,27]. However, dither modulation based steganography [15] will cause some changes with high costs and short modification distances due to the negligence of asymmetric distortion, which weakens the detection resistant capability. To enhance security performance, we propose a generalized dither modulation method based on asymmetric distortion, which can be combined with double-layered STCs to further improve the statistical undetectability.

The embedding schematic of generalized dither modulation is presented in Fig. 4. Similar to dither modulation in Section 2.2, the coordinate axes of de-quantized cover elements are divided into odd class and even class intervals according to the quantization step q to express message bit '1' and '0', respectively. Then the message bit w can be embedded into the de-quantized DCT coefficient d during quantizing, i.e., the message bit represented by the interval that the quantization result $\hat{d}$ locates is identical to w. If w equal to '1', we can easily calculate the modification distances h^{-} and h^{+} with opposite polarities as shown in Fig. 4. Given the asymmetric costs ρ^{-} and ρ^{+}, the embedding costs for de-quantized DCT coefficient d are defined as:

$$\zeta^{-}=\rho^{-}/q,\ \zeta^{+}=\rho^{+}/q, \tag{8}$$

then we can obtain the modifying costs:

$$\xi^{-}=\zeta^{-}\times h^{-},\ \xi^{+}=\zeta^{+}\times h^{+}, \tag{9}$$

To minimize the embedding costs, we propose the following **modifying rule**:

$$\hat{d}=\begin{cases}d+h^{+}, & \xi^{-}>\xi^{+}\\ d-h^{-}, & \xi^{-}\leqslant\xi^{+}\end{cases}, \tag{10}$$

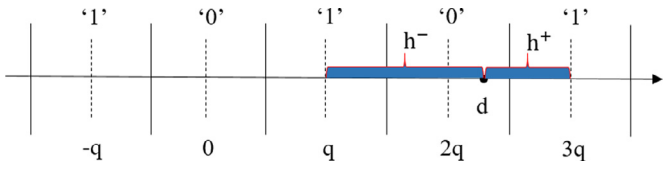


Fig. 4. The embedding schematic of generalized dither modulation.

which means that the modification polarities with smaller embedding costs rather than shorter modification distances will be implemented.

3.4. Generalized dither modulation using ternary STCs

As ternary STCs have higher embedding efficiency than their binary version and can reach the theoretical bound security performance, we will combine them with generalized dither modulation to embed message. Using the symbols d_{ij} and q_{ij} to denote the de-quantized cover element and the corresponding quantization step, respectively, then the modifying costs can be calculated as follows:

If $d_{ij}\in((k-\frac{1}{2})q_{ij},(k+\frac{1}{2})q_{ij})$,

$$\zeta_{ij}^{+}=\rho_{ij}^{+}/q_{ij},\ h_{ij}^{+}=(k+1)q_{ij}-d_{ij},\ \xi_{ij}^{+}=\zeta_{ij}^{+}\times h_{ij}^{+}, \tag{11}$$

$$\zeta_{ij}^{-}=\rho_{ij}^{-}/q_{ij},\ h_{ij}^{-}=d_{ij}-(k-1)q_{ij},\ \xi_{ij}^{-}=\zeta_{ij}^{-}\times h_{ij}^{-}, \tag{12}$$

where $k\in N$ is an integer. After STCs encoding, the changes information can be obtained to guide the quantization process with the modification distances information h_{ij}^{-} and h_{ij}^{+} calculated in advance. It is worth noting that we do not change the coefficients when their denoted-message bits are identical to the carried-message bits to maintain the statistical models of cover images.

When extracting the messages embedded by STCs from stego images attacked by channel JPEG compression, we should first calculate the de-quantized DCT coefficients and use the same quantization tables shared with senders to quantize them, then the messages can be obtained through STCs decoding.

3.5. Theoretical model of embedding domain

As pointed out in Section 3.1, robustness and security are a pair of contradictions and it is a challenging problem to balance them. However, DMAS [15] only embeds messages on the middle frequency domain as shown in Fig. 5(a) to simply pursue high robustness while ignoring security. Since embedding message on high frequency domain will introduce severe noise, we will exploit more available elements within low frequency domain as shown in Fig. 5(b) by building a theoretical model and implementing experiments practically to further improve the undetectability.

Given the embedding domain E and the selected batch of covers $\mathbf{X}_{\mathrm{N}}$ with N images, we first utilize our proposed GMAS (no RS codes) to embed messages on $\mathbf{X}_{\mathrm{N}}$ at a relative payload p to get the stegos $\mathbf{Y}_{\mathrm{N}}$, then obtain the average error rate $\bar{P}_{\mathrm{E}}$ by using the FLD ensemble [29] and specified feature set. Secondly, the attacked stegos $\widetilde{\mathbf{Y}}_{\mathrm{N}}$ can be obtained through channel JPEG compression. Thirdly, the messages will be extracted from $\widetilde{\mathbf{Y}}_{\mathrm{N}}$ by STCs decoding and the average bit error rate $\bar{R}_{\mathrm{N}}$ could be calculated. Then we can get the coding redundancy as Eq. (13) according to coding theory [30], which assumes that the error correction code has the theoretical-bound error correction capability,

$$H(\bar{R}_{\mathrm{N}})=-\bar{R}_{\mathrm{N}}\log_2\bar{R}_{\mathrm{N}}-(1-\bar{R}_{\mathrm{N}})\log_2\left(1-\bar{R}_{\mathrm{N}}\right), \tag{13}$$

and the perfect payload P_{perfect} that can be received without any error bits is calculated as:

$$P_{\mathrm{perfect}}=p\times(1-H(\bar{R}_{\mathrm{N}})). \tag{14}$$

After repeating multiple experiments at different relative payloads p, we can get the relationship between P_{perfect} and $\bar{P}_{\mathrm{E}}$, which

