

Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm

Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani

Abstract—Due to the rapid development in digital communication through the international networks, data security has become an important problem in this field. Through different ways of hiding data in communications; steganography is used to hide the existence of the secret message. Steganography is a branch of hidden information's science, which tries to achieve an ideal security level in military and commercial usages, so that sending the invisible information will not be exposed or distinguished by the others. Steganography is implemented in different frequency and spatial domains. JSteg algorithm is one the first methods used for hiding data in frequency domain. In this algorithm; all of DCT coefficients are manipulated sequentially to hide secret data in the least significant bits of pixel values. In this way some characteristics of the cover image such as PSNR and histogram diagrams will be changed. These changes can be used later to diagnose the existence of the secret data behind the image and steganography will be failed. In this paper a new method for embedding data in the DCT coefficients is proposed. DCT values in this way will not be changed directly and for hiding reason the middle frequencies are replaced with each other. This algorithm has greater PSNR values and coefficient histogram of the steganogram is more similar to the original one. So this algorithm has higher robustness against the statistics attacks.

Index Terms—Coefficient histogram, Discrete Cosine Transform, DCT, PSNR, Steganography.

I. INTRODUCTION

Steganography is a method for hiding secret data in another media which is called cover. The selection of cover and techniques for hiding data is for catching less attention and visual distortion. The outlet of steganography system is called Steganogram which has the similar characteristics to the cover, and also it contains our hidden information. Steganography is not a new subject which is considered nowadays, its history can be traced in 440 BC. In the first usage of this knowledge the secret messages were written on the shaved head of Greek soldiers, when their hair grew up, the messages were concealed from the others. By development of digital communication and multimedia technology, steganography is being entered to a new season. These days images, audio and video files can be used as a cover media. In this paper, a digital image is used for this reason. By changing the way of data embedding in JSteg algorithm a new method can be achieved, which has higher signal to noise ratio and also its coefficient histogram is more similar to the cover image histogram.

Most of the steganography techniques; which hide the data

directly in the pixels of the image, use the Least Significant Bit (LSB) embedding method. By using random factors and secret keys the security of steganography can be increased, but by considering the statistical characteristics of these images, most of these techniques will be fractured. However the least significant bits of the pixels looks random, practically they don't have random properties and represent some characteristics of the image. Evaluation on the properties of the image before and after steganography process, can indicate the changes in these least significant bits. As a result the application of steganography technique in spatial domain is not safe enough against the recent developing attacks. In the next section a brief introduction to the steganography in frequency domain is presented. Next the JSteg algorithm will be introduced as one of the first methods in this field. Steps of data embedding in the replacement algorithm are similar to this method and study of JSteg algorithm can help us to improve the results of the replacement method. After implementation of these methods, the outlet results will be compared. This comparison includes the Perceptibility of steganogram in the percent of PSNR, the capacity of hidden information and robustness against the statistical attacks on the image histogram.

II. REVIEW OF STEGANOGRAPHY

The term steganography illustrates the art and science of hidden communication. By using steganography there is a chance to send messages so that nobody can detect the existence of the message. The message is embedded by weakening some characteristics of another media, which is called cover. Final output has equal properties to cover media, and also it includes our secret information. This new object is transmitted. If somebody is able to interpret this transmitted package, the secret message can be distinguished. While this transmitted package is really similar to cover media, detection of any embedded information is very difficult. For implementation of the steganography system, two algorithms are needed to be designed: one for hiding data and the other to extract this successfully. The main subject in embedding algorithm is to hide the secret message within the cover media without attracting any attention. The extraction algorithm has a simpler process and can be achieved by inverting the steps of embedding algorithm. All of the steganography steps can be shown graphically in Fig. (1).

The secret message usually is a text file or another image file which contains the secret information. This file is sent to the encoder unit in the first step. The encoder must be designed and implemented with high precision, to hide the secret message with a few distortion and changes in the cover image. Encoder unit usually needs a key to increase the security level of hiding method; this key is used in the

Manuscript received July 8, 2012; revised July 28, 2012.

