Utilizing Image Block Properties to Embed Data in the DCT Coefficients with Minimum MSE

Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, and Fathy Z. Amer

Abstract—**Steganography aimed at hiding the presence of communication in a medium that is used to carry secret messages (image, audio, or video). Many steganographic systems can be attacked visually or statistically (steganalysis). In this paper, block based steganography algorithm with minimum MSE is presented, an algorithm that embed data in the least significant bit (LSB) of the discrete cosine transform (DCT) coefficients of JPEG image blocks. This technique exploits the ratio of even to odd coefficients in each image block and embeds data bits in a way that preserves the ratio between even and odd DCT coefficients of each image block. Block Based Steganography (BBS) algorithm offers high capacity with statistically minimal changes compared to current steganographic algorithms. The mean square error of BBS algorithm in the spatial domain is presented.**

Index Terms—**JPEG hiding, information hiding, steganography, steganalysis,.**

I. Introduction

A steganographic system embeds message bits in an innocuous looking cover medium (for example image, audio, or video) so as not to arouse an eavesdropper's suspicion. There is a distinction between encryption and steganography in the sense that in encryption a third party knows there is a communication is taken place between two parties, but a decryption algorithm is needed to attack this communication.

Hence the strength of encryption comes from how powerful the encryption algorithm to prevent any attacker from deciphering the message exchanged between sender and intended recipients.

In steganography, the communication occurs in a way such that a third party can not observe a hidden communication is taking place other than exchange of media files. In order to not raise a third party suspicion, the redundant bits in a cover medium are utilized to transfer information without distorting the cover medium statistical properties [1] - [5].

The primary goal in a steganographic system is to keep its mere presence unobservable by modifying some of the cover medium redundant bits. These modifications to cover medium's redundant bits leave detectable traces. Even if the hidden message is not revealed, the existence of it is detected. Any significant changes to cover medium redundant bits will change its statistical properties; as a result a third party can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is referred to as statistical steganalysis. After embedding message bits in a cover medium, the result is a stego medium that should be secure against visual and statistical attacks and robust against modification such as recompression. Modern steganographic systems are robust against visual attacks and weak against statistical attacks and the ones that are robust against first order statistical attacks offer a relatively small capacity [6] - [10].

In this paper, the block based steganographic algorithm is introduced that hide data in the least significant bits (LSB) of the Discrete Cosine Transform (DCT) coefficients of JPEG image blocks. This technique embeds data in a way that matches the ratio between even and odd DCT coefficients of each image block so as to preserve the statistical properties of JPEG images. Message bits are divided into segments, the segment length is determined by the number of nonzero AC DCT coefficients in each 8x8 block of the image, and each segment is possibly modified by embedding the bitwise complement so as to preserve the ratio between even and odd nonzero AC DCT coefficients. The embedding process is referred to as Block Based Steganography (BBS) algorithm. The BBS algorithm offers high capacity with statistically minimal changes compared to other existing steganographic algorithms. A comparison between BBS and modern steganographic systems is presented and the mean square error of the BBS algorithm is measured.

The rest of this paper is organized as follows. In section II, the block based steganography algorithm is introduced. Simulation results and comparisons between the proposed algorithm and the current embedding algorithms are presented in section III. The final section gives the conclusion and future work.

II. Block Based Steganography

This algorithm utilizes the statistical properties of DCT coefficients of the image blocks (Fig. 1) to hide data bits. In each image block, the ratio of even to odd coefficients is different from other blocks. The first order statistical properties of the JPEG images can be preserved by embedding message bits that match the distribution of even and odd DCT coefficients.

The uniformly distributed message bits can be divided into small segments of variable lengths. Each segment length equals to the number of nonzero AC DCT coefficients of the

Manuscript received January 20, 2011; revised May 10, 2011.

H. A. Morsy is with the Telecommunication Department, Helwan University, Cairo 11792, Egypt (e-mail: hmorsy@helwan.edu.eg).

Z. B. Nossair is with the Telecommunication Department, Helwan University, Cairo 11792, Egypt (e-mail: znossair@helwan.edu.eg).

A. M. Hamdy is with the Telecommunication Department, Helwan University, Cairo 11792, Egypt (e-mail: ahamdy@helwan.edu.eg).

