www.ijarcsse.com

Volume 2, Issue 7, July 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT

Er. Mahender Singh *
Department of IT
MMU Mullana, India

Er. Rohini Sharma
Department of IT
MMU Mullana, India

Er. Dinesh Garg
Department of IT
RPIIT, Karnal,India

Abstract— ***Image steganography is the art of hiding information into the cover image in such a way that no one; apart from the sender and intended recipient even understand there is hidden message. In this paper, a novel steganography technique mainly based on joint photographic expert group (JPEG) is proposed. This technique is based on 2-D Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain.***

Keywords: DCT, Steganography, Embedding, Extracting, JPEG.

I. Introduction

With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. However, message transmissions over the Internet still have to face all kinds of security problems. Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA . These methods scramble the secret message so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper's attention. Hence, a new scheme, called steganography [4], arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files) so that it cannot be observed. Steganography is the art and science of invisible communication. The word steganography is derived from the Greek words *stegos* meaning "cover" and grafia meaning "writing" defining it as covered writing.

Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [5].

Data hiding methods for images can be categorized into two categories. They are spatial-domain methods and frequency-domain ones[2]. In the spatial domain, the secret messages are embedded in the image pixels directly. In the frequency-domain, however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed coefficients.

Joint photographic expert-group (JPEG)[25] is a famous file for images. It applies the discrete cosine transformer (DCT) to image content transformation. DCT is a widely used tool for frequency transformation. If we used JPEG images for data hiding, the stego-image will not easily draw attention of suspect. There is a JPEG hiding-tool Jpeg–Jsteg [1]. In the Jpeg–Jsteg embedding method, secret messages are embedded in the least signification bits (LSB) of the quantized DCT coefficients whose values are not 0, 1, or -1. The main drawback of Jpeg–Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coefficients are almost all zero and cannot hide messages according to the definition of Jpeg–Jsteg. To improve the message capacity of Jpeg–Jsteg[17], a new data hiding method based on JPEG and quantization table modification is proposed. Our method is inspired by Chan, Chang and Chung's approach[1]. We embed the secret messages in the least signification bit (LSB) of the quantized DCT coefficients that are located in the middle and lower frequency part. Our method generates a stego-image finally. Note that the secret messages are embedded in the quantized DCT coefficients in our method.

Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether, forcing people to study other methods of secure information transfer. Businesses have also started to realise the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit[8]. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

II. PROPOSED WORK

Our proposed method's capacity is higher than the methods previously and as far as stego image quality is concerned, image quality is higher than the other methods. The quality of stego image proposed by our method is comparably equal to Chang, Chan and Chung Method. Our method is also inspired by the technique Chang, Chan and Chung Method

A. The embedding procedure

We use JPEG image for data hiding since size of this image is quite small and this format is widely used on the internet. So stego image will not be suspected by anyone. Our embedding procedure contains five phases. These are message encryption, image pre-processing, secret message embedding, JPEG entropy coding, and JPEG stego-image generation.

In this method, a data encryption method is applied with a secret key k to encrypt the message M in the first phase. Here the message M can be a text, a video, or an image, etc. The encrypted result is called the secret message S = {s_1, $s_{2,}$ $s_{3,}$ . . . , s_{m}}, where s_i is a secret bit containing 0 or 1and m is the length of S.

16	11	10	16	1	1	1	1
12	12	14	1	1	1	1	1
14	13	1	1	1	1	1	1
14	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Table 1. The modified quantization table

In this phase, we use DCT to transform each block into DCT coefficients. The DCT coefficients are then scaled with a quantization table. The quantization table is listed in Table 1. This table is notably different from the quantization table of JPEG and Chang, Chen and Chung. This is because our secret message will be embedded in the middle and lower frequency part of the quantized DCT coefficients. Therefore, the quantization table of previous needs a modification. In Table 1, there are 54 coefficients located in the middle and lower part that are set to be one. They are p[0,4], p[0,5], p[0,6], p[0,7], p[1,3], p[1,4], p[1,5], p[1,6], p[1,7], p[2,2], p[2,3], p[2,4], p[2,5], p[2,6], p[2,7], p[3,1], p[3,2], p[3,3], p[3,4], p[3,5], p[3,6], p[3,7], p[4,0], p[4,1], p[4,2], p[4,3], p[4,4], p[4,5], p[4,6], p[4,7], p[5,0], p[5,1], p[5,2], p[5,3], p[5,4], p[5,5], p[5,6], p[5,7], p[6,0], p[6,1], p[6,2], p[6,3], p[6,4], p[6,5], p[6,6], p[6,7], and p[7,0] p[7,1], p[7,2], p[7,3], p[7,4], p[7,5], p[7,6], p[7,7]. Here p is the modified quantization table and p[a, b] is the value of the a^{th} row and b^{th} column element of p. Based on this quantization table, the secret messages can be reserved and the reconstructed image will not be too much distorted.

