Computers and Electrical Engineering 000 (2017) 1–10

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Medical JPEG image steganography based on preserving inter-block dependencies☆

Xin Liao[a], Jiaojiao Yin[a], Sujing Guo[a], Xiong Li[b,*], Arun Kumar Sangaiah[c]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[c] School of Computer science and Engineering, VIT University, Vellore 632014, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 13 February 2017
Revised 21 August 2017
Accepted 21 August 2017
Available online xxx

Keywords:
Medical JPEG image
Image steganography
DCT Coefficients
Inter-block dependencies

ABSTRACT

With the development of computer and biomedical technologies, medical JPEG images contain the patients' personal information and the security of the private information attracts great attention. Steganography is utilized to conceal the private information, so as to provide privacy protection of medical images. Most of existing JPEG steganographic schemes embed messages by modifying discrete cosine transform (DCT) coefficients, but the dependencies among DCT coefficients would be disrupted. In this paper, we propose a new medical JPEG image steganographic scheme based on the dependencies of inter-block coefficients. The basic strategy is to preserve the differences among DCT coefficients at the same position in adjacent DCT blocks as much as possible. The cost values are allocated dynamically according to the modifications of inter-block neighbors in the embedding process. Experimental results show that the proposed scheme can cluster the inter-block embedding changes and perform better than the state-of-the-art steganographic method.

1. Introduction

With the rapid reform and development of the biomedical system, digital medical images have become increasingly important in recent years [1]. Medical images can be transmitted conveniently through the networks for the purposes of research, education, and consultations. Since medical images contain the patients' personal information, information security and privacy protection have become greatly significant during transmitting medical images over the Internet [2–4]. Therefore, steganography is introduced to provide protection and confidentiality for medical images, and it could make the patients' information undetectable [5,6].

Bremnavas et al. [7] presented a new steganographic method to hide the patient's information into medical images. The information is embedded by the least significant bit (LSB) method, and then the medical image is encrypted using chaos algorithms. Pandey et al. [8] combined image cryptography and steganography techniques for the secure transmission of medical images. The medical image is first encrypted and then embedded with the patients' information. There are some steganographic schemes for the encrypted medical images. Qin et al. [9] proposed an inpainting-assisted reversible steganographic scheme using histogram shifting mechanism. They designed an effective reversible steganographic scheme for the

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. R. C. Poonia.

* Corresponding author.
E-mail address: lixiongzhq@163.com (X. Li).

http://dx.doi.org/10.1016/j.compeleceng.2017.08.020

privacy protection of medical image content [10]. Liao et al. investigated reversible data hiding in encrypted medical images based on the absolute mean difference of multiple neighboring pixels [11].

Recently, the JPEG format has been increasingly adopted for medical image storage and transmission, since it can achieve not only higher compression rate but also good visual quality. Hence, JPEG image steganography can be utilized to embed the patients' personal information into medical JEPG images. Researchers have made much helpful progress on JPEG image steganography. A classic method called F5 was proposed by A. Westfeld [12]. It only embeds messages into the non-zero alternating current (AC) DCT coefficients, but introduced the shrinkage effect if a coefficient becomes zero after embedding. Non-shrinkage F5 [13], an improved version of F5, assigned infinite costs to some DCT coefficients, and thus alleviated the negative effect. Guo et al. [14] spread the embedding modification to each DCT coefficient evenly and designed a cost function for homogeneous embedding according to the principles of the spread spectrum communication. Huang et al. [15] presented a new channel selection rule for JPEG image steganography, aiming to find the DCT coefficients that may introduce minimal detectable distortion. Wang et al. [16] proposed an efficient JPEG steganography scheme based on the block entropy of DCT coefficients and syndrome trellis coding (STC) [17]. In 2013, Huang et al. [18] divided DCT coefficients into two portions and assigned different weights for them, and designed the cost function based on the quantization step, quantified coefficients and quantitative disturbance error. Filler et al. [19] constructed the cost function and JPEG image steganographic scheme by designing and optimizing a multi-parameter model with specific statistical features. Lately, they proposed JPEG universal wavelet relative distortion (J-UNIWARD) [20] which evaluates the embedding costs of DCT coefficients in the spatial domain by using inverse DCT, and implements the embedding operations in JPEG domain. Wang et. al [21] exploited block fluctuation and quantization steps to design a hybrid distortion function for JPEG image steganography.

In a JPEG image, DCT coefficients exhibit two kinds of complex dependencies, intra-block dependencies, and inter-block dependencies. Intra-block dependencies refer to the relationship among coefficients with similar frequency in the same block, while inter-block dependencies describe the relationship among coefficients at the corresponding positions in different DCT blocks. However, the existing JPEG image steganographic schemes might destroy the inter-block dependencies. As a modern JEPG image steganalysis approach, the union of JPEG and spatial rich model (JSRM) [22] could detect the data hiding traces according to the dependencies of DCT coefficients. Thus, the security performance of JPEG image steganographic schemes could be improved by preserving the inter-block dependencies.

