
Article:
Zhang, Yi, Luo, Xiangyang, Zhu, Xiaodong et al. (2 more authors) (2019) Enhancing reliability and efficiency for real-time robust adaptive steganography using cyclic redundancy check codes. JOURNAL OF REAL-TIME IMAGE PROCESSING. 115–123. ISSN 1861-8200

https://doi.org/10.1007/s11554-019-00905-7

J Real-Time Image Proc manuscript No.
(will be inserted by the editor)

Enhancing Reliability and Efficiency for Real-time Robust Adaptive Steganography Using Cyclic Redundancy Check Codes

Yi Zhang · Xiangyang Luo* · Xiaodong Zhu · Zhenyu Li · Adrian G. Bors

Received: date / Accepted: date

Abstract The development of multimedia and deep learning technology bring new challenges to steganography and steganalysis techniques. Meanwhile, robust steganography, as a class of new techniques aiming to solve the problem of covert communication under lossy channels, has become a new research hotspot in the field of information hiding. To improve the communication reliability and efficiency for current real-time robust steganography methods, a concatenated code, composed of Syndrome-Trellis Codes (STC) and Cyclic Redundancy Check (CRC) codes, is proposed in this manuscript. Using its strong error detection capability, high coding efficiency and low embedding costs, an enhanced robust adaptive steganography framework and three adaptive steganographic methods resisting JPEG compression and detection are proposed. On this basis, to provide a theoretical reference for message extraction integrity, the fault tolerance of the proposed steganography methods is analyzed using the residual model of JPEG compression, thus obtaining the appropriate coding parameters. Experimental results show that the proposed methods have a significantly stronger robustness against compression, and are more difficult to be detected by statistical based steganalytic methods comparing with existing robust steganography methods.

Keywords Robust steganography · STC-CRC codes · JPEG compression resistant · Statistical detection resistant

Yi Zhang · Xiangyang Luo · Xiaodong Zhu · Zhenyu Li
State Key Laboratory of Mathematical Engineering and Advanced Computing, 62# Science Rd, Zhengzhou, China.
E-mail: tzyy4001@sina.com, luoxy_ieu@sina.com (corresponding author), zxd10@tsinghua.org.cn, zheenyuli@gmail.com

Adrian G. Bors
Department of Computer Science, University of York, York YO10 5GH, York, United Kingdom.E-mail: adrian.bors@york.ac.uk

1 Introduction

With the rapid development of multimedia technology and intelligent devices, digital images processed and transmitted by the smart mobile devices have become an important potential carrier for covert communication [13]. Meanwhile, the deep learning technology has made a tremendous progress in the past few years, which brings new challenges for covert communication [19][17]. Hence, the real-time image steganography based on instant communication tools, for its excellent concealment and outstanding convenience, has become a new research hotspot in the field of information hiding techniques. However, JPEG image compression, which usually happens to cover images during the transmission through instant communication tools, brings a serious threat for the transmission of covert information [24], such as that embedded by steganographic algorithms proposed in [27], [25], [12] and so on. Furthermore, image steganalysis algorithms based on deep learning technology, such as Convolutional Neural Network (CNN) models, often use various network structures to learn the effective features of images to distinguish cover and stego images [18], thus proposing higher requirements for the detection resistant performance of steganographic algorithms. Therefore, how to balance the resilience of embedded messages under lossy channel [1] and the detection resistance of stego images [3] is a major problem for image steganography on mobile devices, which access multiple changing communication channels.

For detection resistant image steganography techniques, current adaptive steganography algorithms, such as Highly Undetectable steGO (HUGO) steganography [11], Wavelet Obtained Weights (WOW) steganography [6], MiPOD (Minimizing the Power of Optimal Detector) [14], JPEG UNIversal Wavelet Relative Distortion (J-UNIWARD) steganography [7] and other algorithms [5], have become a research priority in the field of information hiding techniques. Utiliz-

ing the appropriately defined distortion functions and minimizing embedding cost codes —— STCs (Syndrome-Trellis Codes) [4], these algorithms can adaptively select embedding locations according to the content of cover images, thus realizing message embedding with a good detection resistance against steganalysis based on statistical features [8]. However, these algorithms usually do not consider the situation when the stego images are attacked during the transmission through public lossy channels exposed to image processing attacks, resulting in the embedded messages hard to survive after these attacks and the failure of covert communication under lossy channels [20].

In terms of JPEG compression resistance information hiding techniques, robust watermarking algorithms can realize message embedding with a good visual invisibility and a strong resistance against JPEG compression and other image processing attacks. Utilizing the robust embedding domains constructed based on imposing constraints[2], coefficients' relationships [10], image features [15, 16], or other methods, these algorithms can embed and retrieve watermarks with a high accuracy after the watermarked images are suffered from different image processing attacks. However, it should be noted that the embedding capacity of these algorithms might be relatively limited considering the visual quality of watermarked images. Meanwhile, these methods often leave out the statistical detection resistance of watermarked images, and the successful retrieval of the watermark is not guaranteed [20], which results in a non-secure covert communication under lossy channel.