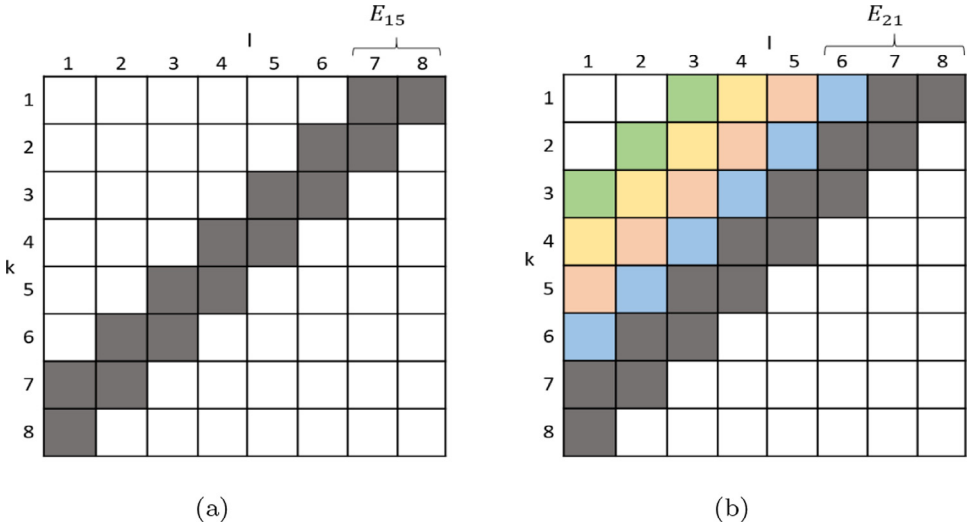


Fig. 5. (a) is the embedding domain of DMAS (E_{15}), we will gradually expand the embedding domain from mid-low frequency to low frequency as shown in (b) and E_{21} is our finally adopted embedding domain.

reflects the overall performance of the embedding domain E in the case that embedded messages can be extracted correctly by using an ideal error correction code.

The above theoretical model can guide us how to expand the embedding domain to some extent, but the final embedding domain needs to be confirmed through experiments due to the limitations of the error correction ability of the real-adopted error correction codes, i.e., RS codes, and we will determine the expanded embedding domain in Section 4.3.

3.6. Pseudo-code procedure

To further clarify the scheme of Generalized dither Modulation-based robust Adaptive Steganography (GMAS), we provide a pseudo-code that describes the implementation of the embedding process. Since the extracting process is the same as DMAS that has already been introduced in Section 2.3, we no longer describe it here.

Embedding process of GMAS

Input: A cover image $\mathbf{X}$ with N DCT coefficients; L bits of message $\mathbf{m}$ which determines the relative payload of target $\gamma = L/N$.

Output: The stego image $\mathbf{Y}$.

1. Get the quantization table $\mathbf{Q}$ and calculate the de-quantized DCT coefficients $\mathbf{D}$ of the cover image $\mathbf{X}$;
2. Utilize the existing distortion functions (e.g., J-UNIWARD) to calculate the original symmetric costs;
3. Adjust the symmetric costs with the method described in Section 3.2 to get the asymmetric costs $\boldsymbol{\rho}^+$ and $\boldsymbol{\rho}^-$;
4. Extract cover elements $\mathbf{d}$ and their corresponding asymmetric costs $\boldsymbol{\rho}^+$ and $\boldsymbol{\rho}^-$ from the expanded embedding domain E_{21};
5. Calculate the modification distances $\mathbf{h}^-$ and $\mathbf{h}^+$ according to the method in Section 3.3, then the modifying costs $\boldsymbol{\xi}^+$ and $\boldsymbol{\xi}^-$ can be obtained according to Eqs. (11) and (12);
6. Encode the message $\mathbf{m}$ by RS encoding (e.g., RS (31,15)) to get the encoded message $\hat{\mathbf{m}}$;
7. Embed $\hat{\mathbf{m}}$ through ternary STCs encoding and obtain the changes information $\mathbf{I}$;
8. Quantize the cover elements $\mathbf{d}$ with changes information $\mathbf{I}$, $\mathbf{h}^-$ and $\mathbf{h}^+$, then process the quantized DCT coefficients through Huffman coding to get the stego image $\mathbf{Y}$.

4. Experiment

4.1. Setups

All experiments in this paper are carried out on BOSSbase 1.01 [28] containing 10,000 grayscale 512×512 images. The original images are JPEG compressed using different quality factors ranging from 65 to 85, so we have about twenty image databases in the format JPEG. The relative payload $p = n_{\mathrm{m}}/n_{\mathrm{nzac}}$, where n_{m} is the length of the original embedded messages rather than the encoded messages by RS codes and n_{nzac} is the number of non-zero AC DCT coefficients of the image. We set the range of the relative payloads of robust adaptive steganography from 0.05 to 0.15 bits per non-zero AC DCT coefficients (bpnzac) due to the small embedding domain. The extraction error rate $R_{\mathrm{error}} = n_{\mathrm{error}}/n_{\mathrm{m}}$, where n_{error} is the number of wrong message bits. The quality factor of cover image and channel JPEG compression are denoted as Q_{cover} and Q_{channel}, respectively, and two effective feature sets (CCPEV [20], DCTR [22]) are selected for steganalysis of JPEG image. We will set the secure parameter $h = 10$ of STCs, and if not specified, RS (31,15) will be adopted at the following experiments except for Section 4.3. As for (n^*, k^*) RS codes, n^* and k^* denote the code length and message length, respectively, and the greater the ratio of k^* to n^*, the stronger the error correction ability of RS codes.

The detectors are trained as binary classifiers implemented using the FLD ensemble with default settings [29]. A separate classifier is trained for each embedding algorithm and payload. The ensemble by default minimizes the total classification error probability under equal priors $P_{\mathrm{E}} = min_{P_{\mathrm{FA}}} \frac{1}{2}(P_{\mathrm{FA}} + P_{\mathrm{MD}})$, where P_{FA} and P_{MD} are the false-alarm probability and the missed-detection probability respectively. The ultimate security is qualified by average error rate $\overline{P}_{\mathrm{E}}$ averaged over ten 5000/5000 database splits, and larger $\overline{P}_{\mathrm{E}}$ means stronger security.