In 2015, clustering modification directions (CMD) strategy [23] was presented, which mainly focused on preserving the correlation between neighboring pixels in the spatial domain. Consequently, it can synchronize the modification directions, and enhance the performance evaluated by the powerful spatial image steganalysis. In this paper, inspired by CMD, we propose an adaptive JPEG image steganographic scheme, and it preserves the correlation among inter-block adjacent coefficients by adjusting cost values in the embedding process. The initial cost values of all coefficients are firstly computed by one of the existing distortion functions. The original JPEG image is divided into several non-overlapping sub-images, ensuring that the neighboring DCT coefficient blocks belong to different sub-images. For a given DCT coefficient, it has four corresponding points at the same locations in the four adjacent DCT blocks (we name them inter-block neighbors). The cost value of each coefficient would be dynamically adjusted in accordance with the modifications of its neighbors. Experimental results show that the proposed scheme performs better than J-UNIWARD in resisting the modern JPEG image steganalysis.

The rest of the paper is organized as follows. A strategy for preserving inter-block dependencies is introduced in Section 2. In Section 3, we describe the proposed JPEG image steganographic scheme in details. The comparative experiments are presented in Section 4. Finally, the conclusion is given in Section 5.

2. The strategy for preserving inter-block dependencies

JPEG image steganographic schemes usually hide information into an image by adding or subtracting the values of DCT coefficients. In the ternary embedding framework, the coefficients might be modified by plus one or minus one. From the perspective of steganalysis, modern steganalytic methods always detect the data hiding traces by capturing the fluctuations. When inter-block dependencies remain unchanged, the fluctuations might be reduced.

In order to maintain the inter-block dependencies, the embedding impacts of inter-block neighboring coefficients should be considered while assigning cost values, i.e., the modifications of coefficients should be consistent with its inter-block neighbors. Thus, cost values might not be assigned simultaneously, and the positive modification and negative modification might be different.

According to the above analysis, a strategy is designed for preserving the inter-block dependencies as below. JPEG image is primarily divided into several sub-images, and the messages are also decomposed into several portions accordingly. Each information segmentation is embedded into the corresponding sub-image. The initial cost values of DCT coefficients are calculated by one of the existing cost functions. The first sub-image is embedded based on the initial cost values. The cost values of coefficients in the other sub-images will be updated according to the modifications of inter-block neighbors. The mutual embedding impacts of DCT coefficients are taken into account in the process of assigning cost values to maintain the difference of inter-block neighbors unchanged as much as possible. Since the initial cost values can be computed by any of the existing cost functions, the proposed strategy can be flexibly implemented together with the state-of-art JPEG image steganographic methods.

The main idea of the proposed strategy is expressed as Fig. 1. For a $M \times N$ JPEG image, it is composed of $M \times N/64$ DCT blocks obtained by DCT transform. The size of each DCT block is 8×8, and each DCT block includes 64 quantized

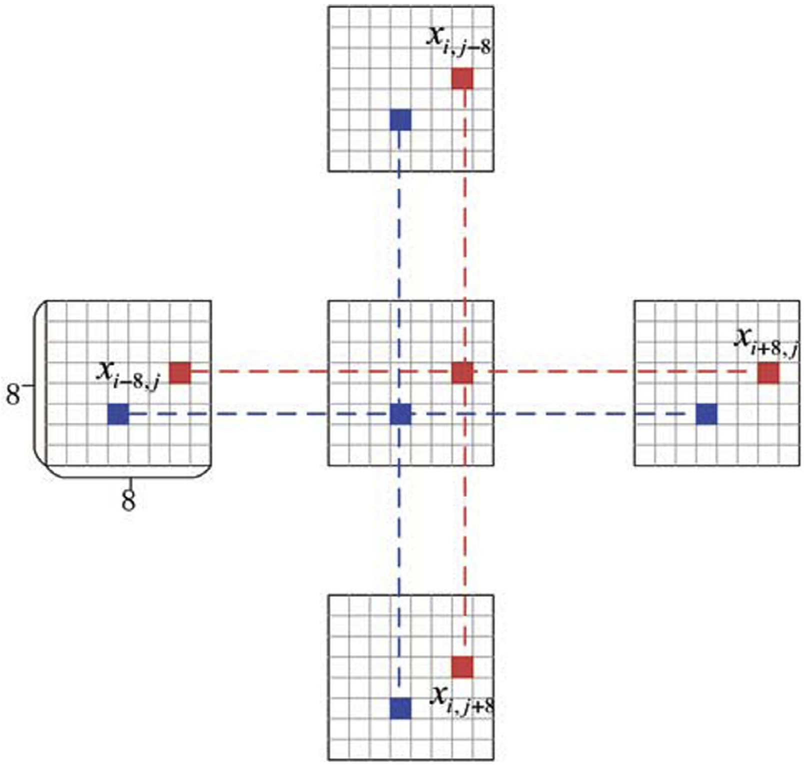


Fig. 1. The main idea of the proposed strategy.