Since the above information hiding algorithms cannot realize message embedding with both JPEG compression and detection resistance, utilizing the advantages of adaptive steganography and robust watermarking, the DCRAS (DCT Coefficients Relationship based Adaptive Steganography), FRAS (Feature Region based Adaptive Steganography), and DMAS (Dither Modulation based Adaptive Steganography), are proposed in previous studies [21, 22, 26], respectively. Utilizing the coefficients' relationship invariability against compression, the embedding domain is constructed in the DCRAS algorithm. Combined with the embedding cost function to measure compression and detection resistance, messages are embedded by STCs with minimum costs after RS coding, thereby acquiring both compression and detection resistance. On this basis, the FRAS algorithm utilizes the Harris-Laplacian feature to construct and select the compression maintainable image regions, achieving the balance between JPEG compression and detection resistant properties of cover elements. Combined with the embedding cost function, RS coding and STCs, the message embedding with minimal costs can be realized. For DMAS algorithm, the embedding domain is constructed based on the correspondence between quantization tables and coefficients' variance caused by compression, and the cost function is enriched with the side-information corresponding to the quantization errors of different locations, thus realizing robust adaptive steganography based on RS-STCs with lower complexity.

Although the above three robust adaptive steganographic methods can achieve basic resistance to JPEG compression and detection, the serious error spreading problem caused by STCs decoding and heavy error correction burden of RS codes [23] lead to the bottleneck in embedding efficiency and detection resistance. Therefore, how to achieve higher reliability, lower cost and higher efficiency of message coding and embedding is a key issue that limits the further development of robust steganography. To this end, we propose to combine the Cyclic Redundancy Check (CRC) codes with STCs in this paper, in order to achieve message coding and embedding with higher reliability and efficiency, and solve the error spreading problem caused by STC decoding, thus providing a preliminary solution for secure and reliable covert communication under lossy channel exposed to JPEG compression attacks.

In the next section, the enhanced robust steganography based on STC-CRC codes is proposed. In Section 3, the fault tolerance is analyzed, and the recommended coding parameters are given as well. The experiment results are presented in Section 4, and the paper is concluded in Section 5.

2 Enhanced Robust Steganography

In order to solve the heavy error spreading problem caused by STCs and JPEG compression for current robust adaptive steganography methods, the STC-CRC codes is proposed in this section, considering both error detection and correction performance, thus enhancing the framework of robust adaptive steganography in terms of communication reliability and efficiency at the same time.

2.1 STC-CRC Codes

The principle of the proposed concatenated code, STC-CRC codes, can be described as follows. Suppose the cover and stego sequences with length l are $\mathbf{c}$, $\mathbf{s}$ respectively, and the message sequence with length n is $\mathbf{m}$. The messages is first embedded into the cover sequences using STC codes [4], which can be expressed by the following formulas.

$$\mathbf{s} = \mathrm{Emb}(\mathbf{c}, \mathbf{m}) = \arg \min_{\mathbf{s} \in \mathbf{C}(\mathbf{m})} D(\mathbf{c}, \mathbf{s}) \tag{1}$$

$$\mathbf{m} = \mathrm{Ext}(\mathbf{s}) = \mathbf{H}\mathbf{s} \tag{2}$$

where $\mathbf{H} \in \{0,1\}^{n \times l}$ is a parity-check matrix, $D(\mathbf{c}, \mathbf{s})$ is the distortion function which can measure the embedding cost of each cover element, and $\mathbf{C}(\mathbf{m}) = \left\{ \mathbf{z} \in \{0,1\}^l | \mathbf{H}\mathbf{z} = \mathbf{m} \right\}$ is the coset corresponding to syndrome $\mathbf{m}$.

Since the errors will spread in the extracted stego sequences after STCs decoding when stego sequences are damaged during the transmission through public lossy channels, which can be seen from Formula (2), the CRC codes [9] is utilized to encode the stego sequences after STCs and detect errors in received stego sequences before STCs decoding, in order to guarantee the reliability of extracted messages after JPEG compression and improve the coding efficiency of error checking and correcting codes.