The authors are with the Department of electrical engineering, Razi University, Kermanshah, Iran (e-mail: sheisi@razi.ac.ir, jmesgarian@yahoo.com, mostafa.rahmani1365@gmail.com).

extraction phase too. Without using this key, the message will be available without any impediment, if someone guesses the embedding or extraction algorithm.

Output of the encoder unit is called steganogram which should be close enough, to cover media. Then this image and the key, which is used in embedding phase, are transmitted via a communication channel. In the next step this package are applied to decoder unit. Output of the decoder unit is delivered in the receiver side. The output of extraction unit is just an estimate of secret message, because during transmission through the communication channel, the steganogram is exposed to different types of noises, which can change the values of some bits.

The application of steganographic technique can be broadly classified as operating in two different domains, such as spatial domain and frequency domain. In spatial domain, the embedding and hiding process are mostly carried out by bitwise manipulation. For example, manipulating the LSB in one of the color components in an image. While, the frequency domain includes those which involve manipulation of transformed image such as Discrete Cosine Transformation (DCT) and wavelet transformation. Such manipulation includes changing the value of the quantized DCT coefficients.

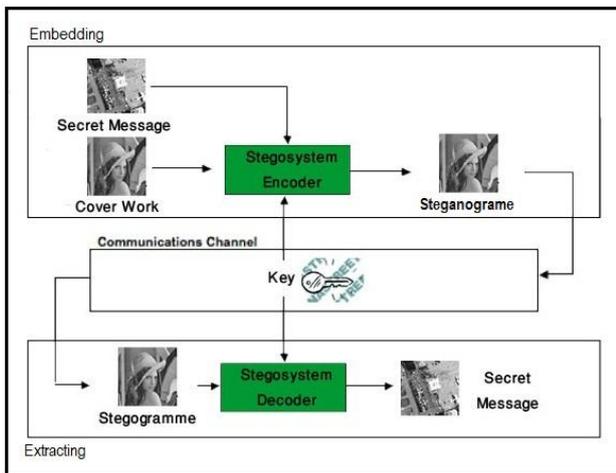


Fig. 1. Steganography steps in a graphical view

III. JSTEG ALGORITHM

Basically the JSteg algorithm is the precise copy of the LSB embedding method in the spatial domain. This method also uses the least significant bits for hiding data. In this algorithm, data bits are hidden in the least significant bits of the DCT coefficients instead of the real values of the pixels. DCT is a special kind of Fourier transformation. The Fourier transform is more common and contains realistic and imaginary parts. DCT can be called the real part of Fourier transform. Discrete cosine transform is given as refer to “(1)”.

$$F(u, v) = \frac{1}{4} C(u)C(v) \cdot \sum_{x=0}^7 \sum_{y=0}^7 \left[f(x, y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \right]. \quad (1)$$

In this equation $x, y, u, v \in \{0, 1, \dots, 7\}$, $f(x,y)$ is the particular pixel color space component, $C(u) = 1/\sqrt{2}$ if $u = 0$ and otherwise $C(u) = 1$.

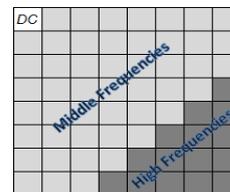
This transformation builds an 8*8 blocks, included 64 DCT coefficients from each 8*8 block of image. Before starting the steganography process, the image is transformed to DCT domain as a separated 8*8 blocks. The next step is to quantize the transformed DCT coefficients. This can be done by using element wise division and rounding the result as refer to “(2)”.