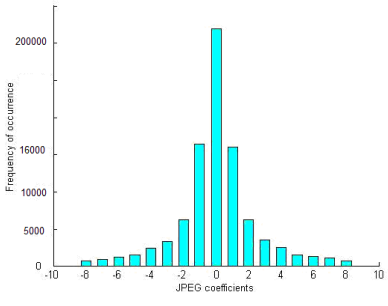
F. Z. Amer is with the Telecommunication Department, Helwan University, Cairo 11792, Egypt (e-mail: famer@hlewan.edu.eg).

corresponding JPEG image block which will be modified according to the data bits in that segment. Some segments will be further divided into two segments of equal number of bits to minimize the changes that affect the ratio of odd and even AC DCT coefficients introduced by embedding data with different even to odd ratios.

Let N be the total number of DCT coefficients and n_0, n_{DC}, and n_H are the zeros of DCT coefficients, the number of DC DCT coefficients and the total number of control bits in the image respectively. One bit will be assigned for the number of segments in the block and another bit is assigned for the polarity of data. This bit equals to one if the data are embedded directly or zero if the complement of data is embedded. Choosing to embed the data or the complement of the data depends on the ratio of even to odd coefficients in the corresponding block that minimize the changes introduced by embedding data to that block. An extra bit will be assigned only if the embedded segment is divided into two smaller segments of equal lengths. Two segments in one block are used if the changes introduced by one segment are larger than that introduced by two segments. On the average there are 2.5 bits used as a header in each block. The efficiency of embedding per nonzero AC DCT coefficients will be:

$$\eta = \frac{N_{AC} - n_H}{N_{AC}} \quad (1)$$

(a)



(b)

Fig. 1. Standard test image and its histogram:
(a) Boat, (b) The histogram

where $N_{AC} = N - n_0 - n_{DC}$ is the total number of nonzero AC DCT coefficients. For a 512x512 JPEG image with 75 % of zero values AC DCT coefficients and $n_H = 2.5$ bits per block, the embedding efficiency will be 84.4 % of nonzero AC DCT coefficients.

The embedded data are encrypted with RC4 stream cipher this will add more security to the steganography algorithm. Since each block has variable lengths of non zero AC DCT coefficients, some blocks will have control bits larger than the data bits as a result this will affect the overall utilization of non zero AC DCT coefficients. A condition is added to minimize the number of control bits in each block that is the control bits n_h in each block has to be less than 50% of non zero AC DCT coefficients in that block n_b. This can be formulated as follows

$$n_h = \begin{cases} 0 & n_b < 3 \\ 1 & 3 \le n_b < 7 \\ 2 \text{ or } 3 & n_b \ge 7 \end{cases} \quad (2)$$

Equation 2 describes how many control bits required for each block of the image. If $n_b = 1$ or 2 , there is no need to add polarity bit or a bit referred to the segment number as a result the data will be embedded directly to the block. Also if n_b is between 3 and 7, it is a capacity consuming if a segment number is added to the embedded data since the probability of dividing the block bits into two segments is almost zero only polarity bit is required. The last option agrees with the algorithm technique. The following is the embedding and extracting algorithms.

A. Embedding algorithm

1) Encrypt message bits with encryption algorithm (e.g. RC4 stream cipher).
2) Apply DCT transform and quantization for image compression in JPEG image format.
3) Extract the nonzero AC DCT coefficients.
4) Divide message bits into segment of lengths equal to nonzero AC DCT coefficients in each block.
5) The LSB of first nonzero AC DCT coefficient equal to one for one segment and 0 for two segments.
6) The LSB of next coefficient will refer to the data polarity of the first segment.
7) Check the ratio of even to odd coefficients with embedding one segment and two segments.
8) Assign the LSB of the third coefficient for second segment if two segments choice is selected.
9) Embed message segments into non zero AC DCT coefficients.
10) Use Huffman coder for image encoding.

B. Extracting algorithm

1) Decode the compressed image using Huffman Decoder.
2) Convert odd coefficients into ones and even coefficients into zeros
3) If the first bit in a block is one, treat the rest of a block as one segment.
4) If the second bit is one, save the data directly to a file and if it is a zero save the complement.
5) If the first bit is zero, treat the rest of a block as two segments.
6) The second bit refers to the polarity of the first segment and the third bit refers to the second segment.
7) Repeat step 3 to 6 for the rest of nonzero AC DCT coefficients and append the extracted segment into the previous ones
8) Decrypt the message bits using decryption algorithm.