In the third phase, the secret message will be embedded in the middle and lower frequency part of the quantized DCT coefficients for each block O_i . Let C_i be the modified quantized DCT coefficients, and let C_i [a, b] denote the value of the a_{th} row and b_{th} column coefficients of the block C_i. Each coefficient in the middle and lower frequency part will embed one secret bits to increase the message load of the stego-image. This method embeds s_1 into LSB of C_1[0,4], s_2 into LSB of C_1[0,5], s_3 into LSB of C_1[0,6], s_4 into LSB of C_1[0,7], s_5 into LSB of C_1 [1,3], and so on. The embedding order is listed in Fig.1.

1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Table 2. Embedding sequence

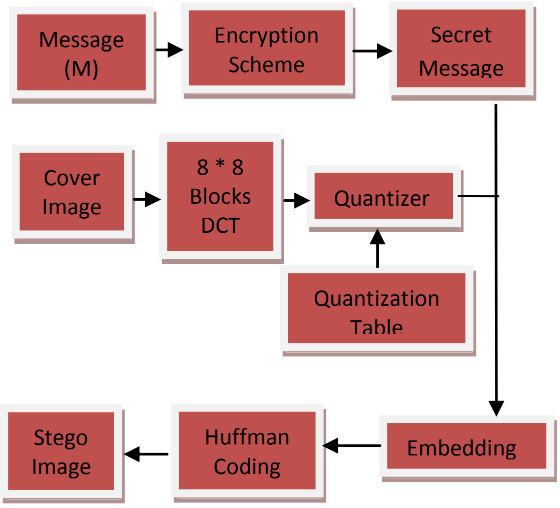


Figure 1. The block diagram of the embedding procedure

Algorithm of the embedding procedure

Input: A cover-image O, message M, and a secret key k.

Output: A stego-image E.

Step 1: Input a cover-image O. Suppose its size is N * N pixels. Partition the cover-image into non-overlapping blocks {$O_{1,}O_{2,}O_{3,}$ . . . ,$O_{N/8\ *N/8}$}. Each O_i contains 8 * 8 pixels [1].

Step 2: Use DCT to transform each block O_i into DCT coefficient matrix F_i, where F_i [a, b] = DCT(O_i[a, b]), where 1<=a, b<=8 and O_i[a, b] is the pixel value in O_i [1].

Step 3: Use modified quantization table p to quantize each F_i. The result can be represented as Ci[a, b] = truncate (F_i [a, b]/P[a, b]) [1].

Step 4: Apply an encryption method with secret key k to encrypt the message M. The resulted message is S = {s_1, $s_{2,}$

$s_{3,}$ . . . , $s_{m\}}$, where s_i is a secret bit and m is the length of S [1].

Step 5: Select C_i [a, b] to hide respectively, where [a, b] equals to [0,4], [0,5], [0,6], [0,7], [1,3], [1,4], [1,5], [1,6], [1,7], [2,2], [2,3], [2,4], [2,5], [2,6], [2,7], [3,1], [3,2], [3,3], [3,4], [3,5], [3,6], [3,7], [4,0], [4,1], [4,2], [4,3], [4,4], [4,5], [4,6], [4,7], [5,0], [5,1], [5,2], [5,3], [5,4], [5,5], [5,6], [5,7], [6,0], [6,1], [6,2], [6,3], [6,4], [6,5], [6,6], [6,7], and [7,0] [7,1], [7,2], [7,3], [7,4], [7,5], [7,6], [7,7], respectively.

Each C_i [a, b] embeds one secret bits into it.