$$F'(u, v) = \text{Round} \left(\frac{F(u, v)}{Q(u, v)} \right) \quad (2)$$

$Q(u, v)$ are the indices of quantization matrix. Two types of coefficient could be seen in every 8*8 block: DC and AC. The value at the top left of each 8*8 block is known as the DC coefficient. It contains the mean value of all the other coefficients in the block, referred to as the AC coefficients. The DC coefficients are highly important in each block as they give a good estimate of details in the block. Changing the value of the DC coefficient will also change many of the values of the AC coefficients, and this will create a visual discrepancy when the image is converted back to the spatial domain and viewed normally. For this reason, JSteg algorithm does not embed message data in any of the DC coefficients for every block. In computer science, the term least significant bit refers to the smallest (right-most) bit of a binary sequence. The structure of binary is such that each integer may only be either 0 or 1. Now let us consider the following 8-bit binary sequence:

1 0 1 1 0 0 1 1

Summing the entire values yield a result of 179. The right-most value (denoted in bold text) is the LSB of this sequence. Changing the LSB value from 0 to 1 does not have a huge impact on the final value; it will only change to +1. If each 8-bit binary sequence is considered as a DCT coefficient of a block, changing the LSB value from 0 to 1 will only change the DCT value to +1. This change is not very noticeable when this value is transformed to the spatial domain.



No key is used for this algorithm. So long as the decoder knows that the embedding took place in the DCT domain, it will be capable of extracting the message successfully. In the final step, the new DCT coefficients, which the last bit of them represents one bit of data are transformed reverse to the spatial domain. The out coming image in this step is the Steganogram which is sent to receiver.

IV. DCT REPLACEMENT ALGORITHM

The process of embedding data in this proposed algorithm is the same as JSteg algorithm in the first steps. The only

difference is in manipulation of coefficients. First step is to divide the cover image in to the 8*8 blocks, and then each block is transformed to the discrete cosine transformation domain. Similar to the JSteg algorithm, DCT coefficients are sorted in the frequency order by zigzag ordering method. So they stand in the frequency positions 0 to 63, the zero frequency is called DC and the rests are called AC coefficients. Unlike the JSteg algorithm which is applied on the all AC coefficients, in this method the embedding is done only on the middle frequencies. Therefore the perceptibility of image can be increased after changing the DCT values. Generally no bordering is defined between the middle and high frequencies. Here according to the experimental result of the algorithm, the last 15 coefficients as shown in the Fig. (2) are called high frequencies and the other coefficients except the DC are named middle frequencies.

By starting from the last coefficient in the middle frequencies area, the LSB of each coefficient is replaced with data bits. In this algorithm, parameter **b** is defined as the number of bits which can be changed in each coefficient. If the bits of data are shown with MB (Message Bit) and the least significant bits of coefficients with LSB, by selecting **b=1**, this will yield three possibilities on the changes as shown below :

- LSB = 1 & MB = 0 ----- Possibility (1)
- LSB = 0 & MB = 1 ----- Possibility (2)
- LSB = 0 and MB = 0 or LSB = 1 & MB = 1-- Possibility (3)

Fig. 2. DC, middle and high frequencies

In Possibility (3), both of the LSB and MB are 0 or both of them are 1, therefore they are equal and there is no need to change the LSB. In the first and second possibilities, the MB and LSB are different, in the first one, LSB bit needs to be decreased and in the second it must be increased. In this algorithm, in the first and second possibilities, before changing LSB bits, this change is stored in intermediate variable; this variable is then used to search for another coefficient in the block, which has the equivalent value. For example in Fig. (3), there is an AC coefficient with the even value “8”, which is considered to embed “1” in it, as a result its value will be increased to “9”. While in the same block, if there is another AC coefficient with value “9”, these two coefficients can be replaced with each other simply. If any exact equal value can not be found after searching the whole block, the closest coefficient is used for replacement. The closest value here is defined a coefficient, which only is different in **b** LSB bits. If **b** is selected “1”, the closest value should be the same type (even or odd) as the altered coefficient value. So if “9” is not found in the block, any of the “1”, “3”, “5” or “7” can be used instead.