DCT coefficients. The upper case bold symbol **X** denotes the cover JPEG image after operating DCT transform, and the low case $x_{i,j}$ represents the individual DCT coefficient, where i and j indicate the location in the cover JPEG image block. Stego image is represented by a matrix $\mathbf{Y} = \{y_{i,j}\}^{M\times N}$. For a given DCT coefficient $x_{i,j}$, the inter-block neighbors of $x_{i,j}$ are $Z_{inter} = \{x_{i+8,j}, x_{i-8,j}, x_{i,j+8}, x_{i,j-8}\}$, i.e., a set of the coefficients at the same position in the adjacent four blocks of $x_{i,j}$. The modification direction of $x_{i,j}$ should be consistent with the most elements in Z_{inter}, which can be expressed by

$$\begin{cases} P(x_{i,j}+1) > P(x_{i,j}-1), if \mathcal{N}\{x+1|x\in Z_{inter}\} > \mathcal{N}\{x-1|x\in Z_{inter}\} \\ P(x_{i,j}+1) < P(x_{i,j}-1), if \mathcal{N}\{x+1|x\in Z_{inter}\} < \mathcal{N}\{x-1|x\in Z_{inter}\} \end{cases} \tag{1}$$

where $P(\bullet)$ represents the modification probability and $\mathcal{N}\{W\}$ denotes the number of elements in set W.

3. A Novel JPEG Image steganographic scheme based on preserving inter-block dependencies

3.1. The proposed image JPEG steganographic scheme

In this subsection, a novel adaptive JPEG image steganographic scheme based on preserving inter-block dependencies is proposed. The most important operation is the process of updating the cost values. The cost values assignment fully explores the mutual embedding impacts of inter-block coefficients. The detailed steps of embedding and extracting algorithms are as follows.

3.1.1. Embedding algorithm

Step 1: Divide the cover JPEG image into four non-overlapping sub-images on the basis of 8×8 blocks, ensuring that the adjacent two DCT blocks belong to different sub-images. Define the sub-images as S_t $(t = 1, 2, 3, 4)$ via the zig-zag scan. The process of dividing the cover image into sub-images is shown in Fig. 2.

Step 2: Obtain the numbers of non-zero AC coefficients (nzAC) of each sub-image n_t $(t = 1, 2, 3, 4)$. Then calculate the proportion p_t $(t = 1, 2, 3, 4)$ by the following equation.

$$p_t = \frac{n_t}{\sum_{i=1}^{4} n_i} \tag{2}$$

Given a piece of messages with the length of m, divide the messages into four portions I_t $(t = 1, 2, 3, 4)$ with the length of $p_t \times m$.

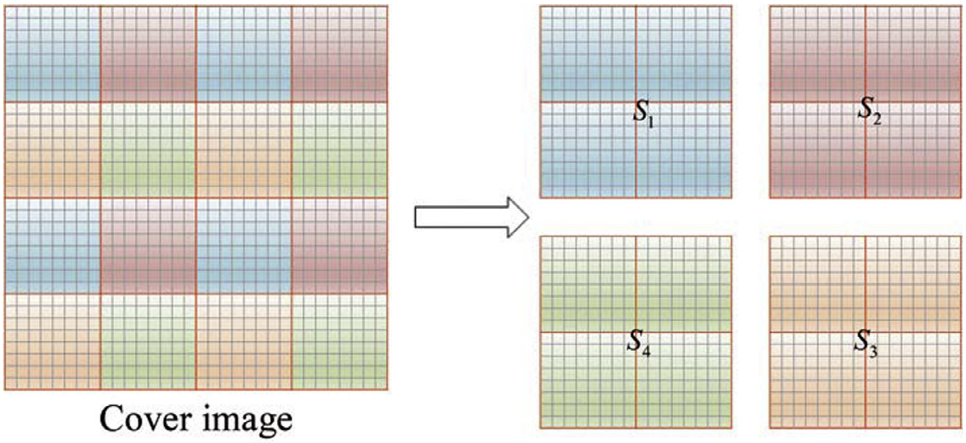


Fig. 2. The process of dividing the cover image into sub-images.

Step 3: Calculate the initial cost value matrix C of all DCT coefficients by applying cost functions. In this paper, the initial cost value matrix $C = (c_{i,j})^{M\times N}$ is computed by the cost function in J-UNIWARD as below.

$$C = (c_{i,j})^{M\times N} = \sum_{k=1}^{3}\sum_{u=1}^{M}\sum_{v=1}^{N} \frac{\left|W_{uv}^{(k)}(\Gamma(\mathbf{X})) - W_{uv}^{(k)}(\Gamma(\mathbf{Y}))\right|}{\sigma + \left|W_{uv}^{(k)}(\Gamma(\mathbf{X}))\right|} \tag{3}$$

where the symbol $\Gamma(\cdot)$ represents the operation of decompressing the JPEG images $\mathbf{X}$ and $\mathbf{Y}$ to the spatial domain. $W_{uv}^{(k)}(\Gamma(\mathbf{X}))$ and $W_{uv}^{(k)}(\Gamma(\mathbf{Y}))$ represent the corresponding uv-th wavelet coefficient of the JPEG and stego image in the k-th sub-band of the first decomposition level. $\sigma > 0$ is a quantity to stabilize the numerical calculations.

Step 4: Let the stego image $\mathbf{Y} = \mathbf{X}$ when $t = 1$.