4.2. Performances of modified asymmetric distortion scheme

To verify the effectiveness of the modified asymmetric distortion scheme, J-UNIWARD (abbreviated as JUNI) and UERD are chosen as the seed methods. The steganographic methods adopting Block Artifact Compensation with rounded (like [11]) and non-rounded side-information are named by suffixing the original name with "_BAC_round" and "_BAC", respectively, such

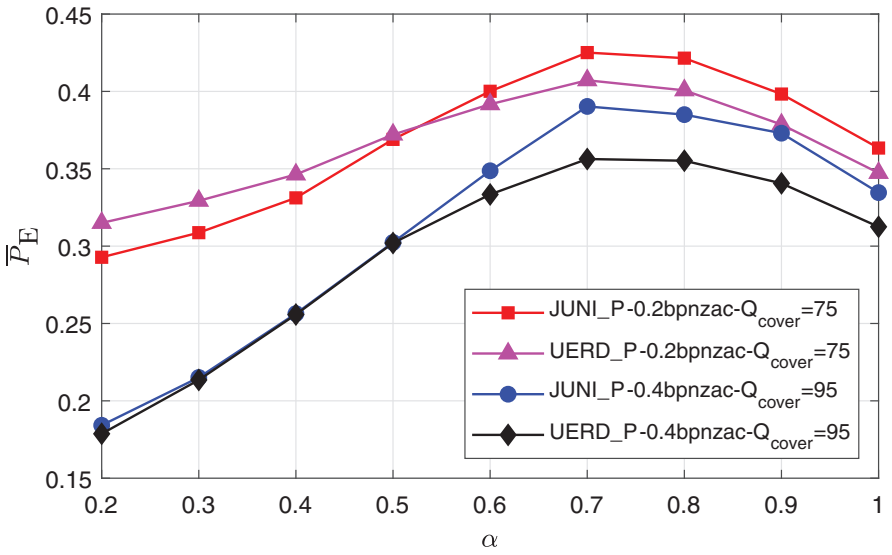


Fig. 6. The average detection error rates $\overline{P}_E$ of the modified asymmetric distortion scheme with different values of α on 2000 images randomly selected from BOSSbase 1.01 using the FLD ensemble classifier with feature sets DCTR.

Table 2
Detectability in terms of $\overline{P}_E$ versus embedded payload size in bits per non-zero AC DCT coefficients (bpnzac) for steganographic schemes with $Q_{cover} = 75$ on BOSSbase 1.01 using the FLD ensemble classifier with feature sets DCTR.

Feature	Embedding Method	0.1	0.2	0.3	0.4	0.5
DCTR	JUNI	.4382 ± .0043	.3405 ± .0047	.2402 ± .0039	.1541 ± .0015	.0890 ± .0018
	JUNI_BAC_round	.4497 ± .0016	.3911 ± .0021	.3200 ± .0029	.2457 ± .0027	.1755 ± .0036
	JUNI_BAC	.4541 ± .0016	.3993 ± .0029	.3337 ± .0039	.2612 ± .0032	.1869 ± .0033
	JUNI_P	**.4573 ± .0019**	**.4098 ± .0041**	**.3440 ± .0023**	**.2673 ± .0028**	**.1915 ± .0043**
	UERD	.4294 ± .0033	.3293 ± .0038	.2283 ± .0041	.1439 ± .0023	.0851 ± .0022
	UERD_BAC_round	.4376 ± .0026	.3620 ± .0025	.2868 ± .0035	.2132 ± .0030	.1510 ± .0032
	UERD_BAC	.4434 ± .0028	.3733 ± .0035	.3002 ± .0026	.2265 ± .0034	.1616 ± .0022
	UERD_P	**.4495 ± .0029**	**.3843 ± .0022**	**.3112 ± .0040**	**.2333 ± .0035**	**.1624 ± .0033**

as JUNI_BAC_round and JUNI_BAC, while JUNI_P and UERD_P represent the seed methods adopting the modified scheme in Section 3.2. We conduct several experiments to find the optimal solution of α on 2000 images randomly selected from BOSSbase 1.01 against DCTR. It can be seen from Fig. 6 that the optimal value of α is around 0.7 and independent of Q_{cover} and steganographic methods, thus we set the value of α to 0.7.

Table 2 shows the average detection error rate $\overline{P}_E$ of the seed and improved algorithms when resisting DCTR with $Q_{cover} = 75$. It is clear that both JUNI_BAC and UERD_BAC perform better than their original version with rounded side-information, which verifies that the rounding operation will invalidate some weak side-information and reduce the effectiveness of block artifact compensation. For all cases, both JUNI_P and UERD_P clearly outperform the other schemes by a sizeable margin, e.g., JUNI_P performs better than JUNI_BAC_round by 0.76%-2.40%, and UERD_P performs better than UERD_BAC_round by 1.14%-2.44%, indicating that the modified asymmetric distortion scheme is far more efficient than the original one.

4.3. Determining the expanded embedding domain

To simulate the theoretical model of different embedding domains described in Section 3.5, 2000 images are randomly selected from BOSSbase 1.01 [28] with $Q_{cover} = 65$ and embedded by GMAS with distortion function JUNI_P. We adopt the low dimensional feature CCPEV [20] to detect stegos and set $Q_{channel} = 85$ to simulate the channel JPEG compression. For simplicity, we gradually expand the embedding domain from mid-low frequency to low frequency as shown in Fig. 5(b) and name the different embedding domains E_{15}, E_{21}, E_{26}, ..., etc, where the integers represent the number of available cover elements of different embedding domains in each 8×8 block.

The theoretical security performance of different embedding domains when the embedded messages can be extracted correctly by using an ideal error correction code is shown in Fig. 7. It is obvious that the bigger the embedding domain, the higher the security performance with the same $P_{perfect}$ when utilizing ideal error correction codes. However, the adopted RS codes cannot reach the theoretical bound of error correction ability. To determine the embedding domain in the practical application, additional experiments with RS codes are carried out under the same experimental environment. We use the syntax of names following the convention:

$$name = \{scheme\} - \{distortion\} - \{embeddingdomain\} - \{code\}. \quad (15)$$

For instance, GMAS-JUNI_P-E_{21}-RS(31,15) represents that the robust steganographic scheme is GMAS, the distortion function is JUNI_P, the embedding domain is E_{21} and the error correction code is RS(31,15). It can be observed in Figs. 8 and 9, the embedding domain E_{21} has higher security performance than E_{15} when they have similar extraction error rates. However, the embedding domain E_{26} has lower security performance than E_{21} even it has higher extraction error rates, which reveals some divergence with the theoretical consequence. We implement experiments on other larger