Step 6: Apply JPEG entropy coding, which contains Huffman coding to compress each block C_i. Collect the above results and generate a JPEG file E that contains the quantization table p and all the compressed data [1].

Step 7: Transfer the secret key k and the JPEG stego-image E to the receiver.

79	0	-1	0	2	-2	-3	0
-2	-1	0	-3	-3	0	0	0
-1	-1	-2	2	0	-1	0	-1
0	-2	0	1	1	0	0	0
-1	-1	1	2	0	0	0	0
2	0	2	0	1	0	-1	0
-1	0	0	0	0	0	2	0
-1	0	0	0	0	3	0	0

Table 3. The Result of Quantizer

79	0	-1	0	2	-1	-3	0
-2	-1	0	-3	-2	1	0	0
-1	-1	-2	1	0	0	-1	0
0	-2	0	1	1	0	3	0
-1	-1	1	2	0	0	0	0
2	0	2	0	0	0	0	0
-1	0	0	0	-1	0	1	0
-3	0	2	0	0	4	0	0

Table 4. The Result of Block After Embedding

The Extracting Procedure

In our method, the extracting procedure contains three phases. The first phase is the JPEG entropy decoding, the second phase is the secret message extracting, and the last phase is the decryption of the secret message.

This method then imports the secret key k to the decryption method to decrypt the secret message. Finally, we achieve the extraction of the original message M. Figure 4.2.1 shows the extracting procedure.

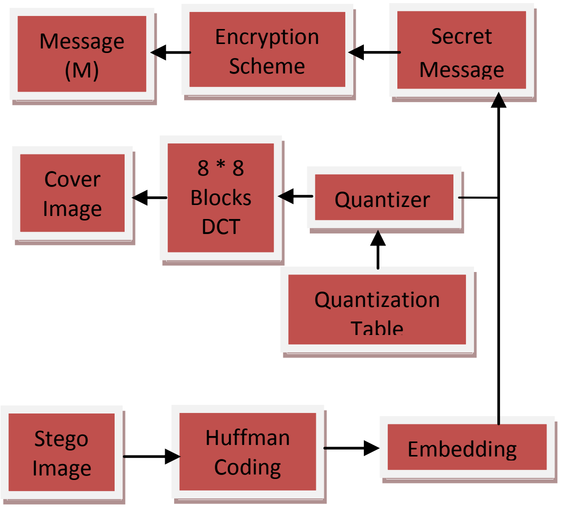


Figure 2. The block diagram of the extracting procedure

Extraction Algorithm.

Input**:** An $M_1 \times N_1$ Stego-image.

Output: Secret image.

1. Divide the stego-image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the stego-image.
2. The size of the encoded bit stream is extracted from 1st 8 × 8 DCT block by collecting the least significant bits of all of the DCT coefficients inside the 1st 8×8 block.
3. The least significant bits of all of the DCT coefficients inside 8×8 block (excluding the first) are collected and added to a 1-D array.
4. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
5. Construct the Huffman table by extracting the LSB of all of the DCT coefficients inside 8×8 blocks excluding first block and the block mentioned in step 3.
6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
7. End.

In this method, the capacity of message being embedded is increased, but image degrades since it is changing all DCT coefficient of each block.

Algorithm of the extracting procedure

Input: A stego-image E and a secret key k.

Output: The hidden message M.

Step 1: Use the first phase of JPEG decoding procedure to decompression the JPEG file. The decoding procedure contains Huffman decoding [1].

Step 2: Extract the secret message S from LSB of the 54 middle and lower frequency coefficients C_i[0,4], C_i[0,5], C_i[0,6], C_i[0,7], C_i[1,3], C_i[1,4], C_i[1,5], C_i[1,6], C_i[1,7], C_i[2,2], C_i[2,3], C_i[2,4], C_i[2,5], C_i[2,6], C_i[2,7], C_i[3,1], C_i[3,2], C_i[3,3], C_i[3,4], C_i[3,5], C_i[3,6], C_i[3,7], C_i[4,0], C_i[4,1], C_i[4,2], C_i[4,3], C_i[4,4], C_i[4,5], C_i[4,6], C_i[4,7], C_i[5,0], C_i[5,1], C_i[5,2], C_i[5,3], C_i[5,4], C_i[5,5], C_i[5,6], C_i[5,7],C_i[6,0], C_i[6,1], C_i[6,2], C_i[6,3], C_i[6,4], C_i[6,5], C_i[6,6], C_i[6,7], and C_i[7,0], C_i[7,1], C_i[7,2], C_i[7,3], C_i[7,4], C_i[7,5], C_i[7,6], C_i[7,7], where 1 <= i <= (N/8 * N/8). Collect those secret bits to regenerate the secret message S

Step 3: Import secret key k to the decryption method to decrypt the secret message S and reconstruct the original message M [1].