Step 5: Compute the embedding modification D between $\mathbf{X}$ and $\mathbf{Y}$.

$$D = \mathbf{X} - \mathbf{Y} = (d_{i,j})^{M\times N} \tag{4}$$

Step 6: We define ρ^+ and ρ^- as the cost values of positive modification and negative modification respectively. If $t = 1$, $\rho^+_{i,j} = \rho^-_{i,j} = c_{i,j}$. Otherwise, ρ^+ and ρ^- should be adjusted as follows.

$$\rho^+_{i,j} = c_{i,j}/\alpha \quad if \quad N^+_{i,j} > N^-_{i,j} \tag{5}$$

$$\rho^-_{i,j} = c_{i,j}/\alpha \quad if \quad N^+_{i,j} < N^-_{i,j} \tag{6}$$

where $\alpha > 1$ is an adjusting parameter. The related analyses about α are shown in Section 4.1. For a DCT coefficient $x_{i,j}$, $N^+_{i,j}$ and $N^-_{i,j}$ are the numbers of coefficients which add one and subtract one in the inter-block neighbors Z_{inter}, respectively.

Step 7: Combining with the cost value $\rho = \{\rho^+, \rho^-\}$, we can utilize STC to embed the sub-messages I_t into the sub-image S_t. Update the stego JPEG image $\mathbf{Y}$.

Step 8: Repeat the algorithm from Step 5 until all sub-images are embedded.

3.1.2. Extracting algorithm

The receiver can extract messages without the original JPEG image. The stego image is divided into sub-images, and the receiver extracts sub-message from each sub-image and combines all sub-messages. The detailed steps are as follows.

Step 1: Divide the stego JPEG image $\mathbf{Y}$ into four non-overlapping sub-images on the basis of 8×8 blocks as the step 1 in the embedding algorithm. Denote the sub-images as Y_t $(t = 1, 2, 3, 4)$ via the zig-zag scan.

Step 2: Extract sub-message I_t from each sub-image Y_t by using the STC decoding approach.

Step 3: According to the order of embedding operations, combine all sub-messages I_t $(t = 1, 2, 3, 4)$ to obtain the entire messages m.

3.2. Discussions

The key of the proposed scheme is to maintain the difference of the neighboring coefficients, and it is realized by adjusting the cost values dynamically. The cover JPEG image is divided into several sub-images, and adjacent DCT coefficients are in different sub-images, so that the mutual embedding impacts can be considered. For each coefficient, the cost values of positive modification and negative modification are distinguished as $\rho^+_{i,j}$ and $\rho^-_{i,j}$. Both of them are equal to the initial