Suppose the generator polynomial with the highest power k is $G(x)$, and the stego sequence $\mathbf{s}$ with length l is denoted by $\mathbf{y} = (y_{l-1}, y_{l-2}, \cdots, y_1, y_0)$. The CRC coding and verification process can be presented by the following formulas.

$$x^k Y(x) + R(x) = Q(x) \cdot G(x) \tag{3}$$

$$R(x) = r_{k-1}x^{k-1} + r_{k-2}x^{k-2} + \cdots + r_1 x + r_0 \tag{4}$$

where $Y(x) = y_{l-1}x^{l-1} + y_{l-2}x^{l-2} + \cdots + y_1 x + y_0$, $Q(x)$ is the quotient polynomial, and $R(x)$ is the remainder polynomial. Then the check sequence $\mathbf{r}$ and generated coding sequence $\mathbf{y}_c$ can be expressed as follows.

$$\mathbf{r} = (r_{k-1}, r_{k-2}, \cdots, r_1, r_0) \tag{5}$$

$$\mathbf{y}_c = (y_{l-1}, y_{l-2}, \cdots, y_1, y_0, r_{k-1}, r_{k-2}, \cdots, r_1, r_0) \tag{6}$$

During the procedure of verification, if the received sequence is divisible by $G(x)$, the messages are considered to be accurate, otherwise it is considered some errors have occurred during transmission.

By appropriately selecting the generator polynomial, the CRC codes can correct any random error of length 1, and detect any burst error of length $b \leq k$ [9]. In the context of robust embedding domain, the combination of STCs and CRC codes can realize message embedding with minimum costs while detecting and correcting the few errors caused by compression in stego sequences, thus solving the error spreading problem caused by STC decoding and acquiring higher reliability and efficiency.

2.2 Robust Steganography Framework

Based on the structure of "Compression-resistant Domain Constructing + STC-CRC Codes", a robust adaptive steganography framework which can enhance both communication reliability and efficiency is proposed in this section, which is shown in Figure 1.

The embedding process includes the following two steps.

(1) **Compression-resistant Domain Constructing**
   (a) *Embedding Domain and Methods Constructing*: Construct, select and extract the coefficients, regions, or relationships that are robust to JPEG compression, and apply certain embedding method, such as that of DCRAS [21], FRAS [22] and DMAS [26], to reshape cover sequence $\mathbf{c}$ with length l_c.
   (b) *Embedding Cost Function Design*: Improve distortion functions of adaptive steganography considering the robustness of cover elements. Design and calculate embedding costs corresponding to the above embedding domains.

(2) **Message Embedding with Minimized Costs**
   (a) *STC Coding*: Scramble the cover sequence $\mathbf{c}$ and encrypt message $\mathbf{m}$ to obtain $\mathbf{c}_s$ and $\mathbf{m}_e$ respectively. If the message length in each group of CRC codes is l_r, and the highest power of generator polynomial is k, the cover length for STC coding can be calculated by equation (1) ($\lceil \bullet \rceil$ means the ceiling integer of $\bullet$). Extract the first l_e bits from $\mathbf{c}_s$ to obtain cover sequence $\mathbf{c}_e$, and perform STC coding to generate stego sequence $\mathbf{s}_e$.
   $$l_e = l_c - \left\lceil \frac{l_c}{l_r} \right\rceil \cdot k \tag{7}$$
   (b) *CRC Coding*: Perform CRC coding to $\mathbf{s}_e$ using $G(x)$ according to the group length l_r, and connect every group of CRC codes to obtain sequence $\mathbf{r}_c$ with length $k \cdot \lceil l_e / l_r \rceil$. In accordance with the above embedding method, embed $\mathbf{r}_c$ into the first $k \cdot \lceil l_e / l_r \rceil$ bits of the remaining cover sequence $\mathbf{c}_s$ with length $l_c - l_e$, thus obtaining stego sequence $\mathbf{s}_s$. Inversely scramble $\mathbf{s}_s$ to obtain sequence $\mathbf{s}$ and generate the corresponding stego image.

Accordingly, the extraction process mainly includes the following two steps.

(1) **Compression-resistant Elements Extracting**
Utilizing the compression resistant embedding domain construction methods corresponding to the embedding process, such as that of DCRAS [21], FRAS [22] and DMAS [26], extract the stego elements sequence $\mathbf{s}'$ with length $l_{s'}$ ($l_{s'} = l_c$).

(2) **Stego Sequence Decoding**
   (a) *Scrambling*: Scramble the stego sequence $\mathbf{s}'$ to obtain sequence $\mathbf{s}'_s$, utilizing the same scrambling algorithm as message embedding process.
   (b) *CRC Decoding*: Perform CRC decoding using $G(x)$ for each group of CRC codes in the first $l_e + k \cdot \lceil l_e / l_r \rceil$ elements in stego sequence $\mathbf{s}'_s$, in which the first l_e bits are the extracted STC codes and the rest $k \cdot \lceil l_e / l_r \rceil$ bits are the extracted CRC codes using for error detecting and correcting. Then, obtain the STC code sequence $\mathbf{s}'_e$ with length l_e after CRC decoding.
   (c) *STC Decoding*: Perform STC decoding to the sequence $\mathbf{s}'_e$ utilizing the same parameters used in the message embedding process, and obtain the extracted message sequence $\mathbf{m}'_e$. Then, decrypt message sequence $\mathbf{m}'_e$ with the same key used to encrypt the secret messages before embedding, and obtain extracted message sequences $\mathbf{m}'$.

