A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity

Arup Kumar Pal[1], Kshiramani Naik[1], and Rohit Agarwal[2]
[1]Department of Computer Science and Engineering, Indian Institute of Technology(ISM), India
[2]Department of Computer Science and Engineering, JSS Academy of Technical Education, India

Abstract: *Joint Photographic Experts Group (JPEG) is one of the widely used lossy image compression standard and in general JPEG based compressed version images are commonly used during transmission over the public channel like the Internet. In this paper, the authors have proposed a steganography scheme where the secret message is considered for embedding into the JPEG version of a cover image. The steganography scheme initially employs block based Discrete Cosine Transformation (DCT) followed by some suitable quantization process on the cover image to produce the transformed coefficients. The obtained coefficients are considered for embedding the secret message bits. In general, most of the earlier works hide one bit message into each selected coefficient, where hiding is carried out either directly modifying the coefficients, like employing the LSB method or indirectly modifying the magnitude of the coefficients, like flipping the sign bit of the coefficients. In the proposed scheme, instead of embedding the secret message bits directly into the coefficients, a suitable indirect approach is adopted to hide two bits of the secret message into some selected DCT coefficients. As per the conventional approach, the modified coefficients are further compressed by entropy encoding. The scheme has been tested on several standard gray scale images and the obtained experimental results show the comparative performance with some existing related works.*

Keywords: *Chi-square attack; (DCT); Histogram; (JPEG); statistical steganalysis; steganography*.

Received May 27, 2015; accepted October 19, 2015

1. Introduction

The Internet is one of the most popular and the easiest medium for transmission of digital data among people, but one of the common threats during transmission is that anybody can access these data and Internet itself does not provide any protection on these data. Meanwhile, the sender prefers to adopt some security mechanisms on these digital data to protect them from being accessed by illegitimate users. To protect the confidentiality of the data, in general, two approaches are mainly used, i.e., cryptography [15] and steganography [17]. In cryptography, the encryption process transforms the secret data, i.e., known as plain text into cipher text using an encryption key. The cipher text appears as unreadable form; only the decryption process of the cryptography can convert the cipher text into the original or plain text from using the decryption key. In cryptography, its main concern is that the illegitimate users should not able to decrypt the cipher text into plain text without knowing the decryption key. However, in cryptography, the cipher text resembles into an unreadable form, so it attracts the opponent to exploit the content of the cipher text by employing some cryptographic attacks [16, 18]. In cryptography, we cannot avoid such type of brute force attack. There is another approach, i.e., known as steganography, can divert the opponent's attention to employ any brute force attack on the secret data. The word, steganography, derived from the Greek word Steganos means covered or secret and graphic means writing or drawing. Its objective is to hide the secret data into some other unsuspected cover media so that the secret data will be visually imperceptible. Steganography hides the secret message within cover media, where the cover media may be audio, video, text or an image. The media that is looking inoffensive can be used as the cover media in which the secret data are embedded. After embedding the secret data into the cover media, the obtained media is known as stego media. The common intention of any steganography technique is to embed the maximum number of secret message bits into the cover media in such a way that both the cover media and the stego media do not differ in large extent against human visual perception. To enhance the security level, sometimes the secret data are encrypted by the conventional cryptography approach prior to embedding into any cover media [2]. In latest, the steganography schemes based on the cover media like images have gained lots of research interest due to its frequent used in the Internet based applications. The secret data embedding into image can be realized into two domains, i.e., spatial domain and transform domain. In the spatial domain [3, 11, 23] based steganography scheme, the secret data are embedded into the cover image by directly modifying each pixel value of the cover image itself. The most common and simplest steganography approach in the