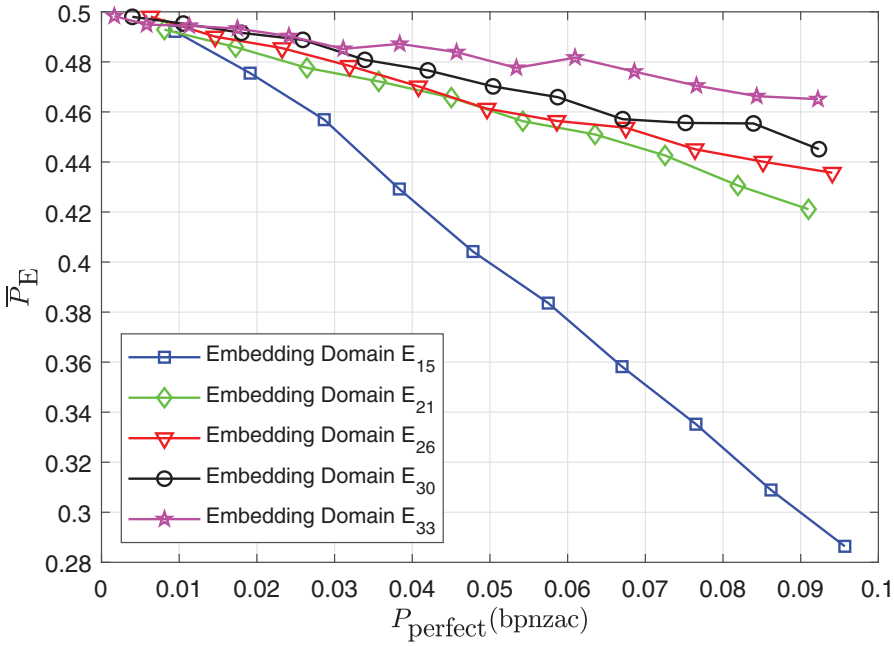
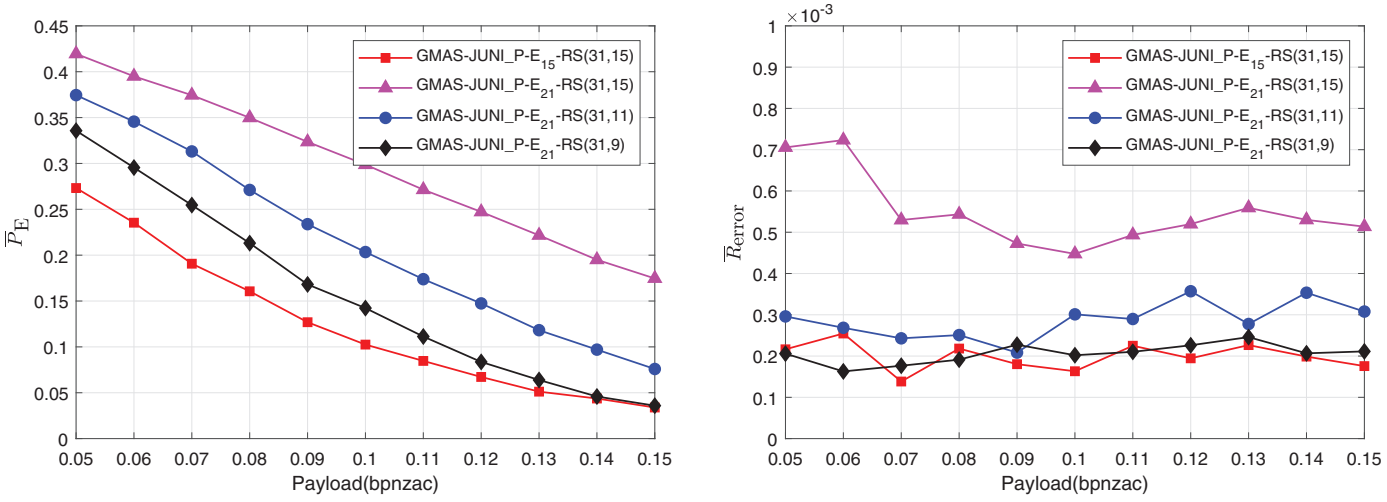


Fig. 7. The theoretical security performance of different embedding domains when the embedded messages can be extracted correctly by using an ideal error correction code. P_{perfect} represents the perfect payload that can be received without any error bits.



(a) CCPEV (b) $Q_{\text{channel}} = 85$

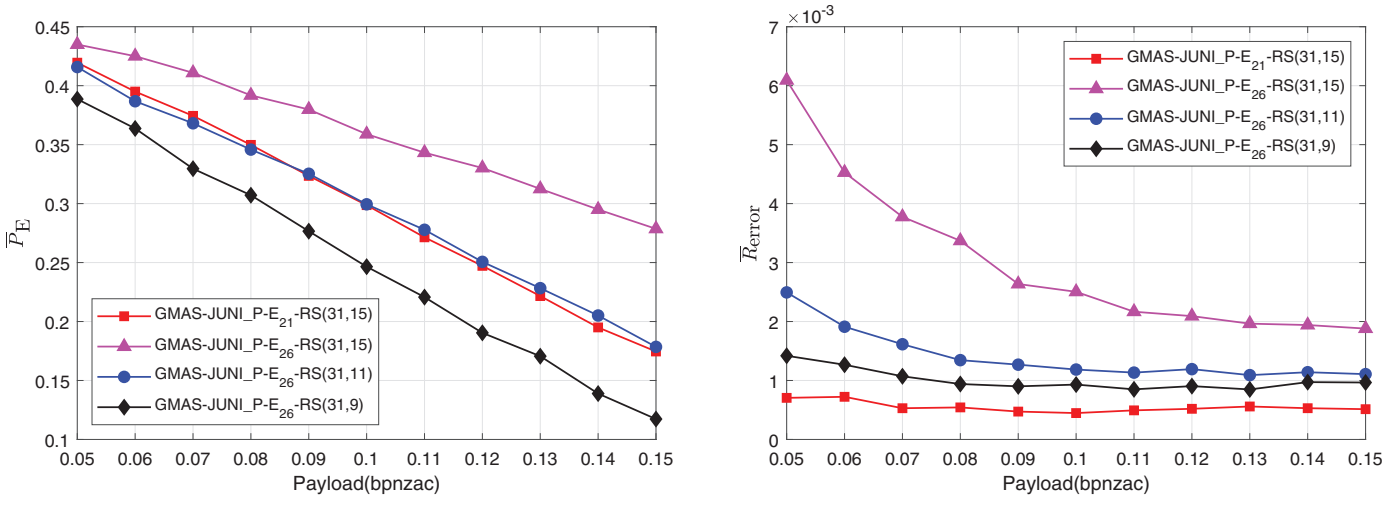
Fig. 8. (a)-(b) are average detection error rates $\overline{P}_E$ and average extraction error rates $\overline{R}_{\text{error}}$ of the proposed scheme GMAS with different embedding domains (E_{15} and E_{21}) and RS codes against CCPEV feature and $Q_{\text{channel}} = 85$ on 2000 images randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 65$, respectively.