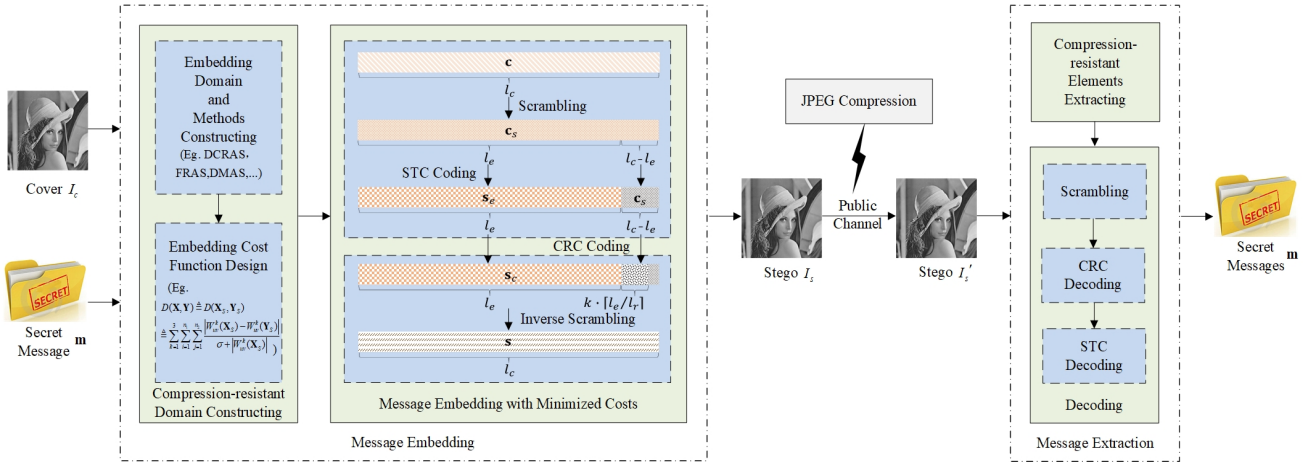


Fig. 1 Robust steganography framework based on “Compression-resistant Domain Construction + STC-CRC Codes"

Above all, based on the proposed framework, the current robust steganography methods, such as DCRAS, FRAS and DMAS, can be enhanced by utilizing the strong error detection capability, appropriate error correction capability and high coding efficiency of CRC codes, thereby taking communication security, reliability and efficiency into consideration. In the following sections, the enhanced version of these methods mentioned above are denoted as E-DCRAS, E-FRAS and E-DMAS.

3 Analysis of Fault Tolerance

In this section, utilizing the residual model of JPEG compression [23], the fault tolerance of proposed methods is analyzed, and the coding parameters are discussed as well.

Based on the similarity between JPEG compression residuals and burst errors, the errors in stego images caused by compression can be described as a series of Poisson points t_i with average rate v and length d, and the number of non-zero residuals n_l in successive stegos of length l has a the Poisson distribution with the following probability density function,

$$P(n_l = n_s) = \frac{\lambda^{n_s}}{n_s!}\cdot e^{-\lambda}, n_s = 0,1,\cdots \tag{8}$$

where $\lambda = v\cdot d$ is the average rate of burst errors, and also that of non-zero residuals in successive stegos of length l.

Considering the error detection and correction capability of CRC codes under appropriate generator polynomials, the fault tolerance of proposed methods is given as below,

(1) if $\lambda\cdot l \le k$, all the errors in stego sequences of length l can be detected, thus the communication reliability can be ensured for the extracted message sequences;

(2) if $\lambda\cdot l \le 1$, the bust error in stego sequences of length l can be corrected, thus the communication accuracy can be guaranteed for the extracted message sequences.

On this basis, the recommended CRC coding parameters can be given corresponding to compression-resistant domains with different average burst error rates λ. According to the conclusion in [23], the parameter λ can be approximately estimated by the stego sequences' average error rates λ'. Then utilizing the compression-resistant embedding domains defined in DCRAS, FRAS and DMAS with parameters in Table 1, the average error rates λ' of cover sequence constructed from randomly selected 2000 images after JPEG compression with quality factors of 65, 75, and 85 are calculated, and the results are shown in Table 2.