spatial domain is the Least Significant Bit (LSB) substitution method [3]. Some other substitution methods have been proposed by enhancing the conventional LSB substitution such as Local Pixel Adjustment Process (LPAP) [19], Optimal Pixel Adjustment Process (OPAP) [3] etc., Several authors have enhanced the embedding capacity of spatial domain based steganography further by exploiting the image data. In [10], the authors have used OPAP along with genetic algorithm to enhance the embedding capacity of the cover image where in [7], the authors have exploited the edge property of the cover image in order to enhance the hiding capacity. In spatial domain based steganography schemes, the secret message are hidden into the uncompressed cover image. In literature, another category of steganography schemes [1, 5, 6, 12, 20, 24] can be realized in transform domain of the cover image. Generally, the spatial domain based steganography scheme performs superior to the transform domain based steganography in terms of embedding capacity still several transform domain based steganography schemes have been proposed in literature. The reason is that nowadays, before transmission of the data over the communication channel, generally, the compressed version of the data set are preferred for efficient communication and storage. It has been found that in case of image data, the transformation tools like Discrete Cosine Transformation (DCT), Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) etc., are highly suitable to exploit the presence of redundancy in the data set. So in the transform domain based steganography, the secret data can be embedded into the compressed version of the cover image. In this category of steganography schemes, initially the cover image is transformed using any suitable transformation tools like DCT, SVD, DWT etc., and subsequently the secret data are embedded after modifying the selective transformed coefficients. In this paper, we have studied on the Joint Photographic Experts Group (JPEG) cover image based steganography scheme since the JPEG image is one of the mostly used compressed version of the image over the internet. The embedding procedure of the secret data into the quantized DCT coefficients are realized in two ways, i.e., directly inserting secret message into the quantized DCT coefficients using LSB methods [3] or indirectly by modifying the quantized DCT coefficients based on the type of secret message bits. In steganalysis, it has been observed that the indirect steganography mechanism is superior to direct steganography mechanism, due to its resisting capability against some statistical attacks [8, 13, 21, 25, 26]. Still now, most of the JPEG based steganography schemes embed one bit of secret data into per quantized DCT coefficients through indirect message embedding mechanism. Although in [4], the embedding capacity in terms of per coefficient is two bits but it provides low visual quality of stego image due to consideration of direct secret message bits embedding approach. Also, another constraint in the JPEG based steganography is the limited number of non zero quantized DCT coefficients. The embedding capacity can be further improved if the number of non zero quantized DCT coefficients is increased and two bits of secret data can be embedded into per quantized DCT coefficients by indirect embedding approach. In this paper, we have suggested a steganography scheme which embeds two bits of the secret message indirectly into per quantized DCT coefficients.

The rest of the paper is organized as follows. Section 2 describes in brief some related JPEG based steganography schemes. The proposed scheme, including the embedding and the extraction process, is presented in section 3. The experimental results are furnished in section 4. Finally, the conclusions are drawn in section 5.

2. Related Works

Several steganography schemes based on the JPEG compressed image data, are found in literature like JSteg [9], F5 [22], OutGuess [14], the proposed scheme by Chang *et al.* [4] and the proposed scheme by Liu and Liao [12]. In this section, we will discuss in briefly all these schemes with their merits and demerits. JSteg steganography scheme was the first publicly available steganography scheme which is devised on JPEG compressed image data. In embedding process, it embeds the secret message bits sequentially into the Least Significant Bits (LSB) of some selected quantized DCT coefficients along the zigzag scanning order. Those coefficients having value 0, 1, or -1 are not considered for embedding of the secret message bits for avoiding the shrinking effects [12] where the shrinkage effect occurred due to the modification of the quantized DCT coefficients those having the absolute value of 1 and -1 into zero. The embedding capacity of JSteg is found low due to the presence of less number of permissible carriers quantized DCT coefficients for transmitting or embedding the secret message bits. To increase the number of nonzero quantized DCT coefficients, Chang *et al*. [4] used a modified quantization table during JPEG based image compression. It has been found that the number of non zero quantized DCT coefficients are increased when the DCT coefficients are quantized using the modified quantization table. Therefore, in their proposed scheme more number of secret message bit can be embedded into the quantized DCT coefficients. Moreover, Westfeld and Pfitzmann [21] noticed that steganographic scheme that modifies the coefficients sequentially using the LSB methods, does not survive against some statistical steganalysis like chi-square family attacks [21]. Both the JSteg and the proposed scheme of Chang et al. are not suitable to