IV. Simulation Results

Assume c is the nonzero AC DCT coefficient index of DCT transform of JPEG image and the frequency of occurrence of two adjacent DCT coefficients are n_{2c} and n_{2c+1}. one can notice that the absolute value of frequency of occurrences of the histogram is monotonically decreasing as shown in Fig. 1, which means that $n_{2c}>n_{2c+1}$. If the embedded message is uniformly distributed, the number of frequency of occurrences of the LSB of DCT coefficients n^*_{2c} and n^*_{2c+1} for the stego image will have equal values. Based on this observation, Westfeld and Pfitzmann designed a statistical test to detect the similarity of the PoVs of stego images [8], [9]. This statistical steganalysis is known as Chi-square attack. The average number of each pair of values is $n^*_{2c} = (n_{2c} + n_{2c+1}) / 2$ and the Chi-square test can be calculated as

$$x^2 = \sum_{c=1}^{k} \frac{(n_c - n_c^*)^2}{n_c^*} \tag{3}$$

The probability of embedding as a function of Chi-square value is given as

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{x^2} e^{-\frac{t}{2}} t^{\frac{k-1}{2}-1} dt \tag{4}$$

where k is the degree of freedom – 1, the distribution of DCT coefficients of any JPEG image can be tested for uniform distribution using equation (4). Fig. 2 shows the probability of embedding with 50 % sample size for Jsteg algorithm and BBS algorithm; it is clear that the BBS algorithm is undetectable using Chi-square attack for any sample size.

Embedding data bits into DCT coefficients will affect the distribution of DCT coefficients [11], [12], [14], [15]. Assume N_D is the total number of distinct nonzero AC DCT coefficients and N_{AC} is the total number of nonzero AC DCT coefficients. Then the change density D_{AC} introduced in an image as a result of message embedding is given by

$$D_{AC} = \sum_{c=1}^{N_D} \frac{|n_c - n_c^*|}{N_{AC}} \text{ x } 100 \tag{5}$$

A comparison between BBS algorithm and Jsteg and F5 algorithms based on the absolute number of changes made to the nonzero AC DCT coefficients of an image (Boat image)[13]. Change density D_{AC}, is shown in Fig. 6. A reference algorithm is added in this comparison which has the property of embedding data directly into nonzero AC DCT coefficients without any processing or adding control bits; let's call it direct embedding algorithm (DEA). In addition to the randomly generated message bits, BBS algorithm is applied on a text file (Matlab readme file). Outguess is excluded from this comparison, since its maximum capacity is limited to 50 % of the available AC DCT coefficients. From Fig. 6 it can be noticed that F5 behaves very well when the message size is less than 33 %, the 40 % intersection in the figure can not be obtained with F5 algorithm for the total number of available DCT coefficients. Once the message size exceeds this limit, BBS algorithm outperforms other algorithms on both computer generated data and on real text files.

The size of an image and its textural properties affect the maximum limit of embedding data bits using different steganographic systems. Assume C is the maximum number of message bits that can be embedded into the non-zero AC DCT coefficients and N is the total number of DCT coefficients, the relation between C and N is given as:

$$C = \eta(N - n_0 - n_{DC}) \tag{6}$$

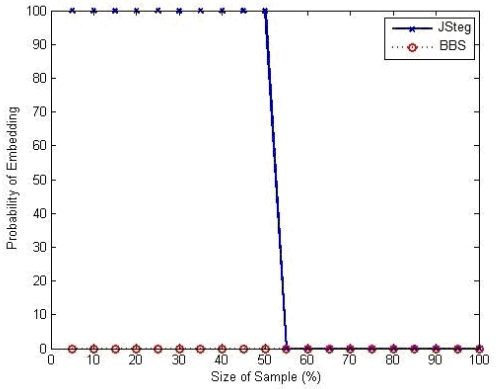


Fig. 2. The probability of embedding in Jsteg and BBS algorithms

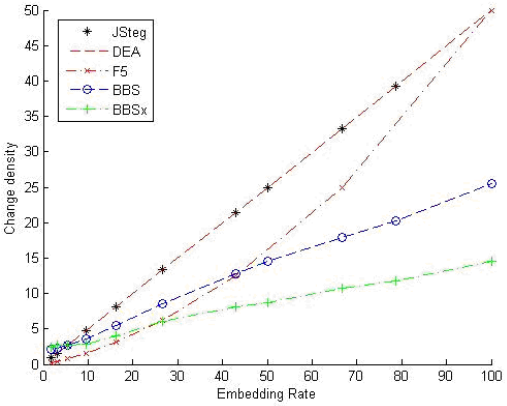


Fig. 3. A comparison between BBS algorithm and other existing algorithms

Equation 6 defines the relation between the capacity of embedding and the DCT coefficients. There is a tradeoff between the capacity and change density; the maximum capacity required the maximum change density will be introduced to the histogram. Fig. 4 shows some standard test images of size 512x512 of different textural properties used for capacity measurements. BBS algorithm provides high capacity in all gray images used in testing with different textural properties as shown in table I.

Fig. 4. Standard test images from left-top Barbara, Boat, Camera man, and Jungle and from left- bottom Lena, Living room, Mandrill, and Pirate

TABLE I: CAPACITY MEASUREMENTS (IN BITS) USING VARIOUS EMBEDDING ALGORITHMS

Test images	Capacity in bits			
	BBS	Jsteg	F5	Outguess
Mandrill	69214	54621	52621	27311
Jungle	54238	48311	42977	24156
Boat	39085	30680	32522	15340
Barbara	36702	31198	30671	15599
Living room	27035	26010	24357	13005
Pirate	27517	25974	24491	12987
Lena	19793	19848	18841	9924
Camera man	19771	18940	17663	9470

Some images provide high capacity using BBS algorithm than others, this is due to the textural properties of the cover image. BBS algorithm provides higher capacity of embedding with image of higher textural properties.

The mean square error (MSE) of an image due to embedding message bits in the frequency domain can be given as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j) - I_2(i,j))^2 \qquad (7)$$

where $I_1(i,j)$ and $I_2(i,j)$ are the image pixel values before and after embedding and M and N are the dimension of the image. MSE can be used to calculate the peak signal to noise ratio as follows:

$$PSNR = 20\log_{10}(\frac{255}{\sqrt{MSE}}) \qquad (8)$$

This criterion can measure the effect of embedding message bits in the frequency domain on the spatial domain. Another criterion which measures the changes due to message embedding is cross correlation and is given by:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j) - M_1)(I_2(i,j) - M_2)}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j) - M_1)^2} \qquad (9)$$

A comparison between BBS algorithm and DEA algorithm (Jsteg with utilizing the one coefficient) is shown in table II. BBS algorithm outperform the direct embedding algorithm based on PSNR but the cross correlation depends on the textural properties. The cross correlation of BBS algorithm is higher than the DEA algorithm with images with high textural properties.

TABLE II: THE MSE, PSNR AND CC OF STANDARD TEST IMAGES OF BBS ALGORITHM AND STANDARD EMBEDDING ALGORITHM.

Test Image	DEA			BBS		
	MSE	PSNR	CC %	MSE	PSNR	CC %
Mandrill	177	25.65	96.92	146	26.49	96.07
Jungle	230	24.51	91.06	187	25.41	91.11
Boat	105	27.92	95.99	88	28.69	99.87
Barbara	108	27.8	94.68	89	28.64	96.09
Living room	56	30.65	98.94	48	31.32	97.7
Pirate	55	30.73	99.19	48	31.32	98.08
Lena	41	32	99.39	38	32.33	98.11
Camera man	32	33,08	100	19	35.34	99.46

V. CONCLUSION

In this paper, a new steganographic algorithm is introduced that can provide maximum embedding capacity compared to current existing algorithms. This algorithm minimizes the changes introduced to the first order statistical properties of the cover media due to message embedding by reducing the changes introduced to each individual block of the image. The overhead used in this algorithm is fixed with each block as a result the algorithm provides high capacity of embedding with images of high textural properties. BBS algorithm proved to defeat both visual and statistical attacks exploiting the fact that uniformly distributed messages have non uniform distribution over small segments of the message bits. The peak signal to noise ratio and the cross correlation increase with images of low textural properties.