Replacing LSB bits of image with the data bits decrease the similarity between steganogramme and the cover image. This kind of changing in the first look can be considered as adding some noises to the cover image. So the perceptibility of this change is calculated with the Peak Signal-to-Noise Ratio (PSNR), which is used in the noisy communication channels to evaluate the ratio between the signal and the noise. The phrase PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its

representation. It is most easily defined via the mean squared error (MSE) which for two X by Y monochrome images “I” and “K” is defined as refer to “(3)”.

$$MSE = \frac{1}{XY} \sum_{i=0}^{X-1} \sum_{j=0}^{Y-1} [I(i,j) - K(i,j)]^2 \quad (3)$$

And the PSNR is defined as refer to “(4)”.

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ = 20 \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (4)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. Usually the images with PSNR value less than 40, will be extremely ruined and can not be compared with the original image.

Finally, if the embedding process using of replacement method failed and neither nor closest coefficient were not found , then replacement process can be ignored and similar to JSteg, data bit is embedded in the LSB bit directly. The less these direct embeddings are, the total number of coefficients and their histograms will be closer to the cover image. In the last step of algorithm, DCT blocks returned to the original form by inverting zigzag method and transformed again to the spatial domain by inverting DCT transformation. In this algorithm the internal parameters **n** & **b** are used to change the number of embedded coefficients (**n**) and the number of bits in each coefficient (**b**). For decoding the message in the receiver side, these parameters will be used to extract the secret message successfully. These parameters work as a key. Without any information about this key nobody can access the message correctly. There for the security level in this algorithm is higher than the JSteg algorithm which does not use any keys for communication.

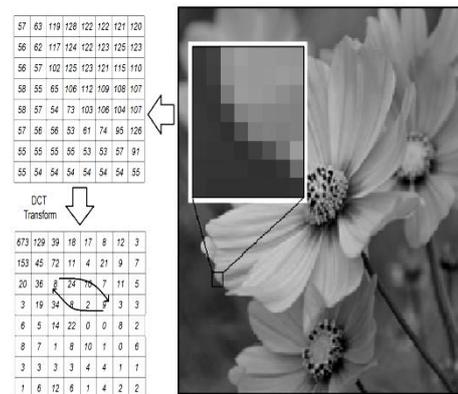


Fig. 3. Graphical view of the replacement algorithm

V. RESULTS OF ALGORITHMS

A. Perceptibility

Perceptibility means, the similarity between steganogramme and the original cover image. The more the outlet of algorithm is similar to the original image, the more

perceptibility of algorithm will be achieved, therefore the recognition of hidden data will be more difficult. PSNR ratio is used for comparison the perceptibility of two images. By changing the parameters n & b in replacement and JSteg algorithms, PSNR diagrams can be drawn as Fig. (4-a). In this Fig. b is constant, equal to 1 and n is increased from 5 to 60. As it can be seen in this Fig. the PSNR of Replacement algorithm for all selected n is greater than the JSteg algorithm.

In smaller n , PSNR values of both algorithms are high and the PSNR for replacement algorithm is much higher than the JSteg. By increasing n , PSNR values are getting smaller and also getting close together. It means that for the smaller n , the similarity between the steganogramme and the cover image is higher and by choosing the bigger values of n , perceptibility of output images will be decreased. The most difference between two algorithms happens in n about 25. So the most proper area for operation is $n=20$ to $n=30$.