resist against chi-square family attacks since both the schemes used LSB substitution method for embedding the secret message bits sequentially into the quantized DCT coefficients. In order to avoid chi-square attack, the OutGuess steganography scheme embeds the secret message bits into quantized DCT coefficients non-sequentially by replacing the LSB bits of the quantized DCT coefficients. In addition, the OutGuess method uses only a half of the permissible quantized DCT coefficients to embed the secret message bits so it has embedding capacity about half of the JSteg. So the steganographic schemes like JSteg, the proposed scheme of Chang *et al*. [4] and OutGuess all are based on the direct modification of the quantized DCT coefficients by using LSB substitution methods for embedding the secret message bits. In this respect, some indirect embedding mechanisms for transmitting or embedding the secret message bits through the quantized DCT coefficients were proposed in literature. Among them, F5 is one the of popular steganographic scheme where they have not used LSB substitution method for embedding the secret message bits. In F5, Instead of using LSB substitution, the quantized DCT coefficients absolute value is decremented by one in case of the secret message bit is not matched with the corresponding quantized DCT coefficients LSB value; otherwise no need to change the absolute value of the quantized DCT coefficient. The F5 is able to resist chi-square attack and also has higher embedding capacity than the JSteg steganography scheme. But it suffers from the shrinkage effect and the receiver cannot distinguish a zero value coefficient whether it is steganographically unused or produced due to the modification of the absolute value of 1 and -1. This problem was sorted out by Liu et al. by using the complementary embedding scheme to embed the secret data into the quantized DCT coefficients. In their system, the embedding process are carried out in two phases wherein the beginning phase, half of the permissible quantized DCT coefficients are changed based on the flow diagram as presented in Figure 1. The rest of the coefficients are modified in similar fashion, but instead of performing the subtraction operation, they had performed the increment operation on some quantized DCT coefficients based on the secret message bits. The proposed scheme of Liu and Liao [12] is capable to resist against various steganalysis attacks. The main limitation of all the mentioned JPEG based steganographic schemes is that only a single bit secret message is allowed to embed into each permissible quantized DCT coefficients. In the following section, we will suggest a JPEG based steganography scheme where the proposed scheme is able to embed two bits of secret message through each permissible quantized DCT coefficients and also capable to resist against some steganographic attacks.

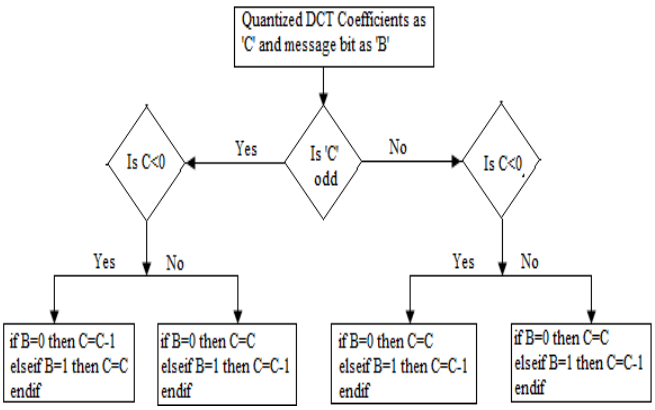


Figure 1. The embedding process of the proposed scheme of Liu and Liao [12].

3. Proposed Method

In this section, we have presented the proposed steganography scheme where the JPEG bit stream of a cover image is considered for carrying or embedding the secret message bits. As discussed earlier, the existing JPEG based steganography schemes do not provide the high embedding capacity and also inferior against some steganography attacks. Among them, Liu and Liao [12] proposed work furnishes better performance compared to the earlier proposed works in terms of defending against some steganography attacks. However, the proposed work of Liu and Liao [12] is capable to embed a single bit secret message through each permissible quantized DCT coefficients of a cover image. In this paper, in order to improve the embedding capacity, initially we have increased the number of non-zero quantized DCT coefficients by employing the modified quantization Table [4] during the quantization process of a DCT transformed cover image and subsequently two bits secret message is considered for embedding into each permissible quantized DCT coefficients of a cover image. The modified quantization table is redefined from the standard quantization table by incorporating variable Scaling Factor (SF). In [4], the authors have considered the Scaling Factor (SF) in such a way that the high visual quality of the reconstructed image from the JPEG bit stream would be maintained. Here the modified quantization table is obtained based on Equation (1).

$$Q'_{x,y} = \left\lfloor \frac{Q_{x,y}}{SF} \right\rfloor \quad (1)$$

Where $Q_{x,y}$ and $Q'_{x,y}$ denotes the quantization value at position *(x, y)* of the conventional quantization table and the modified quantized table respectively. The modified quantized table and the modified zigzag scanning order for selecting the coefficients are presented in Table 1 and Figure 2 respectively. The embedding and extraction procedure of the proposed

steganographic scheme is elaborated in the following sections.

Table 1. Modified quantization table.

16	11	10	16	1	1	1	1
12	12	14	1	1	1	1	55
14	13	1	1	1	1	69	56
14	1	1	1	1	87	80	62
1	1	1	1	68	109	103	77
1	1	1	64	81	104	113	92
1	1	78	87	103	121	120	101
1	92	95	98	112	100	103	99

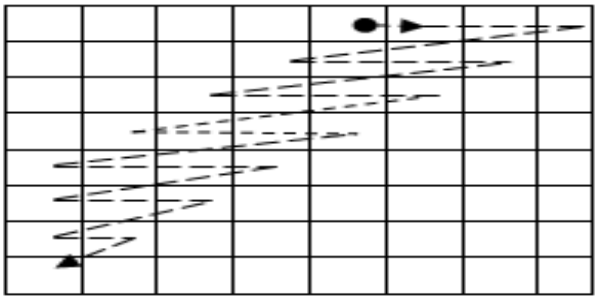


Figure 2. Modified zigzag scanning order.