REFERENCES

[1] R. J. Anderson, and F.A. Petitcolas, " On the limits of Steganography," *J. Selected Areas in Comm.*, vol.16, no. 4, pp. 474–481, 1998.

[2] A. Kerckhoffs, *"La Cryptographie Militaire",* Journal des Sciences Militaires, *9th series, IX pp 5–38; Feb. pp 161–191, Jan. 1883.*

[3] N. Provos, and P. Honeyman, "Detecting Steganographic Content on the Internet," *CITI Technical Report* 01-11, 2001.

[4] C. Cachin," *An Information-Theoretic Model for Steganography*," *Cryptology ePrint Archive,* 2002.

[5] N. Memon, and M. Kharrazi, "Performance study of common image steganography," *Journal of Electronic Imaging* 15(4), 041104 (Oct-Dec), 2006.

[6] G. Cancelli, and M. Barni, "New techniques for steganography and steganalysis in the pixel domain, ", Ph.D. dissertation - Ciclo XXI. Report 2000 /028, 2009. www.zurich.ibm.com/˜cca/papers/stego.pdf.

[7] A. Westfeld, *"F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis,"* Springer-Verlag Berlin Heidelberg, *2001.*

[8] A. Westfeld, *"Detecting Low Embedding Rates, ", 5th* Information Hiding Workshop. *Nooerdwijkerhout, Netherlands, Oct. 7−9, 2002*

[9] A. Westfeld, and A. Pfitzmann, *"Attacks on Steganographic Systems,"* in Andreas Pfitzmann (ed) Information Hiding. Third International Workshop, *LNCS 1768,* Springer- Verlag Berlin Heidelberg. pp. 61–76. 289, 291, 293, 299, 2000.
[10] N. Provos, and P. Honeyman, "Hide and Seek: An introduction to steganography," *IEEE Computer security* 15407993/03, 2003
[11] T. Pevn'y, J. and Fridrich, "Benchmarking for Steganography," *Information Hiding.10th International. Workshop,* Santa Barbara, CA, LNCS vol. 5284, 2008.
[12] *C.* Hung*, "PVRG-JPEG Codec, 1.1," Stanford University, 1993. http://archiv.leo.org/pub/comp/os/unix/graphics/jpeg/PVRG 291.*
[13] D. Upham, "Steganography software for Windows," 1997, *http: //members.tripod.com/steganography/stego/ software.html*
[14] J. Fridrich, M. Goljan, and D. Hogea*, "new methodology for breaking steganographic techniques for JPEGs,"* in Proc. of SPIE: Security and Watermarking of Multimedia Contents, vol. 5020, pp 143–155, 2003.
[15] P. Gope, A. Kumar and G. Luthra *"An Enhanced JPEG Steganography Scheme with Encryption Technique",* International Journal of Computer and Electrical Engineering, 1793-8163, Vol. 2, No. 5, October, 2010.

Hamdy A. Morsy is a PhD student at Faculty of Engineering at Helwan University, Cairo, Egypt. He received his M.Sc. (2002) from Stevens Institute of Technology, Hoboken, NJ, USA. He is currently working as a senior teaching assistant at faculty of engineering at Helwan University.

Zaki B. Nossair received his B.Sc. in electronics and communications engineering, Helwan University (1978) and M.Sc. in electrical engineering (1985), Stevens Institute of Technology, NJ, USA. His PhD in electrical engineering, Old Dominion University, Norfolk, Virginia, USA, 1989. He is currently an associate professor at Helwan University. His current research interests in the field of image processing, speech processing.

Alaa M. Hamdy received his M.Sc. degree in computer engineering from Helwan University in1996 and his PhD degree from the faculty of electrical engineering, Poznan University of technology, Poland in 2004. Currently he is an assistant professor at faculty of engineering, Helwan University. His research interests in the field of image processing, pattern analysis and machine vision.

Fathy Z. Amer is the professor of Electronics in the department of Communications and Electronics, Helwan University, Cairo, Egypt. Previously, He was an associate professor at faculty of training at El ahsaa, Saudi Arabia from 1995 to 2004. His research interests include Microelectronics and Testing and Information Hiding.