B. Capacity

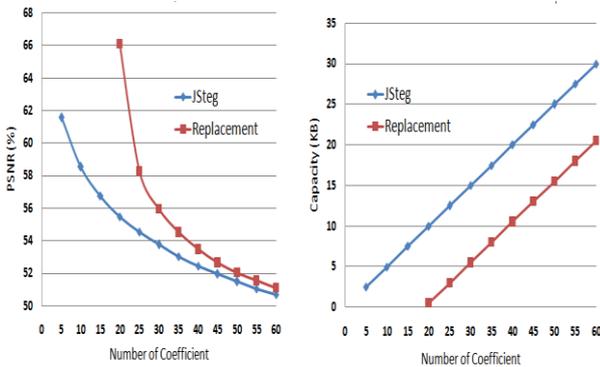


Fig. 4. Results of JSteg & replacement algorithms (a) PSNR, (b) capacity

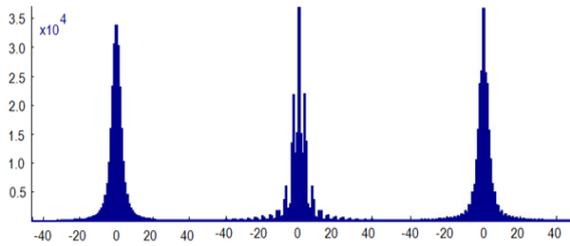


Fig. 5. Coefficient histogram for (a) cover image (b) JSteg steganogramme, (c) replacement algorithm

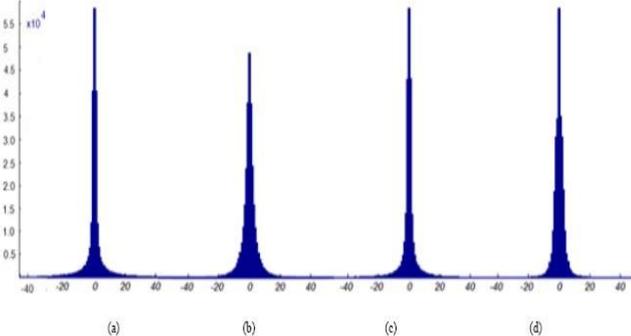


Fig. 5. Coefficient histogram for (a) cover image (b) JSteg steganogramme, (c) replacement algorithm

By considering the method of embedding data in replacement algorithm, the amount of embedded data can be

calculated as refer to “(5)”.

$$Capacity = \frac{X * Y}{64} * b * (n - 15) \quad (5)$$

In this equation, X and Y are dimensions of the cover image. By dividing the product of X, Y by 64, the number of $8*8$ blocks is achieved. During data embedding process, no data is embedded in the last 15 coefficients, so the term $(n-15)$ is used here, and in each coefficient b bits of data will be embedded. It’s practical to compare the capacity of embedded data between JSteg and replacement algorithm. Let b is 1 and increase n from 5 to 60, so the capacity diagram can be drawn as it’s shown in Fig. (4-b).As it can be seen in this Fig., for the same n , JSteg capacity is always more than the replacement algorithm. So by using this algorithm for steganography, the amount of embedded data is less than the JSteg in equal condition.

C. Robustness

The steganalysis attacks can be divided in three main groups; visual attacks, structural attacks and statistical attacks. Frequency domain algorithms are usually exposed to the statistical attacks. The most important and common types of these, are histogram attacks. After data embedding progress in the cover image, the number of pixels with the same brightness level in the spatial histogram, and also number of DCT coefficients in the coefficient histogram will be changed. Because of the symmetrical property of Fourier transform, the images which are chosen as a cover media will have the symmetrical histogram. This means that the coefficient have equal abundance around a central axis in the form of positive and negative values. After applying the steganography algorithm on the image, this symmetrical property in coefficient histogram will be eliminated, and this can be an indication of hiding something in the image. The more the outlet histogram of an algorithm is close to the original image, the algorithm have more efficiency and more robustness against the statistical attacks. In Fig. (5-a), the original histogram of a sample cover image is shown.

As it can be seen in this Fig., the original histogram for cover image has a symmetrical structure. The results of JSteg and replacement algorithms are shown in Fig. (5-b) and (5-c). It can be seen that structure of Fig. (5-b) is different from the original one. However histogram (5-c) which is the result of replacement histogram is more similar to the cover image histogram. Because of this similarity, detection of secret data, in replacement method, is more difficult and robustness against the steganography attacks is higher than the JSteg algorithm.