3.1. Embedding Process

The schematic diagram of the embedding process is shown in Figure 3 where the embedding process is carried out in three major phases. In the first phase, before embedding the secret message into the cover media, the secret message is encrypted by employing any suitable standard data encryption algorithm like Data Encryption Standard (DES) [15], Advanced Encryption Standard (AES) [15] etc. This process enhances the security level of the secret message, but in general this phase is considered as the optional or additional process in any steganography scheme. The second phase is mainly concerned with the transformation of the cover image by DCT followed by employing the suitable quantization process on the DCT coefficients. All the obtained non-zero quantized DCT coefficients excluding 1 and -1 from the earlier phase are used to transmit or to embed the encrypted secret message bits in the final phase. The details of the three phases are given below.

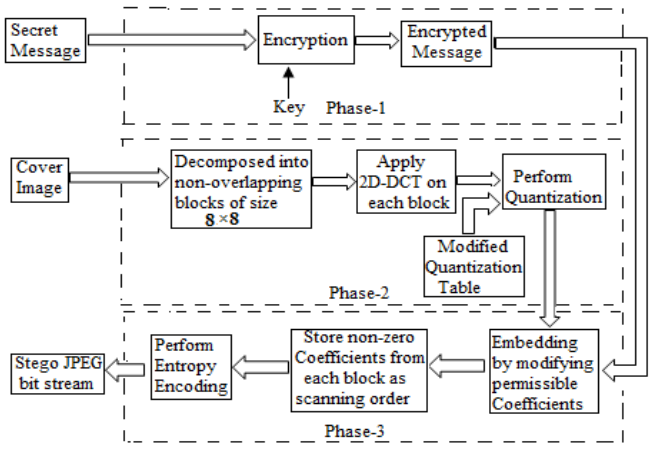


Figure 3. The block diagram of embedding process.

- *Phase 1*: In this phase initially the secret message is encrypted by any standard data encryption algorithm. The encrypted message is further converted into a binary bits sequence and from this sequence, we have chosen two bits message for embedding into each permissible quantized DCT coefficients. The steps of this phase are as follows:
- *Step Em_P1.1*: Encrypt the secret message *M*, by a secret key, *K* into an encrypted bit sequence *S*, such that $S = EncAlgo_K(M)$, where $EncAlgo(\bullet)$ denotes the encryption process with secret key, K.
- *Step Em_P1.2*: Represent the encrypted bit sequence *S* into a set of numbers such that, $S = \{S_1, S_2, \ldots, S_n\}$, where each number, S_i is consist of two bits sequence i.e. B_{2i-1}, B_{2i} from *S*.
- *Phase 2*: In the second phase, the input gray scale cover image, CI is decomposed into non-overlapping blocks of size 8×8 and subsequently each block is individually transformed by employing block based 2D-DCT. Each block produces 64 DCT coefficients that are subsequently quantized by using the modified quantization table as shown in Table 1. It has been observed that most of the energy of the transformed image block is concentrated towards the low frequency sub-band and human visual perception is highly sensible to this region. To embed the secret data in the low frequency region can degrade the visual quality of the constructed stego image. In general, it has been found that the embedding or modification of the middle band-frequency of the transformed image block produces less distortion on the visual quality of the reconstructed stego image from the compressed version of the stego-image. In this paper, we have considered the middle band coefficients from each block for embedding the encrypted message. However to avoid the shrinkage effect, instead of embedding the encrypted message into all the non-zero quantized DCT coefficients, the encrypted message is preferred to embed into the coefficients those have not values -1 and 1. The quantized DCT coefficients those are chosen for embedding the encrypted message are termed as the permissible quantized DCT coefficients. The steps of this phase are summarized as follows:
- *Step Em_P2.1*: Decompose the cover image CI into non overlapping blocks of size 8×8.
- *Step Em_P2.2*: Transform each block into DCT coefficients by employing 2D- DCT.
- *Step Em_P2.3*: Quantize the DCT coefficients using the modified quantization table as shown in Table 1 and round off the quantized coefficient value to the nearest integer value, C.
- *Step Em P2.4*: Select the sequence of quantized DCT coefficients from each block as the zigzag scanning order as shown in Figure 2. Choose the

permissible quantized DCT coefficients from the sequence by discarding the quantized DCT coefficients those having value -1, 0 and 1.

