Journal of Computers Vol. 29 No. 2, 2018, pp. 241-248
doi:10.3966/199115992018042902023

A Novel Message Decomposing and Embedding Scheme for Image Steganography

Zhihai Zhuo[1*], Ning Zhong[2], Hongxia Miao[3]

[1] Schools of Information and Communication Engineering, Beijing Information Science and Technology University, Being, China
zhuozhihai@bistu.edu.cn

[2] Computer Science Teaching and Application Center, China Youth University of Political Studies, Beijing, China
zhnbit@126.com

[3] School of Mathematics and Statistics, Beijing Institute of Technology, Beijing, China
761221369@qq.com

Received 24 July 2017; Revised 19 September 2017; Accepted 19 October 2017

Abstract. In modern society, information security is becoming more and more important. There three useful methods to protect message, names watermarking, encryption, steganography with their own characteristics. Steganography aims at hiding secret message in a cover while has little influence on the cover, plays a more and more significant role. Many steganography algorithms have been proposed in different domains including time and transform domains. Most of the steganographia methods are based on binaryzation of the secret message, while a binary sequence is longer than a ternary sequence of a same decimal number. In this paper, in order to represent the secret message with a sequence less than its binaryzation, we propose a new method to map the secret message into two binary sequences and a ternary sequence. We propose a 'ternary JSteg' method to embed the ternary sequence, which can keep the histogram characters. Indeed, simulations show our method has less influence on the cover and has other advantages.

Keywords: information hidden, information security, steganography, ternary Jsteg

1 Introduction

Internet, as a representative of modern technology and even the innovation of education, has totally changed our daily life. Most of our communication tools are smart phones and computers, which make information exchanging conveniently and leakage of information easily. As a result, information security becomes a focus point. There are three methods to protect the message-encryption, watermarking and steganography and every method having its own advantages and disadvantages. Encryption is the most ancient and obvious method, while watermarking and steganography need a host and more secure than encryption. As the most popular information hiding method, steganography is the science and art of communication where the sender embed secret message in a cover (video, image) and achieve the least possible to be detected. There is a better method to protect message during communicating, that is encrypt the secret message before embedding it into the cover.

Joint Photographic Experts Group (JPEG) is the most widely used form of pictures [1-3] through the internet, because it can be produced by digital cam- eras, scanners and other photographic image capture devices [1-5, 10]. Therefore, many steganography algorithms based non-zero alternate current (AC) discrete cosine transform (DCT) coefficients of JPEG pictures are proposed. There exist many message

* Corresponding Author

hiding methods [4, 6-12]. JSteg [10, 13] is the fundamental and easy method in JPEG steganography, Later F5 [14] improved the JSteg. Recently, Jessica. F [15-17] has proposed many content adaptive steganography methods in JPEG domain. least significant bit (LSB) is a classical but efficient method for information embedding, which encourage us to aimed at using the main idea of JSteg that is replace the LSB of cover according to secret message to propose a new steganography method. Our new method is as simple as JSteg but can solve the pairs of value phenomenon [10].

The cores of steganography are the method of dealing with the secret message and the algorithm of embedding processed message. When processing secret message, most people transform it into binary and then they process the binary sequence by running length coding, bit plane coding, gray coding or Huffman encoding method the to make the message shorter and more secure [18]. Chen [19] proposed a new method to deal with the secret message. Original message is represented by three parts, following the three parts are embedded into HL, LH, HH of DWT separately, where the processed sequences are longer than binary message. As we all known, ternary sequence is shorter than binary sequence for the same decimal number. To replace the binary sequence with its ternary form, we need to find an efficient ternary embedding method. For steganography algorithm, there are many algorithms in both time and trans- form domain. To calculate easily by computer, most algorithms are based on binary. Vasily Sachnev [20] proposed a ternary data hiding technique for JPEG steganography. They prove their ternary method has better data hiding performance than MME (modified matrix coding) method based on binary. But its capacity is lower than binary methods.

Shorter embedding sequence means less modification of the cover image. In this paper, we recombination the binary message into three parts to get a shorter but safer sequence by using a reasonable mapping table, and one of the parts is ternary. To embed the ternary sequence, we propose a new ternary embedding method, it can be terrified straightforward and have higher embed capacity. For the two binary sequences, we just use the exist efficient steganopgraphy method. The rest of this paper is organized as follows. Section 2 introduces the related knowledge. Section 3 shows the encoder and decoder in detail. Some simulations and results are shown in Section 4, Finally in section 5, we conclude this paper.