VI. CONCLUSION

Applying the replacement algorithm on sample images shows that histogram for those images are much similar to the cover images. However the capacity in this method is less than the JSteg algorithm, the PSNR of output image in equal condition is better than JSteg algorithm. PSNR values of these two algorithms on some popular images are shown in Table I.

TABLE I: PSNR VALUES AND CAPACITY FOR SAMPLE IMAGES

File Name	JSTEG		Replacement	
	PSNR (%)	Capacity (KB)	PSNR (%)	Capacity (KB)
Butterfly	51.2	240	56.8	164
Lena	50.5	240	55.1	164
Saturn	50.1	240	55.8	164
Hestain	51.8	240	56.2	164
Pears	51.1	240	55.8	164

As it can be seen in this table, PSNR ratio for all of the images, in replacement algorithm is greater than the JSteg. The histograms of these images are shown in Fig. (6). All of these histograms are much similar to the original cover images. More development in this algorithm can be done by changing the parameters to get more teganography capacity, and PSNR ratio. By changing these parameters the best working area can be found to have the most similar coefficient histogram to the cover image.

REFERENCES

- [1] S. N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust Image-Adaptive Data Hiding Based on Erasure and Error Correction," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1627-1639, Dec. 2004.
- [2] R. C. Gonzalez and R. E. Woods, and S. L. Eddins, "Digital Image Processing using MATLAB Second Edittion," *Addison Publishing*, 2004.
- [3] P. Honeyman, "Hide and Seek: An introduction to steganography", *IEEE Security and Privacy Journal*, 2003.
- [4] K. L. Chiew, L. Jane, F. Sarah, and S. Juan, "Steganography: DCT Coefficients Reparation Technique in JPEG Image," *International Journal of Digital Content Technology and its Applications*, vol. 2, no. 2, 2008.
- [5] N. Hideki, N. Michiharu, and K. Eiji, "High-performance JPEG steganography using quantization index modulation in DCT domain," *Pattern Recognition Letters*, vol. 27, pp. 455-461, 2006.
- [6] C. C. Chen, "A reversible data hiding scheme using complementary embedding strategy," *Information Sciences*, pp. 3045-3058, 2010.
- [7] Q. Liu, A. H. Sung, M. Qiao, Z. C. B. Ribeiro, "An improved approach to steganalysis of JPEG images," *Information Sciences*, vol. 180, 2010, pp. 1643-1655
- [8] C. L. Liu and S. R. Liao, "High-performance JPEG steganography using complementary embedding strategy," *Pattern Recognition*, vol. 41, 2008, pp. 2945 - 2955
- [9] W. Stallings, "Cryptography and Network Security Principles and Practice," *third ed, Pearson Education*, New Jersey, 2003.
- [10] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, pp. 313-336, 1996.
- [11] D. Gruhl and W. Bender, "Information hiding to foil the casual counterfeiter," in *Proc. Information Hiding Workshop*, Portland, OR, Apr. 1998.
- [12] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conference on Image Processing*, Austin, TX, 1994, pp. 86-89.
- [13] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *Proc. IEEE ICASSP '96*, 1996, pp. 2168-2171.
- [14] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in *Proc. IEEE Digital Signal Processing Workshop*, Loen, Norway, Sept. 1996, pp. 37-40.
- [15] J. R. Smith and B. O. Comiskey, "Modulation and information hiding in images," in *Proc. Int. Workshop on Information Hiding*, Cambridge, UK, May 1996, pp. 207-226.
- [16] J. Zhao and E. Koch, "Embedding robust labels into images for Copyright protection," in *Proc. Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, R. Oldenbourg, E. Vienna, Austria, 1995, pp. 242-251.
- [17] [17] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. 1996 Int. Conf. Image Processing*, vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 219-222.
- [18] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoan, "Secure spread Spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673-1687, Dec. 1997.



Jafar Mesgarian received the Computer hardware engineering degree from Shahid Beheshti University, Tehran, Iran in 2000. The M.S. degree in electrical engineering from Razi University, Kermanshah Iran in 2011.