embedding domains and obtain similar results. Therefore, we will use E_{21} as our embedding domain in this paper.

4.4. Comparison with DMAS

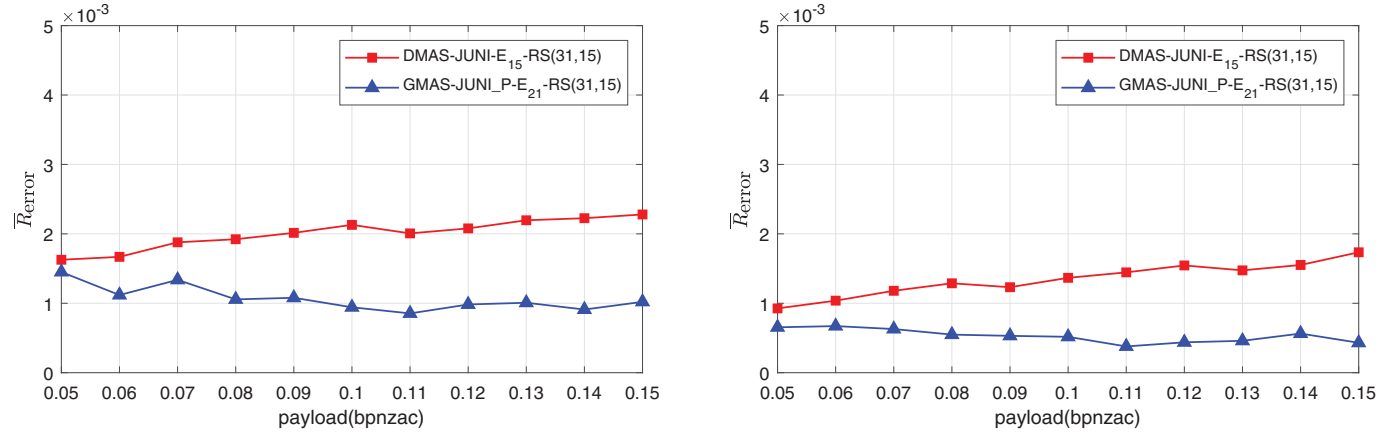
The performance of the proposed scheme GMAS and the original DMAS [15] in terms of robustness and security would be compared, respectively. To assess the robustness, we randomly select 1000 images from BOSSbase 1.01 with $Q_{\text{cover}} = 65$ and set $Q_{\text{channel}} = 85, 95$. Fig. 10 shows the robustness performance of two methods against two channel JPEG compressions. We can see that GMAS surpasses DMAS with distinct advantages in both cases and the extraction error rates of GMAS can reach half of that of DMAS.

When evaluating the security performance, we implement experiments on the whole BOSSbase 1.01 with $Q_{\text{cover}} = 75$ against feature sets CCPEV [20] and DCTR [22]. As shown in Fig. 11, DMAS can only resist CCPEV at very low relative payload such as 0.05 bpnzac, and it is completely unable to resist DCTR, which is consistent with the common sense that the embedding efficiency of binary STCs is low and embedding messages on the middle frequency regions is very insecure. Since our proposed scheme GMAS adopts ternary STCs with generalized dither modulation and expanded embedding domain, it can adaptively cluster as many modifications as possible on the elements with small costs and obtain higher level of security than DMAS obviously. However, their abilities against DCTR are close at high relative payload due to the modifications would be made in the smooth regions.



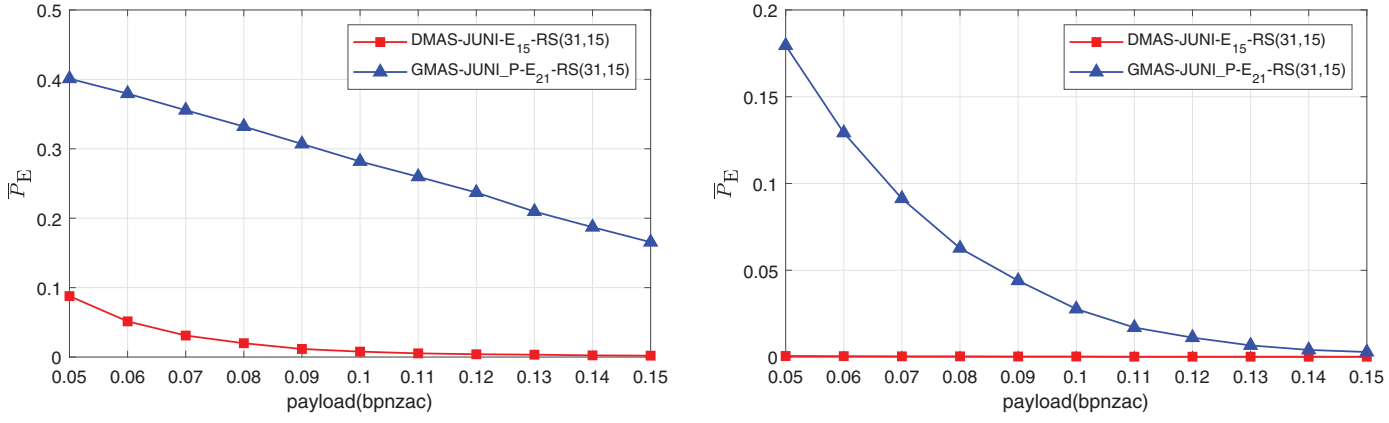
(a) CCPEV (b) $Q_{\text{channel}} = 85$

Fig. 9. (a)-(b) are average detection error rates $\overline{P}_E$ and average extraction error rates $\overline{R}_{error}$ of the proposed scheme GMAS with different embedding domains (E_{21} and E_{26}) and RS codes against CCPEV feature and $Q_{\text{channel}} = 85$ on 2000 images randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 65$, respectively.