Table 1 Parameters Settings

Parameters	DCRAS	FRAS	DMAS
Maximum cost	10^8	10^8	10^8
Iterations T_{step}	3	\	\
Population size N_g	\	100	\
Iterations N_i	\	20	\
Quantify tables	\	\	T_{65}, T_{75}, T_{85}

Table 2 Error Rates of Stego Sequences ($\times 10^{-4}$)

Error rates λ'	QF = 65	QF = 75	QF = 85
λ'_1 of DCRAS	0.12	0.09	0.34
λ'_2 of FRAS	7.26	6.73	8.02
λ'_3 of DMAS	0.13	0.26	0.30

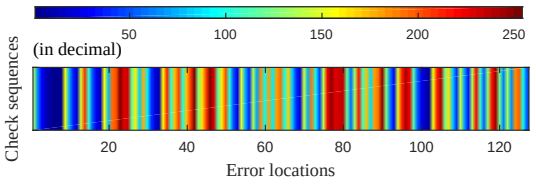
According to the error detection performance of some frequently used CRC codes [9], the appropriate coding parameters can be selected for the above three compression-resistant domains corresponding to their error rates after compression, that is, CRC-8 (0x011D), CRC-12 (0x080F) and

CRC-16 (0x1021). The error rates after error checking of different average error rates λ are shown in Table 3 (where $G(x)$ is the generator polynomial, k is the highest power of $G(x)$, l_r is the code length, and d_h is the Hamming distance).

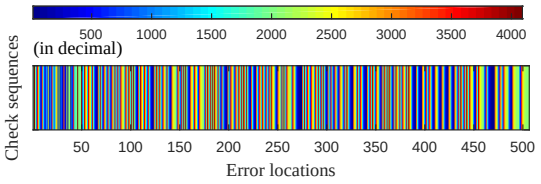
Table 3 Error Rates after CRC Checking [9].

$G(x)$	k	l_r	d_h	$\lambda = 10^{-4}$	$\lambda = 10^{-5}$
0x011D	8	2^7-1	3	1.27×10^{-10}	1.27×10^{-13}
0x080F	12	$2^{11}-1$	4	6.97×10^{-11}	6.97×10^{-15}
0x1021	16	$2^{15}-1$	4	8.78×10^{-10}	8.78×10^{-14}

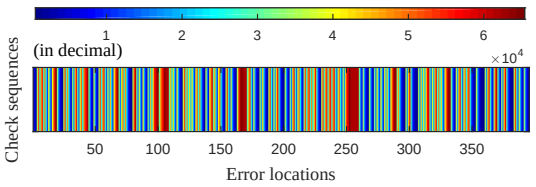
Moreover, a one-to-one correspondence can be found between the check sequence and error location when a burst error occurs, by setting the l_r of the CRC codes as 127, 506 and 395 respectively, which is illustrated in Figure 2.



(a) CRC-8



(b) CRC-12



(c) CRC-16

Fig. 2 One-to-one correspondence in CRC codes

In Figure 2, according to the location of error bit, check sequences of CRC codes in decimal are shown by different colors. From the results, it can be concluded that by selecting appropriate error checking and correcting codes, the errors in received sequences can be found and correct, and a good error detection performance and satisfactory correction capability can be obtained. For the proposed robust steganography framework, comparing with the other coding parameters, the CRC-8 (0x011D) and CRC-12 (0x080F) have better communication reliability and coding efficiency, and consequently are chosen for the proposed approach.

4 Experimental Results

In this section, the performance of the proposed methods is tested comparing with current robust steganography methods in terms of compression and detection resistance.

4.1 Experimental Setting

In the following experiments, the cover sets are constructed by applying JPEG compression with quality factors of 65, 75 and 85, respectively, to the 10000 spatial images in the Bossbase 1.01 database. Then 2000 images are selected randomly corresponding to each group of cover images with different quality factors, and the stego images are generated using DCRAS, FRAS and DMAS with (31,23) RS codes and parameters as Table 1, when considering payloads ranging from 0.01 to 0.1 bpnzAC (bits per non-zero AC coefficient in DCT domain). For the proposed methods, the compression-resistant domains are combined with STC-CRC codes, denoted as E-DCRAS/FRAS/DMAS-8/12, while the stegos are also generated under 3 different quality factors and 10 different payloads. The experiment parameters are shown in Table 4 in details.