2 Preliminaries

2.1 JSteg

JSteg proposed by D. Upham is one of the classical steganography algorithms based on JPEG pictures. Its main ideas are

(1) transforming the gray scale image into 8 × 8 DCT domain by block DCT transform.

(2) quantizing the DCT coefficients.

(3) embedding secret information into the non-zero quantized DCT coefficients by successively replacing the LSBs of them with secret message bits in a zigzag order.

The advantages of JSteg are easy, high-capacity and straightforward. At the same time, the most obvious disadvantage is pairs of value in DCT histogram.

2.2 Ternary LSB

Just like the binary LSB used widely [19], any positive integer can be represented in the form of ternary. For instance, the ternary of 255 is 100110, and its LSB is 0. Here, we define the LSB of a negative integer as the LSB of its absolute value. The weighting configuration of a 6-bit number is illustrated in Table 1.

Table 1. Weighting of a 6-bit number

MSB			⇔		LSB
3^5	3^4	3^3	3^2	3^1	3^0

The characteristics of a ternary number is that its elements are 0, 1, or 2, which is more choice than binary number whose elements are 0 or 1. In order to keep the number of coefficients whose value is zero after the embedding procedure, we must choose the quantized DCT coefficients whose absolute value is larger than 2.

3 Prepare Decomposition of Message and Ternary Jsteg

To embed secret message efficiently and safely, we will encrypt it before embedding. Ternary form of a message is shorter than binary form, but the capacity of ternary steganography methods is lower than that of binary, thus we decomposition the message into three different length sequences, two longer of them are binary and the shortest is ternary sequence. The advantage of the shortest length sequence can cover the shortage of proposed ternary steganography, which means our new method having less influence on DCT histogram.

The decomposition method of secret information and proposed embedding method are shown in next two subsections.

3.1 Decomposition of Message

In this paper, the secret message can be pictures or letters so that it can be transformed from decimal into binary. Suppose the S (assume n is even) is the binary message, it can be represented as

$$S = \{s_i \mid 1 \le i \le n, s_i \in \{0,1\}\}. \tag{1}$$

Firstly, every two consecutive bits are transformed into a decimal value ranging between 0 and 3. We denote the result as

$$S_1 = \{a_i = 2 \times s_{2i-1} + s_{2i} \mid i \le n/2, a_i \in \{0,1,2,3\}\}. \tag{2}$$

For instance, sequence S = {101100110100} can be combined as S = {10, 11, 00, 11, 01, 00}. Then its decimal is S_1 = {2, 3, 0, 3, 1, 0}.

Secondly every two consecutive values in the transformed sequence S_1 perform subtraction operation and form a new sequence shown as

$$S_2 = b_i = a_{2i-1} - a_{2i} \mid 1 \le i \le n/4, b_i \in \{-3,-2,-1,0,1,2,3\}\}. \tag{3}$$

Continuing the above example, we can obtain S_2 = {−1, −3, 1}.

Thirdly, to embed the processed message sequence S_2 using LSB, we define three sequences P_1, P_2, P_3 to represent S_2, of which the elements are 0, 1 or 2.

$$P = \{p_i = \| b_i \|, b_i \in S2, 1 \le i \le n/4\};$$
$$P2 = \{q_i, 1 \le i \le n/2\};$$
$$P3 = \{r_i, 1 \le i \le n/2\};$$

where q_i and r_i are shown in Table 3, where the bold numbers represent q_i and the other numbers stand for r_i. Due to the elements of set P are decimal which is shown in Table 2, we will converge it to binary sequence P_1. In summary, the original message sequence is divided into three sequence, {P_1, P_2, P_3}, which are more secure and shorter. Note, in Table 2 and 3, F is subtrahend set and L is minuend set.

Table 2. Elements of P

F \ L	0	1	2	3
0	0	1	2	3
1	1	0	1	2
2	2	1	0	1
3	3	2	1	0

Table 3. Elements of P_2 and P_3

F \ L	0	1	2	3
0	0 **0**	0 **0**	1 **0**	1
1	1 **1**	0 **1**	0 **1**	1 **1**
2	0 **0**	0 **2**	1 **0**	1 **0**
3	0	0 **1**	1 **2**	1 **1**

We can notice that the rate of the length of P_1 and P_2 is 2, while length of P_2 is larger than P_3 on the condition that P contains element 3. It is worth mentioned that a number '3' in P is obtained by 4 elements in S, that is to say, we can only use 3 numbers (a number in P_2 and two numbers in P_1 to represent 4 numbers in S. Later we will use these characteristics.