(a) $Q_{\text{channel}} = 85$ (b) $Q_{\text{channel}} = 95$

Fig. 10. Average extraction error rates $\overline{R}_{error}$ of DMAS-JUNI-E_{15}-RS(31,15) [15] and GMAS-JUNI_P-E_{21}-RS(31,15) with (a) $Q_{\text{channel}} = 85$ and (b) $Q_{\text{channel}} = 95$, on 1000 images randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 65$, respectively.



(a) CCPEV (b) DCTR

Fig. 11. Average detection error rates $\overline{P}_E$ of DMAS-JUNI-E_{15}-RS(31,15) [15] and GMAS-JUNI_P-E_{21}-RS(31,15) with (a) CCPEV and (b) DCTR, on BOSSbase 1.01 with $Q_{\text{cover}} = 75$, respectively.

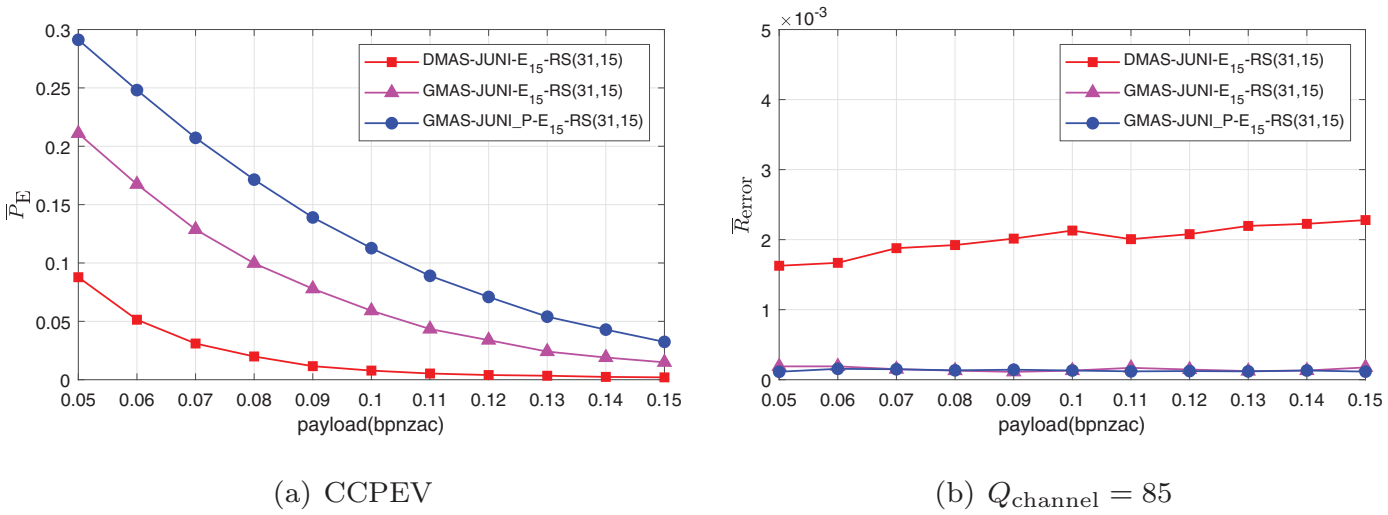


Fig. 12. (a) is average detection error rates $\overline{P}_{\mathrm{E}}$ of DMAS-JUNI-E_{15}-RS(31,15) [15], GMAS-JUNI-E_{15}-RS(31,15) and GMAS-JUNI_P-E_{15}-RS(31,15) against CCPEV on BOSSbase 1.01 with $Q_{\mathrm{cover}} = 75$. (b) is average extraction error rates $\overline{R}_{\mathrm{error}}$ of three methods against $Q_{\mathrm{channel}} = 85$ on 1000 images randomly selected from BOSSbase 1.01 with $Q_{\mathrm{cover}} = 65$.

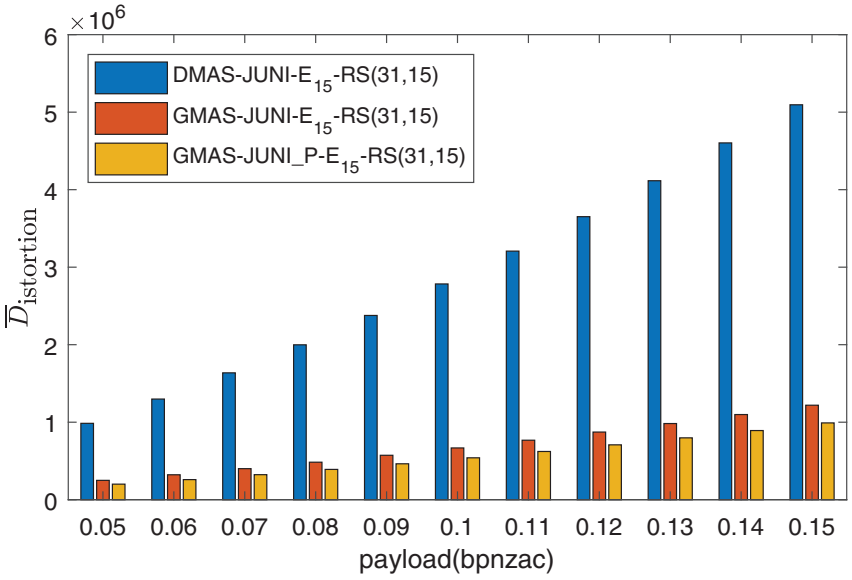


Fig. 13. Average distortion of DMAS-JUNI-E_{15}-RS(31,15) [15], GMAS-JUNI-E_{15}-RS(31,15) and GMAS-JUNI_P-E_{15}-RS(31,15) on 1000 images randomly selected from BOSSbase 1.01 with $Q_{\mathrm{cover}} = 75$.