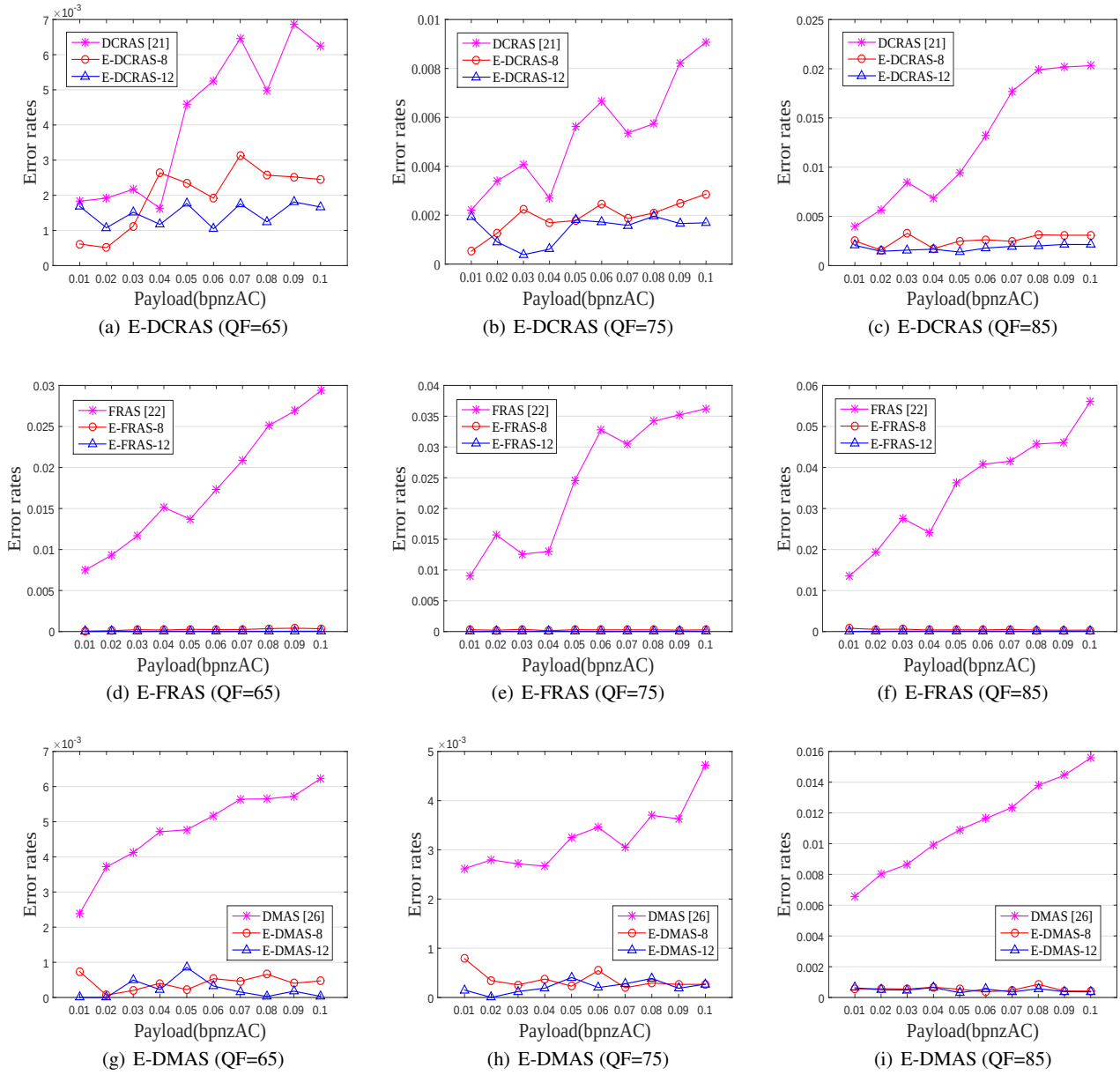
Table 4 Experiment parameters.

Parameters	Settings
Image source	BOSSbase 1.01 image database
Image size	512×512
Quality factors	65/ 75/ 85
Cover sets	10000×3
Cover image numbers	2000 (Randomly selected)$\times$ 3
Payloads	0.01, 0.02, ..., 0.1 bpnzAC
Secret messages	Randomly generated binary sequences
RS coding parameters	(31,23)
Compared methods	DCRAS [21]/ FRAS [22]/ DMAS [26]
Coding parameters	CRC-8 (0x011D)/ CRC-12 (0x080F)
Stego image numbers	$2000\times3\times10\times(3+1\times2)=300,000$

4.2 JPEG Compression Resistance

After compressing the stego images generated by three existing robust steganography methods and the proposed methods with quality factors of 65, 75 and 85, the embedded messages are extracted and the average error rates after CRCs correction are calculated and shown in Figure 3.

The experimental results in Figure 3 demonstrate that comparing with current robust steganography methods, the



(a) E-DCRAS (QF=65) (b) E-DCRAS (QF=75) (c) E-DCRAS (QF=85)

(d) E-FRAS (QF=65) (e) E-FRAS (QF=75) (f) E-FRAS (QF=85)

(g) E-DMAS (QF=65) (h) E-DMAS (QF=75) (i) E-DMAS (QF=85)

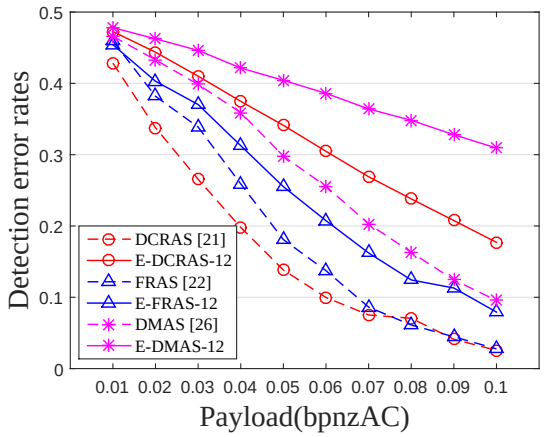
Fig. 3 Average error rates of the extracted messages