To have more number '3' in P_1, the raster-scan order of S can be changed.

It just like rearranging the elements in S.

3.2 Ternary JSteg

In this part, we propose a new embedding method based on the method called "JSteg". Instead of binary computation, we transform the decimal rounded quantized DCT coefficients into ternary.

The details are scanning every 8 × 8 quantized block DCT coefficients in a zigzag order, if the absolute value of the coefficient is larger than 2, its ternary LSB will be replaced by the element in P_3, and if the absolute of the coefficient is no more than2, skipping.

The extracting procedure is scanning every 8×8 quatized block DCT coefficients of stegoimage in a zigzag order and getting the LSBs of the coefficients whose absolute are larger than 2.

It is obvious that the new method has no influence on the coefficients 0, 1 and 2 which is the main part of coefficients. As a result, the DCT coefficients histogram characteristic can be kept. What's more, this method is more straight- forward and easier than the algorithm in [20], which is simulated in section 5.2.

4 Embedding and Extracting Procedure

4.1 Embedding Procedure

Due to we decompose the message into three sequences, it is easier to introduce the embedding procedure for color image. For gray image, we only need to divide it into three parts, so *R, G, B* mentioned next part are three parts of a coverimage. We can embed secret message as following steps. In the embedding procedures, we should record the length of P and P_3 as secret keys.

Step 1. Obtain three channels of the cover-image. Then calculate the rounded quantized DCT coefficients of every channel. Denoting them as *R, G,B* [21].

Step 2. Count the number of absolute value of *R, G, B* which is larger than 2 separately. Note the answer as c_1, c_2, c_3. Without loss of generality, we assume that the order of size is $c_1 \le c_2 \le c_3$. At the same time, count the number of nonzero coefficients in *R, G, B*, assuming the answer is $c_1^{'}, c_2^{'}, c_3^{'}$, accordingly, we assume the order of size is $c_1^{'} \le c_2^{'} \le c_3^{'}$.

Step 3. The first n bits elements of sequence S are processed in the procedure introduced in section 3.1, by which three sequences $P1$, $P2$, $P3$ are obtained.

Noting that n is no more than the length of S as well as

$$min\{4c_3, 2\} \le n \le max\{4c_3, 2\}. \quad \textbf{(4)}$$

Step 4. Adjust the number of every sequence. If n is smaller than the length of S, we can put the *remaining* elements in the sequences $P1$ or $P2$ on the condition that ensuring the number of every sequence is no more than its corresponding parts capacity.

Step 5. Embed the sequence P_3 in part B with the method proposed in section 3.2, and embed the sequence P_1 and P_2 in parts G and R use the proper methods respectively. (such as J SUNIWARD [15], UED [22], nsF5 [16] et al).

Step 6. Transform the modified *R, G, B* into space domain and obtain the stego image.

4.2 Extracting Procedure

Extracting procedure is the inverse steps of embedding. Assume the two secret keys are m and n, the extracting steps as follows:

Step 1. Transform the three channels of stegoimage into DCT domain separately.

Step 2. Extract the sequence P_1, P_2 and P_3 from the quantized DCT coefficients of corresponding channel

with the detection methods respectively.

Step 3. Combine the two consecutive numbers of P_1 to get a decimal value, by which we can get the sequence P. With the help of sequence P_1 and P_2, we can obtain the sequence S_1 by using the Table 2 and Table 3.

Step 4. Transform S_1 to binary in order to obtain S.

5 Simulations and Results

5.1 MSE and PSNR

Parameters *MSE* and *PSNR* are the essential standards to measure the image quality. Our goal is to measure the differences caused by steganography algorithm, so the *MSE* and *PSNR* are calculated as:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| I(i,j) - K(i,j) \right|^2. \tag{5}$$

where the $I(i,j)$ and $K(i,j)$ are the quantized DCT coefficients of cover-image and stegoimage at (i,j), separately. M and N are the numbers of row and column of I accordingly.

$$PSNR = 10 \times \lg \frac{\max_I^2}{MSE} = 20 \times \lg \frac{\max_I}{\sqrt{MSE}}. \tag{6}$$

where max_I is the largest number of I, which is 256 in our experiment. *MSE* and *P SNR* reflects the difference between cover-image DCT coefficients and stegoimage DCT coefficients, and the larger PSNR is, the less difference caused by steganography algorithm.