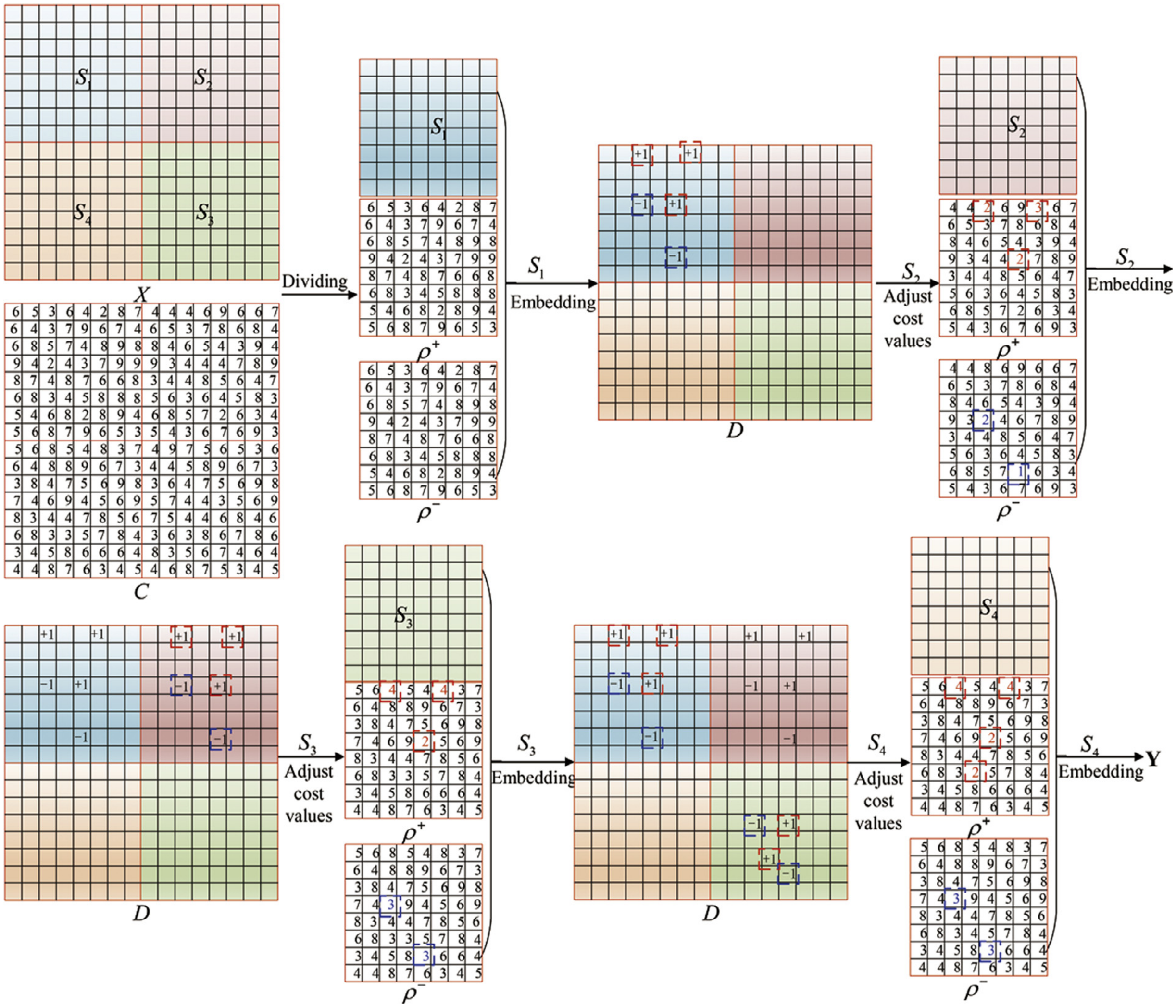


Fig. 3. A simple example of the proposed JPEG image stegaographic scheme.

cost value of the coefficient $x_{i,j}$ in the first sub-image. For the other sub-images, ρ^+ and ρ^- of DCT coefficients are adjusted according to the modifications of inter-block neighbors. If $N^+_{i,j}$ is greater than $N^-_{i,j}$, the coefficient should add one as possible and thus its cost value $\rho^+_{i,j}$ would be decreased. If $N^-_{i,j}$ is greater, the cost value $\rho^-_{i,j}$ should be decreased synchronously. Therefore, the inter-block dependencies can be preserved.

Suppose the cover JPEG image **X** consists of four DCT coefficients blocks, a simple example of the proposed scheme is shown in Fig. 3. The initial cost value C of the cover image can be computed, and the cover image is divided into four sub-images S_1, S_2, S_3, S_4. We first embed sub-messages into sub-image S_1 based on its cost values ρ^+, ρ^- that are equal to the initial cost value. We obtain the embedding modification D between **X** and **Y**. Then we adjust the cost values ρ^+, ρ^- of sub-image S_2 according to the embedding modification D, and then embed sub-messages. We iteratively process sub-images S_3 and S_4 in the same step of S_2.

4. Experimental results

In this section, some experimental results and analyses are presented to demonstrate the effectiveness of the proposed scheme. In Section 4.1, some experiments are performed to determine the adjusting parameter α. The complexity analysis is presented in section 4.2. Section 4.3 illustrates the visualizing embedding changes of the proposed scheme, and verifies that the proposed scheme could effectively cluster embedding changes and preserve the inter-block dependencies. The experimental results in section 4.4 show that the proposed scheme could obtain better performance than the previous J-UNIWARD method, against the modern JPEG image steganalysis.

Table 1
The anti-steganalysis performance of the proposed scheme with different values of the adjusting parameter α.

Parameter α	2	3	4	5	6
Performances	0.1952	0.1928	0.1896	0.1897	0.1889

Table 2
The comparative clustering effects between J-UNIWARD and the proposed scheme. Here nzAC denotes the number of non-zero AC, ECR denotes the embedding change rates, CEC denotes the clustering embedding changes, and CR denotes the clustering rates.

Algorithm	Testing image	nzAC	ECR	CEC	CR
J-UNIWARD	(a)	18,115	0.0913	145	8.7%
	(b)	13,786	0.0851	99	8.4%
	(c)	16,688	0.0929	135	8.7%
	(d)	14,083	0.09	126	9.9%
	(e)	14,062	0.0915	118	9.1%
	(f)	15,358	0.0979	134	8.9%
The proposed scheme	(a)	18,115	0.1025	201	10.8%
	(b)	13,786	0.0950	137	10.5%
	(c)	16,688	0.0963	182	11.3%
	(d)	14,083	0.0906	149	11.6%
	(e)	14,062	0.0969	146	10.7%
	(f)	15,358	0.0985	169	11.2%

4.1. Impact of the adjusting parameter α

The evaluation of the adjusting parameter α is greatly important in the proposed scheme. The value of α might affect the embedding locations and the embedding change rate, and thus might result in different performances.

We test the anti-steganalysis performances under different α with respect to JRM steganalyzer. The testing image database is Break Our Steganographic System (BOSS) [24], which consists of 10,000 original gray-scale images. All the images are compressed with the quality factor 75. We set the embedding payload to 0.4 bits per non-zero AC coefficient (bpnzAC), and a piece of pseudo random messages are embedded into the JPEG images by the proposed scheme with different values of the adjusting parameter α. Table 1 presents the comparative results. The results illustrate that the anti-steganalysis performance of $\alpha = 2$ is better. Therefore, we set $\alpha = 2$ in the following experiments.

4.2. Complexity analysis

In the proposed scheme, we first compute the initial cost value for each DCT coefficient in JPEG image. The JPEG image is divided into four sub-images. We adjust the cost values dynamically and embed messages into each sub-image. Therefore, the computational cost mainly spends on the computing initial cost value, adjusting the cost value and embedding. We compute the initial cost value and adjust the cost value for each DCT coefficient. The computation complexities of the first two operations are $O(M \times N)$, where $M \times N$ is the size of JPEG images. As for embedding, different algorithms have distant computational complexities. In our proposed scheme, STC which consumes more time is utilized to obtain higher security performance.