message extraction error rates of the proposed methods after compression are significantly reduced, especially for FRAS, whose message extraction accuracy is improved by more than 100 times. It is also shown in Figure 3 that the message error rates of the proposed methods, E-DCRAS, E-FRAS and E-DMAS, are relatively stable and at lower level when the payload varies. This is mainly because the strong and stable error correction and detection performance of CRC codes, which is less affected by the embedding domain and different payloads. In addition, similar experimental results can be achieved when the stego images are suffered from JPEG compression with other quality factors. Thus, it can be concluded that utilizing the strong error detection and satisfactory correction capability of CRC codes, the proposed methodology achieves steganography on a communication channel robust to JPEG compression.

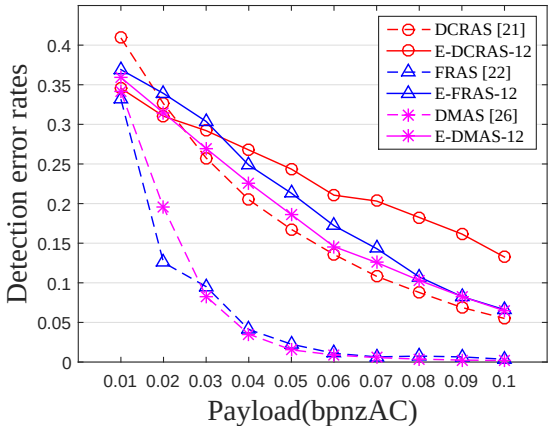
4.3 Statistical Detection Resistance

Utilizing the typical CCPEV (Cartesian Calibrated PEV) and DCTR (Discrete Cosine Transform Residual) steganalytic algorithms, the steganalytic features are extracted from the JPEG compressed cover images with 65 quality factor and the corresponding stego images generated by three existing robust steganography methods and the proposed methods

with payloads of 0.01 to 0.1 bpnzAC. Then half of the samples in the cover images and each group of stego images are selected randomly to train the ensemble classifier, while the rest are used to test the detection resistance, and the results are shown in Figure 4.



(a) Detection error rates against CCPEV features



(b) Detection error rates against DCTR features

Fig. 4 Detection error rates

In Figure 4, the average detection error rates of the enhanced robust steganography methods are illustrated by solid lines, and that of methods proposed in [21], [22] and [26] are illustrated by dotted lines. From the above experimental results, it can be concluded that the detection error rates against steganalytic features are increased significantly by adopting the proposed methods. This is mainly because the high coding efficiency of STC-CRC codes helps reduce the changes in cover images caused by message embedding, comparing with the previous robust steganography methods. Therefore, it can be concluded that, based on the improved robust steganography framework, the proposed methods can hold a stronger robustness against JPEG compression, and a higher detection resistance against statistical features, while enhancing both communication reliability and efficiency.

5 Conclusions

In the past few years, the multimedia technology and deep learning technology have made a tremendous progress, and brings new opportunities and challenges for covert communication. For the practical demands for communication reliability, efficiency, and security in real-time robust steganography, the STC-CRC codes, with strong error detection performance, satisfactory correction capability, and low embedding costs, is proposed in this paper. Utilizing these properties, an enhanced robust steganography framework and three steganographic methods resisting JPEG compression and detection are proposed, which reduce the bottleneck of embedding efficiency and detection resistance in existing robust steganography methods. To address the message extraction integrity of the proposed methods, by combining with the residual model of JPEG compression, the fault tolerance corresponding to each embedding domain is analyzed, and the recommended coding parameters are discussed. According to the experimental results, the proposed methods not only increase robustness against JPEG compression, but also have a higher detection resistance, thus enhancing both communication reliability and efficiency. Since the proposed method only consider the JPEG compression and detection resistance of real-time image steganographic techniques used for covert communication, in the future work, we will continue to study robust steganography with resistance against multiple image processing attacks and improve the communication security as well, thereby expanding the application scenario of image steganography techniques.

Acknowledgements This work was supported in part by the National Natural Science Foundation of China (NSFC No.U1804263, U1736214, U1636219, 61872448, 61772549, and 61602508), the National Key R&D Program (No. 2016YFB0801303, 2016QY01W0105), and the Science and Technology Innovation Talent Project of Henan Province (No. 184200510018).

References

1. M. Amini, M.O. Ahmad, and M.N.S. Swamy. 2017. A new locally optimum watermark detection using vector-based hidden markov model in wavelet domain. *Signal Processing* 137 (2017), 213–222.
2. A.G. Bors and I. Pitas. 1996. Image watermarking using DCT domain constraints. In *IEEE International Conference on Image Processing*. IEEE, 231–234.
3. T. Denemark and J. Fridrich. 2017. Steganography with two JPEGs of the same scene. In *IEEE International*

Conference on Acoustics, Speech and Signal Processing. IEEE, 2117–2121.