5.2 Simulations and Results

In this section, we test the proposed steganpgraphy algorithm using MATLAB 2014a with 'Lena.jpg' and 'Pepper.tiff', two color images with size 512×512. The secret sequence consists of pseudo random binary numbers. *MSE* and *P SNR* are used as two secure standards.

To achieve the biggest embedding capacity of a cover image, first we count the number of absolute quantized DCT coefficients which is larger than 2 and nonzero in three channels. The result is shown in Table 4.

Table 4. Numbers of right coefficient

	R	*G*	*B*
Larger than 2	5663	7109	5307
Nonzero	22232	28042	26791

Obviously we will choose G matrix to embed sequence P_3. Firstly we trans- form the article to binary sequence S. According to formula (4), we take the first n = 35000 elements of S as S'. By adjusting the length of S', and we can obtain the proper length as n = 33166, which determines the length of sequences P_1, P_2, P_3 as 16582, 8291 and 7108 separately. In this case, 33166 bits shrink down to 31981 bits that can be embedded in the cover image with proposed steganography algorithm. Specifically, sequences P_1 and P_2 are embedded in the parts B and R with J UNIWARD algorithm [23, 24] while P_3 is embedded into G with our proposed algorithm. The two cover images and stegoimages are shown in Fig. 1. Due to the results are resemble, we only show cover histogram of G in 'Lena' and that of stegoimage in Fig. 2. The *MSE* and *P SNR* are shown in Table 5.

Table 5. *MSE* and *PSNR*

	R	*G*	*B*
MSE	0.0153	0.0315	0.0430
PSNR	60.1657	63.1501	53.7522

One can measure the security of a steganography algorithm from different angles. For the proposed method, J UNIWARD algorithm has a strong detection resistant performance for most of the popular steganalysis. Now we show the ad- vantages of the proposed algorithm from Sensory Evaluation and quantification analysis. From Fig. 1, we can conclude that this algorithm obtains a good visual effect, which is proofed by numerical characteristics in Table 5 and Fig. 2.

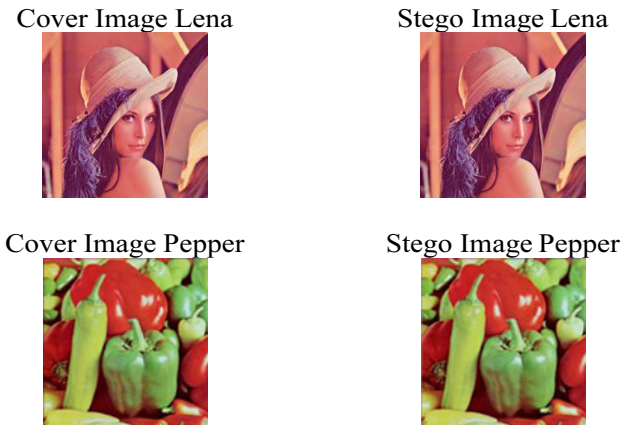

Fig. 1. Cover image (left) and Stego image (right)

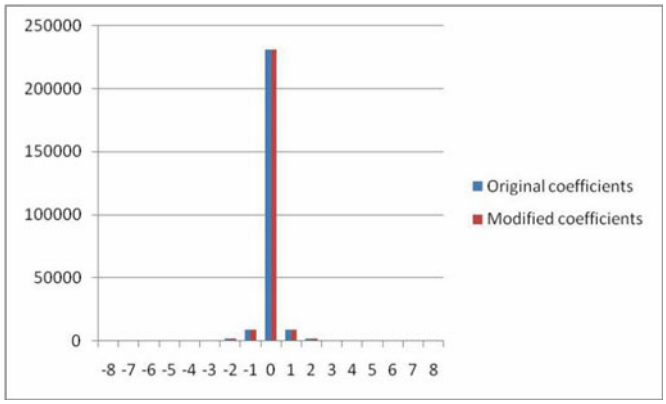

Fig. 2. DCT coefficients histograms of cover image and stegoimage

6 Conclusions

In this paper firstly we propose a new method to dispose the secret message into 3 parts to have a shorter and safer representation. Secondly we propose a embedding method based on ternary. The advantage is that it overcomes the shortcoming of traditional JSteg method and has little influence on the cover-image histogram. The disadvantage is that it will decrease the embedding capacity, yet by proper processing the original sequence that is make full use of the advantage of ternary JSteg algorithm the above disadvantage can be solved. Thirdly, we define a new standard to measure the influence caused by steganography algorithm without the influence of compression.