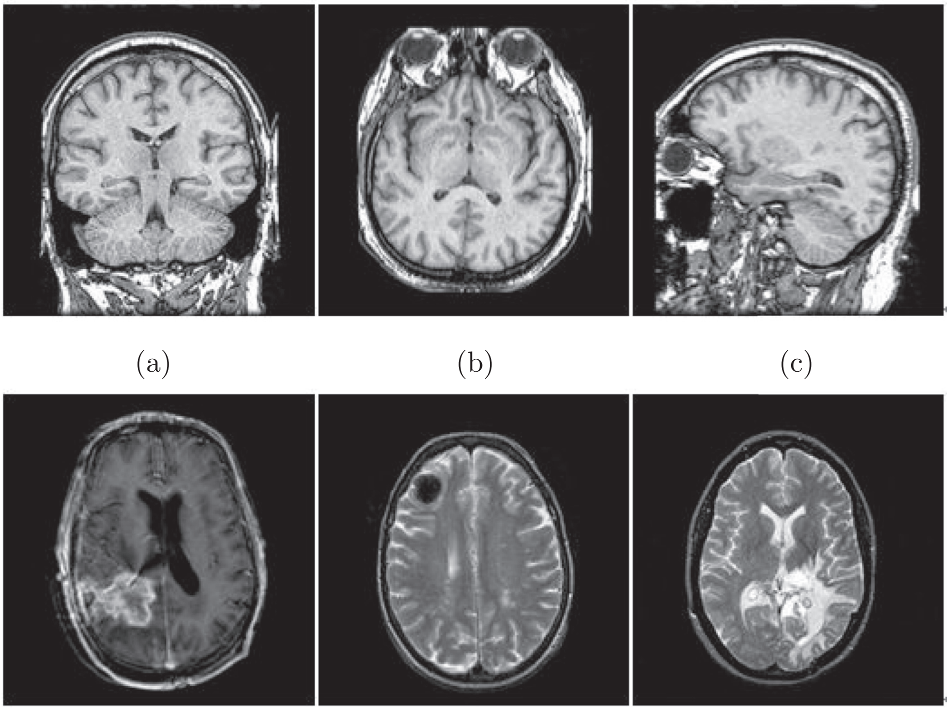
4.3. Illustration of the embedding changes

To verify whether the proposed scheme can effectively cluster the inter-block embedding changes, we utilize six brain magnetic resonance imaging (MRI) images shown as Fig. 4, to illustrate the embedding changes.

We embed messages into the six brain MRI images with the embedding payload 0.4 bpnzAC. The stego images are shown in Fig. 5. It can be observed that the human visual system (HVS) could not perceive the existence of hiding messages from stego images. Thus, the proposed scheme can provide the patients' personal information imperceptibly.

In order to further illustrate the clustering effects among the inter-blocks, we compare the clustering rates (CR) in the six brain MRI stego images obtained by using J-UNIWARD and the proposed scheme. We count the number of the modified nzAC, and then compute the embedding change rates (ECR). The numbers of the clustering embedding changes (CEC) are calculated, and thus the CR is obtained by the following equation.

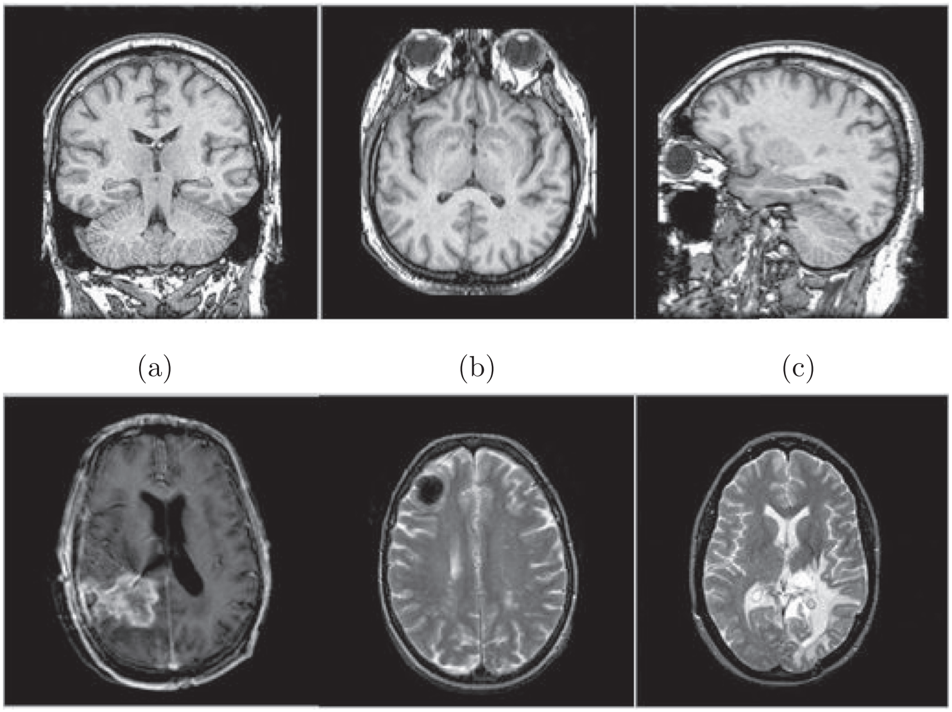
$$\mathrm{CR} = \frac{\mathrm{CEC}}{\mathrm{nzAc} * \mathrm{ECR}} \tag{7}$$



(a) (b) (c)

(d) (e) (g)

Fig. 4. Six brain MRI cover images.