4. T. Filler, J. Judas, and J. Fridrich. 2011. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security* 6, 3 (2011), 920–935.
5. L. Guo, J. Ni, and Y.Q. Shi. 2012. An efficient JPEG steganographic scheme using uniform embedding. In *IEEE International Workshop on Information Forensics and Security*. IEEE, 169–174.
6. V. Holub and J. Fridrich. 2012. Designing steganographic distortion using directional filters. In *IEEE Workshop on Information Forensic and Security*. IEEE, 234–239.
7. V. Holub and J. Fridrich. 2013. Digital steganography using universal distortion function. In *ACM Workshop on Information Hiding and Multimedia Security*. ACM, 59–68.
8. Y.H. Kang, F.L. Liu, C.F. Yang, and et. al. 2019. Color image steganalysis based on residuals of channel differences. *Computers, Materials and Continua* 59, 1 (2019), 315–329.
9. P. Koopman and T. Chakravarty. 2004. Cyclic redundancy code (CRC) polynomial selection for embedded networks. In *International Conference on Dependable Systems and Networks*. IEEE, 145–154.
10. S. Parah, J. Sheikh, N. Loan, and et. al. 2016. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digital Signal Processing* 53 (2016), 11–24.
11. T. Pevný, T. Filler, and P. Bas. 2010. Using high-dimensional image models to perform highly undetectable steganography. In *ACM International Workshop on Information Hiding*. ACM, 161–177.
12. C. Qin, Z.H. He, X.Y. Luo, and et. al. 2018. Reversible data hiding in encrypted image with separable capability and high embedding capacity. *Information Sciences* 465 (2018), 285–304.
13. Z.G. Qu, T.C. Zhu, J.W. Wang, and et. al. 2018. A novel quantum stegonagraphy based on brown states. *Computers, Materials and Continua* 56, 1 (2018), 47–59.
14. V. Sedighi, R. Cogranne, and J. Fridrich. 2016. Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security* 11, 2 (2016), 221–234.
15. J. Tsai, W. Huang, and Y. Kuo. 2011. On the selection of optimal feature region set for robust digital image watermarking. *IEEE Transactions on Image Processing* 20, 3 (2011), 735–743.
16. J. Tsai, W. Huang, Y. Kuo, and et. al. 2012. Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions. *Signal Processing* 92, 6 (2012), 1431–1445.
17. J.W. Wang, L. Ting, X.Y. Luo, and et. al. 2018. Identifying computer generated images based on quaternion central moments in color quaternion wavelet domain. *IEEE Transactions on Circuits and Systems for Video Technology* (2018), 1–12.
18. G.S. Xu. 2017. Deep convolutional neural network to detect J-UNIWARD. In *ACM Workshop on Information Hiding and Multimedia Security*. ACM, 67–73.
19. J. Ye, J.Q. Ni, and Y. Yang. 2017. Deep learning hierarchical representations for image steganalysis. *IEEE Transactions on Information Forensics and Security* 12, 11 (2017), 2545–2557.
20. Y. Zhang, X.Y. Luo, C.F. Yang, and et. al. 2015. A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients. In *IEEE International Conference on Availability, Reliability and Security*. IEEE, 461–466.
21. Y. Zhang, X.Y. Luo, C.F. Yang, and et. al. 2016. A framework of adaptive steganography resisting JPEG compression and detection. *Security and Communication Networks* 9, 15 (2016), 2957–2971.
22. Y. Zhang, X.Y. Luo, C.F. Yang, and et. al. 2017. Joint JPEG compression and detection resistant performance enhancement for adaptive steganography using feature regions selection. *Multimedia Tools and Applications* 76, 3 (2017), 3649–3668.
23. Y. Zhang, C. Qin, W.M. Zhang, and et. al. 2018. On the fault-tolerant performance for a class of robust image steganography. *Signal Processing* 146 (2018), 99–111.
24. Y. Zhang, D.P. Ye, J.J. Gan, and et. al. 2018. An image steganography algorithm based on quantization index modulation resisting scaling attacksand statistical detection. *Computers, Materials and Continua* 55, 1 (2018), 59–70.
25. Y.W. Zhang, W.M. Zhang, K.J. Chen, and et. al. 2018. Adversarial Examples Against Deep Neural Network based Steganalysis. In *Acm Workshop on Information Hiding and Multimedia Security*. ACM, 67–72.
26. Y. Zhang, X.D. Zhu, C. Qin, and et. al. 2018. Dither modulation based adaptive steganography resisting JPEG compression and statistic detection. *Multimedia Tools and Applications* 77, 14 (2018), 17913–17935.
27. Z.L. Zhou, M. Yan, and Q.M.J. Wu. 2018. Coverless image steganography using partial-duplicate image retrieval. *Soft Computing* 2 (2018), 1–12.