III. Results

A block can embed 54 secret bits into it in our method, and thus a cover image of 417 * 417 pixels can embed 54 * (417 * 417)/(8 * 8) = 146718 secret bits into it. In the Jpeg–Jsteg method, however, the message capacity can be inferred from the number of the quantized DCT coefficients whose values are not 0, 1, or -1. Because the DCT coefficients after the quantization are almost all zeros, the message capacity of Jpeg–Jsteg is very much limited.

Methods/Image	Leena	Baboon
Proposed method	146718 bits	146718 bits
Chang,Chen,and Chung method	141284 bits	141284 bits
Jpeg-Jsteg	49798 bits	53142 bits
Biswas, Sarkar, and Sarkar	173889 bits	173889 bits

Table 5. Capacity (bits) Comparison

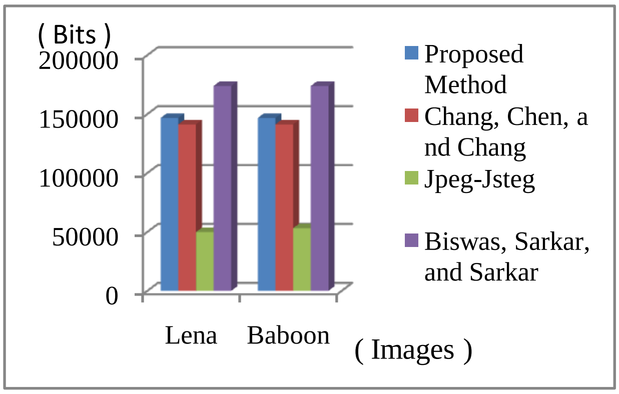


Figure 3. Capacity (bits) Comparision

However, the stego-image size of the proposed image is quite restricted. It cannot be adjusted freely based on the choices of quantization tables, like what we can do with JPEG. This is because, in our method, we set the coefficients to be the ones in the middle and lower part of the quantization table. Thus the quantized DCT coefficients in the middle and lower frequency part will not be zero even if we choose another quantization table to quantize the DCT coefficients. Thus our method can only compress the downright part of the quantized DCT coefficients.

Table 6. The comparison of PSNR values.

Methods/Images	Leena	Baboon
Proposed method	40.83 db	32.54 db
Jpeg-Jsteg	39.10 db	30.63 db
Chang,Chen,and Chung method	38.67 db	28.38 db
Biswas, Sarkar, and Sarkar	38.40 db	30.75 db

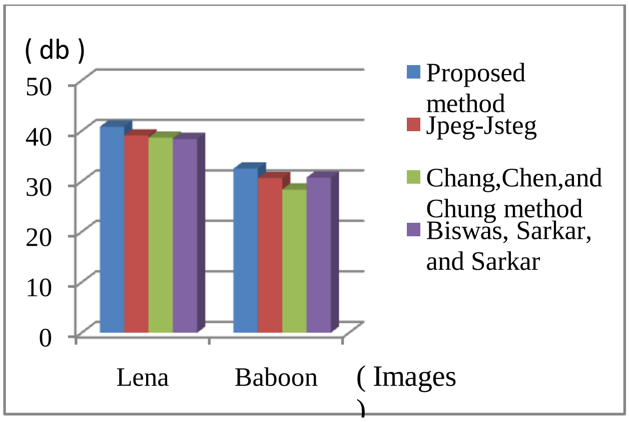
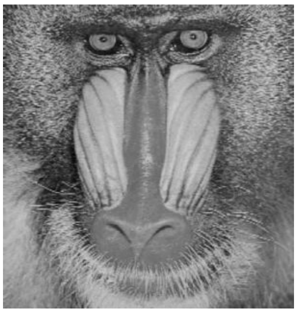
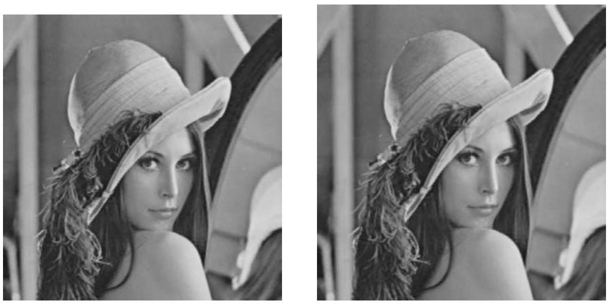