4.5. Effectiveness of generalized dither modulation using ternary STCs

We conduct some comparative experiments to investigate the effectiveness of generalized dither modulation using ternary STCs. For a fair comparison, all the three methods adopt the embedding domain E_{15} just like [15] and GMAS-JUNI-E_{15}-RS(31,15) is the same as DMAS-JUNI-E_{15}-RS(31,15) except for utilizing ternary STCs. According to the results shown in Fig. 12, it is evident that GMAS-JUNI-E_{15}-RS(31,15) performs far better than DMAS-JUNI-E_{15}-RS(31,15) in terms of robustness and security. It may be on account of the higher embedding efficiency of ternary STCs than binary STCs, which could cause fewer modifications and smaller distortion when embedding the same messages. Besides, the security performance of GMAS-JUNI-E_{15}-RS(31,15) can be greatly improved by generalized dither modulation, i.e., GMAS-JUNI_P-E_{15}-RS(31,15), and the reason for which could be that generalized dither modulation can restrain the embedding changes of short modification distances but high embedding costs.

To further verify the above conjecture, the average distortion of the three methods are shown in Fig. 13, which demonstrates that both generalized dither modulation and ternary STCs contribute largely to reduce the average distortion and support the effectiveness of the proposed scheme.

4.6. How to embed when knowing $Q_{channel}$

As long as Q_{cover} is no larger than Q_{channel}, the proposed scheme can work quite well and does not need to know any extra information about SNPs. However, it could happen that we know some useful information in the actual scenario, such as Q_{channel}. How should we select covers to embed messages in this case? The results in Fig. 14 illustrate that we should select images whose Q_{cover} is identical to Q_{channel} to embed message when Q_{channel} is less than 79, and it is a wise choice to embed message on images with Q_{cover} smaller than Q_{channel} in other cases. Moreover, it is clear that we

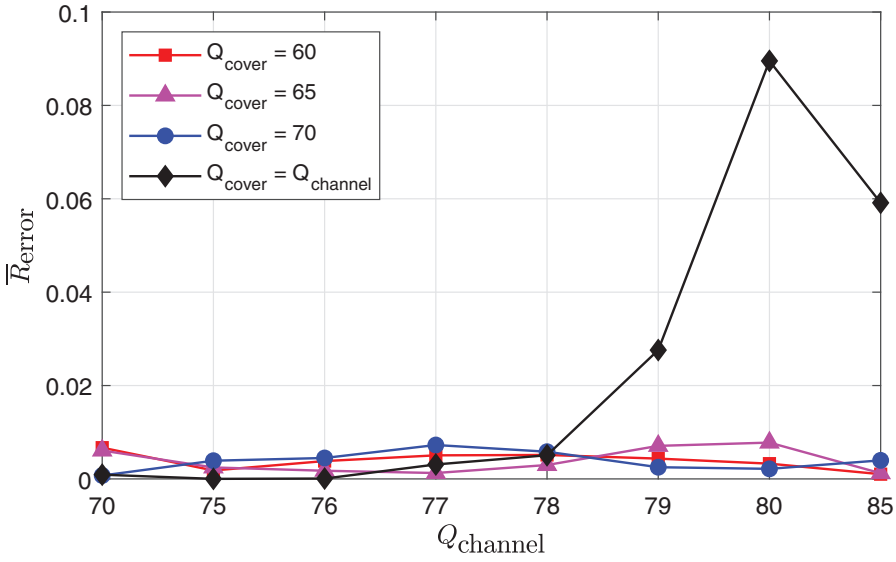


Fig. 14. Average extraction error rates $\overline{R}_{\text{error}}$ of GMAS-JUNI_P-E_{21}-RS(31,15) at 0.1 bpnzac when knowing Q_{channel} on 1000 images randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 60, 65, 70,$ and $Q_{\text{cover}} = Q_{\text{channel}}$.

Table 3
Robustness of GMAS-JUNI_P-E_{21}-RS(31,15) in terms of $\overline{R}_{\text{error}}$ and N_{success} versus Facebook with 60 images randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 60, 65, 70$ and each contains 20 images at 0.1 bpnzac.

SNP	Quality Factor	60	65	70
Facebook	$\overline{R}_{\text{error}}$	.002425	.00123	.0001
	N_{success}	16	15	19

will obtain comparable robustness as long as Q_{cover} is smaller than Q_{channel}.

4.7. Applications

We apply our proposed scheme GMAS to the most popular SNP, Facebook, to test its robustness. Facebook's JPEG encoder is complex and changed over time, which will resize and recompress the uploaded images according to their sizes and quality factors. For small size images (such as 512×512), Facebook will recompress them with $Q_{\text{channel}} = 71$ as long as Q_{cover} is no larger than 85, and otherwise, Q_{channel} varies from image to image. We upload 60 images (randomly selected from BOSSbase 1.01 with $Q_{\text{cover}} = 60, 65, 70$ and each contains 20 images) with hidden messages using GMAS-JUNI_P-E_{21}-RS(31,15) to Facebook, and the results are shown in Table 3, where N_{success} denotes the number of images from which the messages can be completely extracted. As expected, our scheme GMAS has strong robustness and can be applied to the real world effectively.

Since we just set the secure parameter $h = 10$ in STCs and adopt RS(31,15) for all images to maintain high undetectability, it is inevitable that there are still a small number of error bits for some images. We believe that these error bits can be eliminated by enhancing the error correction ability of RS codes or decreasing the parameter h of STCs as suggested in [18,31], which should be reconsidered in the future.

5. Conclusions

Nowadays, posting images on SNPs happens everywhere and every single second, which facilitates covert communication. However, images transmitted through such channels will usually be JPEG compressed, which fails the correct message extraction of the existing steganographic schemes. Although the previously proposed DMAS owns strong robustness against JPEG compression, its ability of resisting steganalysis is very weak.