(a) (b) (c)

(d) (e) (f)

Fig. 5. Six brain MRI stego images obtained by the proposed scheme with the payload 0.4 bpnzAC.

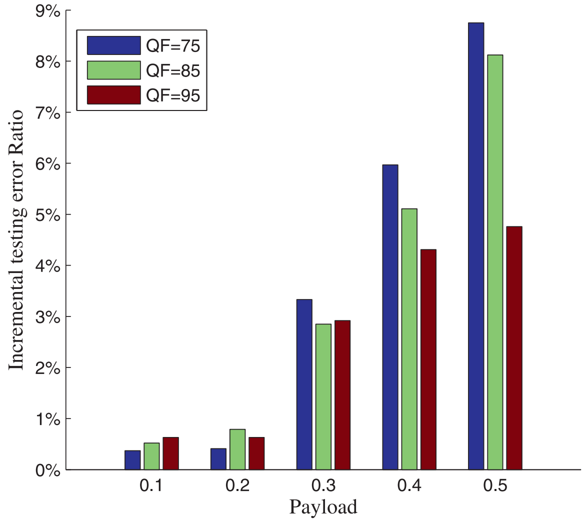


Fig. 6. Comparisons of detection errors *Eoob* based on the BOSS image set with quality factors 75, 85, 95 against JSRM steganalysis. The X-axis presents the embedding payloads, and the Y-axis presents the incremental E_{oob} ratio (by percentage) obtained by the proposed scheme upon J-UNIWARD.

The numerical results are shown in Table 2. It can be observed that the clustering rates of our proposed scheme are higher than that of J-UNIWARD. Therefore, the proposed scheme is able to cluster the inter-block embedding changes, so as to preserve the inter-block dependencies.

4.4. Comparisons of anti-steganalysis performance

This subsection mainly compares the security performance of the proposed scheme and J-UNIWARD resisting the modern steganalytic method.

The testing images are 10,000 original gray-scale images with the size of 512×512 from the BOSS image set. All the images are compressed with three quality factors 75, 85, 95, respectively. The proposed scheme and J-UNIWARD respectively embed messages into JPEG images with five embedding payloads 0.1, 0.2, 0.3, 0.4, 0.5 bpnzAC. We use JSRM to evaluate the anti-steganalysis performance. In JSRM steganalyzer, 35263-dimensional features are used for feature extraction, and the ensemble classifier [25] is applied in training and testing stages. The security performance is quantified by using the ensemble's "out-of-bag" error (E_{oob}), which is an unbiased estimate of the minimal total testing error under equal priors. The greater E_{oob} is, the higher security performance is.

For different quality factors, the comparisons of detection errors E_{oob} of the proposed scheme and J-UNIWARD are presented in Fig. 6. The X-axis presents different embedding payloads, and the Y-axis presents the incremental E_{oob} ratio (by percentage) obtained by the proposed scheme upon J-UNIWARD. For each embedding payload, the incremental E_{oob} ratio is computed as

$$E_{oob}\ ratio = \frac{E_{oob_{ours}} - E_{oob_{J-UNIWARD}}}{E_{oob_{J-UNIWARD}}} * 100\% \qquad (8)$$

where $E_{oob_{ours}}$ is the E_{oob} value of ours proposed scheme, and $E_{oob_{J-UNIWARD}}$ is the E_{oob} value of J-UNIWARD. For example, when the quality factor is 75 and the payload rate is 0.4 bpnzAC, the E_{oob} value of J-UNIWARD is 0.184, and E_{oob} value of the proposed scheme is 0.195. Thus, the proposed scheme could improve the corresponding detection error by about 5.97%. From Fig. 6, it can be observed that the proposed scheme could perform better than J-UNIWARD resisting JSRM.

5. Conclusion

Nowadays, the need for sharing medical images is growing rapidly, and advanced medical information system is changing the way that medical images are stored, accessed and distributed. A large amount of patients' personal information is included in medical JPEG images. Thus, the privacy protection of medical JEPG images has become an important issue. Steganography is a useful tool to conceal patients' information in the medical images. Most of existing JPEG image steganographic schemes might destroy the inter-block dependencies of DCT coefficients, and thus the security performance is not satisfied yet. In this paper, we first investigate an adaptive strategy that synchronizes the modification directions for the same position of adjacent DCT blocks, and then the cost values are adjusted dynamically according to the modifications of inter-block neighbors in the embedding process. A novel medical JPEG image steganographic scheme is designed based on

Please cite this article as: X. Liao et al., Medical JPEG image steganography based on preserving inter-block dependencies, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.08.020

preserving the dependencies of inter-block DCT coefficients. Comparative experiments show that the proposed scheme can effectively cluster the inter-block embedding changes, and obtain better anti-steganalysis performance.

Acknowledgments

This work is supported by National Natural Science Foundation of China (Grant Nos. 61402162, 61572182, 61370225, 61472131, 61272546, 61300220), the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 16B089), Hunan Provincial Natural Science Foundation of China (Grant No. 2017JJ3040), Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security(Grant No. AGK201605), CCF-Venustech Research Fund, Science and Technology Key Projects of Hunan Province (Nos. 2015TP1004, 2016JC2012).