Figure 4. PSNR Values Comparision



(b)

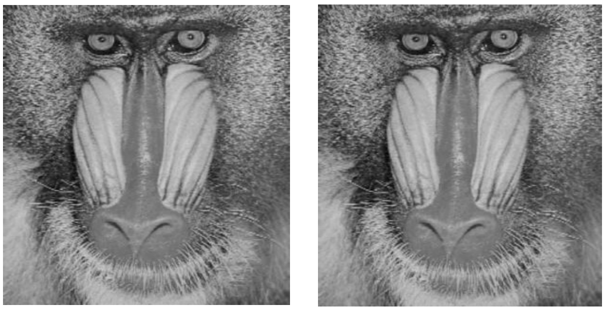
Figure 5. Original Image (a) Baboon (b) Leena



a) PSNR = 40.83 of proposed method

b) PSNR = 39.10 of Jpeg-Jsteg

Figure 6. Stego image Lena PSNR Comparison



a) PSNR = 32.54 of proposed method

b) PSNR = 30.63 of Jpeg-Jsteg

Figure 7. Stego image Baboon PSNR comparison

IV. Conclusion

The goal of data hiding is to avoid peepers from discovering the secret messages embedded in the cover-images. In Jpeg–Jsteg, only few messages can be embedded in the cover-image. To improve the capacity of hidden message, we propose a new steganographic method to increase the message load in every block of the stego-image while keeping the stego-image quality acceptable. In our method, the secret message is embedded in the middle and lower frequency part of the quantized DCT coefficients.

Our experimental results show the proposed method provides acceptable image quality and a large message capacity. Overall, the proposed method matches the requirement of steganography with a larger message capacity and good image quality . Our proposed method has larger message capacity than Jpeg-Jsteg method described in 3.1 and Chang, Chan and Chung Method described in 3.2. Our method has lower message capacity than Biswas, Sarkar , and Sarkar method described in 3.3. but image quality of our method is better than all methods described in the dissertation as shown in the Table 5.1.2 of PSNR values. Since image quality is better than others, our goal is achieved.

V. Future work

Steganographic method proposed in the dissertation although provides a good quality stego-image. Perhaps, we can improve image quality and message capacity by breaking the image into 16 * 16 blocks instead of 8 * 8 blocks . This may be because if block is larger in size on which DCT applied, so changing middle and lower coefficient will affect the image quality least since most of the information for image pixels is in the lower frequency part of the DCT function and coefficient corresponding to these is in upper part of 16 * 16 matrix. These coefficients are not being changed in our algorithm. One more limitation of this method is that it is useful only for gray scale images not for true colour (RGB) images. For these , 3-D block can be used

VI. References

[1] C.-C. Chang, T.-S. Chen and L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification", *Information Sciences*, vol. 141, 2002, pp. 123-138.

[2] Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001, vol. 3, pp. 61-76.

[3] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999, vol. 22, pp. 322-330.

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004, vol. 47, number 10, pp. 76-82.

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Area in Communications*, May 1998, vol. 16, pp. 474-481.

[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transaction on image processing, 8:08*, 1999, vol. 3, pp. 13-17.

[7] N. F. Johnson and S. Katzenbeisser, A survey of steganographic techniques., in S. Katzenbeisser and F. Peticolas (Eds.): *Information Hiding*, pp.43-78. Artech House, Norwood, MA, 2000, vol. 8, number 9.

[8] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001, vol. 9, number 9078.

[9] Simmons, G., "The prisoners problem and the subliminal channel", *CRYPTO*, 1983,vol. 24, pp. 653-660.

[10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003, vol. 16, number 3, pp. 260-276.