In this paper, we propose a refined robust adaptive steganographic scheme by exploring efficient embedding method and expanding the embedding domain. Firstly, we obtain a more effective asymmetric distortion scheme by utilizing a more meticulous compensation and distortion adjustment method. Secondly, the generalized dither modulation method is proposed and then utilized to implement ternary embedding with double-layered STCs, which can enhance the performance of robustness and security significantly. To further improve the detection resistant capability, we expand the embedding domain through building a theoretical model and conducting practical experiments. The experimental results verify that the proposed scheme outperforms the original DMAS in terms of robustness and security observably.

In the future, we will intend to combine error correction and embedding more reasonably like [31] to further improve the overall performance of this work. In addition, expanding this work to color image is also a part of our future work.

Declaration of Competing Interest

None.

Acknowledgement

This work was supported in part by the Natural Science Foundation of China under Grant U1636201 and 61572452, by Anhui Initiative in Quantum Information Technologies under Grant AHY150400, and by the Fundamental Research Funds for the Central Universities WK6030000135.

References

[1] H.-W. Tseng, C.C. Chang, Steganography using JPEG-compressed images, in: in The Fourth International Conference on Computer and Information Technology, 2004. CIT'04., IEEE, 2004, pp. 12–17.
[2] A. Cheddad, P. Mc Kevitt, J. Condell, K. Curran, Digital image steganography: survey and analysis of current methods, Signal Process. 90 (3) (2010) 727–752.
[3] R.M. Rad, K. Wong, An efficient sign prediction method for DCT coefficients and its application to reversible data embedding in scrambled JPEG image, in: 2013 IEEE International Conference on Image Processing, IEEE, 2013, pp. 4442–4446.

[4] T. Filler, J. Judas, J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 920–935.
[5] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, EURASIP J. Inf. Secur. 2014 (1) (2014) 1–13.
[6] L. Guo, J. Ni, W. Su, C. Tang, Y.Q. Shi, Using statistical image model for JPEG steganography: uniform embedding revisited, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2669–2680.
[7] Q. Wei, Z. Yin, Z. Wang, X. Zhang, Distortion function based on residual blocks for JPEG steganography, Multimed. Tools Appl. (2017) 1–14.
[8] X. Hu, J. Ni, Y.Q. Shi, Efficient JPEG steganography using domain transformation of embedding entropy, IEEE Signal Process. Lett. 6 (25) (2018) 773–777.
[9] W. Su, J. Ni, X. Li, Y.Q. Shi, A new distortion function design for JPEG steganography using the generalized uniform embedding strategy, IEEE Trans. Circuits Syst. Video Technol. 28 (12) (2018) 3545–3549.
[10] B. Li, S. Tan, M. Wang, J. Huang, Investigation on cost assignment in spatial image steganography, IEEE Trans. Inf. Forensics Secur. 9 (8) (2014) 1264–1277.
[11] Z. Wang, Z. Yin, X. Zhang, Asymmetric distortion function for JPEG steganography using block artifact compensation, International Journal of Digital Crime and Forensics (IJDCF) 11 (1) (2019) 90–99.
[12] Z. Wang, Z. Qian, X. Zhang, M. Yang, D. Ye, On improving distortion functions for JPEG steganography, IEEE Access 6 (2018) 74917–74930.
[13] Y. Zhang, X. Luo, C. Yang, D. Ye, F. Liu, A framework of adaptive steganography resisting JPEG compression and detection, Secur. Commun. Netw. 15 (9) (2016) 2957–2971.
[14] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, 1977.
[15] Y. Zhang, X. Zhu, C. Qin, C. Yang, X. Luo, Dither modulation based adaptive steganography resisting JPEG compression and statistic detection, Multimed. Tools Appl. 77 (14) (2018) 17913–17935.
[16] Y. Zhang, C. Qin, W. Zhang, F. Liu, X. Luo, On the fault-tolerant performance for a class of robust image steganography, Signal Process. 146 (2018) 99–111.
[17] J. Tao, S. Li, X. Zhang, Z. Wang, Towards robust image steganography, IEEE Trans. Circuits Syst. Video Technol. (2018).
[18] Z. Zhao, Q. Guan, H. Zhang, X. Zhao, Improving the robustness of adaptive steganographic algorithms based on transport channel matching, IEEE Trans. Inf. Forensics Secur. (2018).
[19] G. Forney, On Decoding BCH Codes, IEEE Trans. Inf. Theory 11 (4) (1965) 549–557.
[20] J. Kodovskỳ, J. Fridrich, Calibration revisited, in: Proceedings of the 11th ACM workshop on Multimedia and security, ACM, 2009, pp. 63–74.
[21] T. Pevny, J. Fridrich, Merging Markov and DCT features for multi-class JPEG steganalysis, in: Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505, 2007, p. 650503. International Society for Optics and Photonics
[22] V. Holub, J. Fridrich, Low-complexity features for JPEG steganalysis using undecimated DCT, IEEE Trans. Inf. Forensics Secur. 10 (2) (2015) 219–228.
[23] B. Chen, G.W. Wornell, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Trans. Inf. Theory 47 (4) (2001) 1423–1443.
[24] H. Noda, M. Niimi, E. Kawaguchi, High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recognit. Lett. 27 (5) (2006) 455–461.
[25] A. Miyazaki, A. Okamoto, Analysis of watermarking systems in the frequency domain and its application to design of robust watermarking systems, IEICE Trans. Fundam. Electron.Commun. Comput. Sci. 85 (1) (2002) 117–124.
[26] C. Li, Z. Zhang, Y. Wang, B. Ma, D. Huang, Dither modulation of significant amplitude difference for wavelet based robust watermarking, Neurocomputing 166 (2015) 404–415.
[27] C.-C. Chang, C.-C. Lin, C.-S. Tseng, W.L. Tai, Reversible hiding in DCT-based compressed images, Inf. Sci. 177 (13) (2007) 2768–2786.
[28] P. Bas, T. Filler, T. Pevnỳ, Break our steganographic system the ins and outs of organizing boss, in: International Workshop on Information Hiding, Springer, 2011, pp. 59–70.
[29] J. Kodovskỳ, J.J. Fridrich, V. Holub, Ensemble classifiers for steganalysis of digital media, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 432–444.
[30] R.W. Hamming, Coding and Theory, Prentice-Hall Englewood Cliffs, 1980.
[31] C. Kin-Cleaves, A. Ker, Adaptive steganography in the noisy channel with dual-syndrome trellis codes, 2018.