References

[1] Li M, Poovendrana R, Narayanan S. Protecting patient privacy against unauthorized release of medical images in a group communication environment. Comput Med Imaging Graph 2005;29:367–83.
[2] Nyeem H, Boles W, Boyd C. A review of medical image watermarking requirements for teleradiology. J Digit Imaging 2013;26:323–43.
[3] Li X, Niu J, Khan MK, Liao J. An enhanced smart card based remote user password authentication scheme. J Network Comput Appl 2013;36(5):1365–71.
[4] Li X, Ma J, Wang W, Xiong Y, Zhang J. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Math Comput Model 2013;58(1):85–95.
[5] Cheddad A, Condell J, Curran K, Kevitt PM. Digital image steganography: survey and analysis of current methods. Signal Process 2010;90:727–52.
[6] Liao X, Qin Z, Ding L. Data embedding in digital images using critical functions. Signal Process Image Commun 2017;58:146–56.
[7] Bremnavas I, Poorna B, Kanagachidambaresan G. Medical image security using LSB and chaotic logistic map. In: IEEE conference on advances in recent technologies in communication and computing; 2011. p. 229–31.
[8] Pandey V, Shrivastava M. Medical image protection using steganography by crypto-image as cover image. Int J Adv Comput Res 2012;2(5):45–8.
[9] Qin C, Chang CC, Huang YH, Liao LT. An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. IEEE Trans Circuits Syst Video Technol 2013;23(7):1109–18.
[10] Qin C, Zhang X. Effective reversible data hiding in encrypted image with privacy protection for image content. J Vis Commun Image Represent 2015;31:154–64.
[11] Liao X, Shu C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J Vis Commun Image Represent 2015;28:21–7.
[12] Westfeld A. F5-A steganographic algorithm: high capacity despite better steganalysis. In: Springer international workshop on information hiding; 2001. p. 289–302.
[13] Fridrich J, Pevný T, Kodovský J. Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities. In: ACM workshop on multimedia and security; 2007. p. 3–14.
[14] Guo L, Ni J, Shi YQ. An efficient JPEG steganographic scheme using uniform embedding. In: IEEE international workshop on information forensics and security; 2012. p. 169–74.
[15] Huang F, Huang J, Shi YQ. New channel selection rule for JPEG steganography. IEEE Trans Inf Forensics Secur 2012;7(4):1181–91.
[16] Wang C, Ni J. An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients. In: IEEE international conference on acoustics, speech and signal processing; 2012. p. 1785–8.
[17] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans Inf Forensics Secur 2011;6(3):920–35.
[18] Huang F, Luo W, Huang J. Distortion function designing for JPEG steganography with uncompressed side-image. In: ACM workshop on information hiding and multimedia security; 2013. p. 69–76.
[19] Filler T, Fridrich J. Design of adaptive steganographic schemes for digital images. In: SPIE, electronic imaging, media watermarking, security, and forensics XIII; 2011. p. 181–97.
[20] Holub V, Fridrich J, Denemark T. Digital image steganography using universal distortion. In: SPIE, electronic imaging, media watermarking, security, and Forensics XIII; 2013. p. 59–68.
[21] Wang Z, Zhang X, Yin Z. Hybrid distortion function for JPEG steganography. J Electron Imaging 2016;25(5):050501.
[22] Kodovský J, Fridrich J. Steganalysis of JPEG images using rich models; 2012. p. 83030.
[23] Li B, Wang M, Li X, Tan S, Huang J. A strategy of clustering modification directions in spatial image steganography. IEEE Trans Inf Forensics Secur 2015;10:1905–17.
[24] Bas P, Filler T, Pevný T. Break our steganographic system the ins and outs of organizing boss. In: ACM workshop on information hiding and multimedia security; 2011. p. 59–70.
[25] Bas P, Filler T, Pevný T. Ensemble classifiers for steganalysis of digital media. IEEE Trans Inf Forensics Secur 2012;7:432–44.

Xin Liao received the B.E. degree and Ph.D. degree in information security from Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2012, respectively. He is currently an associate professor with Hunan University, China, where he joined in 2012. His research interests include steganography, watermarking, and multimedia forensic.

Jiaojiao Yin received the Bachelors degree in engineering from Henan Normal University of China, Henan, China. Currently, she is pursuing the Masters degree in College of Computer Science and Electronic Engineering, Hunan University, China. Her research interests include steganography and image processing.

Sujing Guo received the Bachelors degree in College of Computer Science and Electronic Engineering, Hunan University, China. Her research interests include steganography and image processing.

Xiong Li received his Ph.D. degree from Beijing University of Posts and Telecommunications, China, in 2012. He is currently an associate professor at Hunan University of Science and Technology, China. He has published more than 60 referred journal papers in the area of cryptography and information security, and won JNCA 2015 Best Paper Award.

Arun Kumar Sangaiah received his Ph.D. degree in Computer Science and Engineering from the VIT University, India. He is presently working as an associate professor in School of Computer Science and Engineering, VIT University, India. His research interests include software engineering, computational intelligence, wireless networks, bioinformatics, and embedded systems.