Our future work is to find a better algorithm to improve the embedding capacity of ternary sequences. What's more, combining the advantage of ternary sequence with better scanning order of sequence S to have a shorter sequence P_3.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China (no. 61402044) and Beijing City Board of Education Science and Technology Plan (no.KM201711232009).

References

[1] T. Denemark, J. Fridrich, Steganography with multiple JPEG images of the same scene, IEEE Transactions on Information Forensics and Security 12(10)(2017) 2308-2319.

[2] T. Denemark, J. Fridrich, Steganography with two JPEGs of the same scene, in: Proc. 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017.

[3] X. Song, F. Liu, L. Chen, C. Yang, X. Luo, Optimal Gabor filters for steganalysis of content-adaptive JPEG steganography, KSII Transactions on Internet & Information Systems 11(1)(2017) 552-569.

[4] Z. Wang, Z. Yin, X. Zhang, Distortion function for JPEG steganography based on image texture and correlation in DCT domain, IETE Technical Review. <https://www.tandfonline.com/doi/abs/10.1080/02564602.2017.1304289>, 2017 (accessed 28.03.17).

[5] D. Uljarević, M. Veinović, G. Kunjadić, D. Tepšić, A new way of covert communication by steganography via JPEG images within a Microsoft Word document, Multimedia Systems 23(3)(2017) 333-341.

[6] L.J. Guo, J. Q. Ni, Y.Q. Shi, Uniform embedding for efficient JPEG steganography, IEEE transactions on information forensics and security 9(5)(2014) 814-825.

[7] M.C. Trivedi, S. Sharma, V.K. Yadav, Analysis of several image steganography techniques in spatial domain: a survey, in: Proc. the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016.

[7] C. Mohapatra, M. Pandey, A review on current methods and application of Digital image steganography, International Journal of Multidisciplinary Approach and Studies 2(2)(2015) 163-178.

[9] F.Y. Li, X.P. Zhang, J. Yu, W.F. Shen, Adaptive JPEG steganography with new distortion function, Annals of Telecommunications- Annales des Telecommunications 69(7)(2014) 1-10.

[10] B. Li, J.H. He, J.W. Huang, Y.Q. Hi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing 2(2011) 142-172.

[11] H. Noda, M. Niimi, E. AndKawaguchi, High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recognition Letters 27(2006) 455-461.

[12] T. Morkel, J.H.P. Eloff, M.S. Olivier, An overview of image steganography, in: Proc. Information and Computer Security Architecture (ICSA), 2005.

[13] T. Zhang, X.J. Ping, A fast and effective steganalytic technique against JSteg- like algorithms, in: Proc. 8th ACM Symp. Applied Computing, 2003.

[14] A. Westfeld, F5-A steganographic algorithm, in: I. S. Moskowitz (Ed.), Information Hiding 2001, LNCS 2137, Springer Berlin Heideberg, New York, 2001, pp. 289-302.

[15] H. Vojtěch, F. Jessica, D. Tomáš, Universal distortion function for steganography in an arbitrary domain, EURASIP Journal on Information Security, 1(2014) 1-13.

[16] J. Fridrich, T. Pevný, J. Kodovský, Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities, in: Proc. the 9th ACM Multimedia & Security Workshop, 2007.

[17] S. Vahid, C. Rémi, F. Jessica, Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security 11(2)(2016) 221-234.

[18] N. Pandian, R. Thangavel, Gray coded grayscale image steganography using Huffman encoding, International Journal of Image Processing 6(5)(2012) 334-348.

[19] P.Y. Chen, H.J. Lin, A DWT based approach for Image steganography, International Journal of Applied Science and Engineering 4(2006) 275-290.

[20] V. Sachnev, H.J. Kim, Ternary data hiding technique for JPEG steganography, in: Proc. IWDW, Springer Lecture Notes in Computer Science 6526(2010) 202-210.

[21] R. Amirtharajan, S.K. Behera, M.A. Swarap, J.B.B. Rayappan, Colour guided colour image steganography, Universal Journal of Computer Science and Engineering Technology 1(1)(2010) 16-23.

[22] L. Guo, J. Ni, Y.Q. Shi, An efficient JPEG steganographic scheme using uniform embedding, in: Proc. Fourth IEEE International Workshop on Information Forensics and Security, 2012.

[23] V. Holub, J. Fridrich, Digital image steganography using universal distortion, in: Proc. 1st ACM Information Hiding and Multimedia Security Workshop, 2013.

[24] Y. Zhang, X. Luo, C. Yang, D. Ye, F. Liu, A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients, in: Proc. 2015 10th International Conference on Availability, Reliability and security (ARES), 2015.