- *Phase 3*: In the last phase, two bits of the encrypted bit sequence from *S={S1,S2,.....,Sn}* are embedded into each permissible quantized DCT coefficients according to rules as shown in the Figure 4. After completion of the embedding process, the DCT coefficients are further encoded by suitable entropy encoding. The steps of this phase are described as follows:
- *Step Em_P3.1*: Embed two bits of encrypted message say, from bit sequence S into the permissible quantized DCT coefficient according to the proposed embedding rules as shown in Figure 4.
- *Step Em_P3.2*: Perform the entropy encoding on the DCT coefficients to obtain the JPEG stego-image.

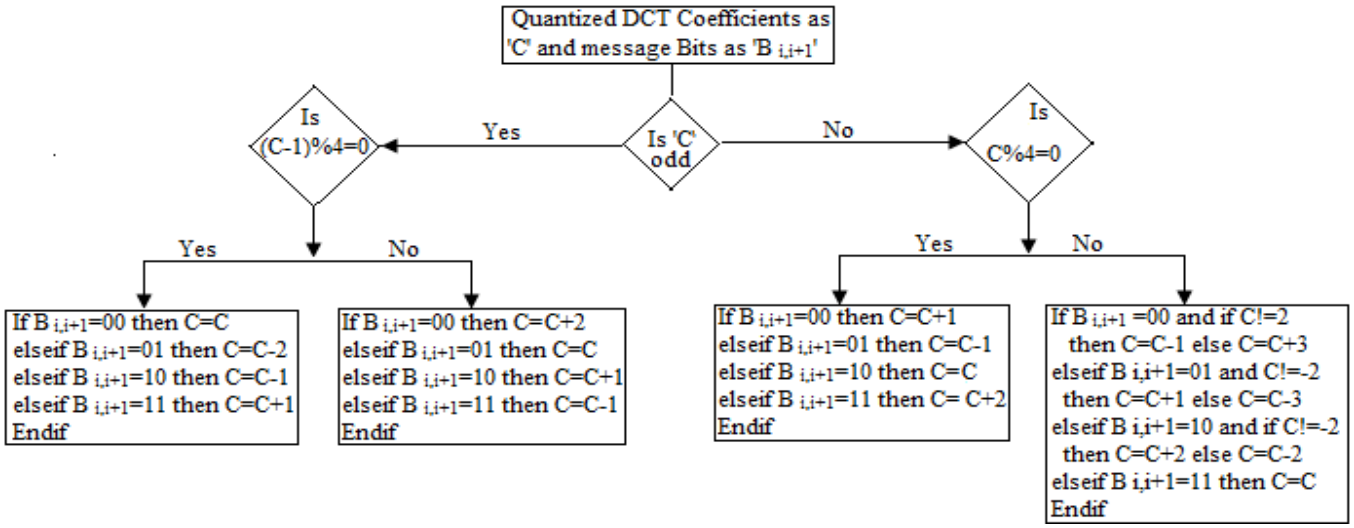


Figure 4. The tree representation of the embedding rules.

3.2. Extraction Process

The schematic diagram of the extraction process is shown in Figure 5 where the extraction of the secret message from the received stego JPEG bit stream has done in two major phases. The details of the proposed extraction process are furnished below:

- *Phase 1*: In this phase, after receiving the stego JPEG bit stream, the entropy decoding is done to recover the quantized DCT coefficients and subsequently the middle band coefficients are identified. The major steps of this phase are as follows:
- *Step Ex_P1.1*: Perform entropy decoding on stego JPEG bit stream to recover the quantized DCT coefficients.
- *Step Ex_P1.2*: Reshape the quantized DCT coefficients into blocks of size 8×8 by appending required numbers of zeros.
- *Step Ex_P1.3*: Traverse the middle band quantized DCT coefficients according to the modified zigzag scanning order as shown in Figure 2 and subsequently, stores the quantized DCT coefficients those do not belong to -1, 0 and 1.
- *Phase 2*: In the second phase, the bit- sequence of the encrypted message is extracted from the middle band coefficients followed by decryption on the extracted bit- sequence to recover the original message. The steps of this phase are given below:
- *Step Ex_P2.1*: Extract the encrypted message bit-sequence, S from the quantized DCT coefficients obtained through Step Ex_P1:3 by checking the condition given in Figure 6.
- *Step Ex_P2.2*: Decrypt the encrypted message bit-sequence, *S* by the secret key, *K* into the secret message, *M* such that $M = DecAlgo_k(S)$, where $DecAlgo(\bullet)$ denotes the decryption process.

The proposed scheme is further explained with a suitable example where we have taken a 8×8 sub image block as shown in Table 2 and the intermediate modification of the sub image block are shown in Tables 3, 4, and 5.

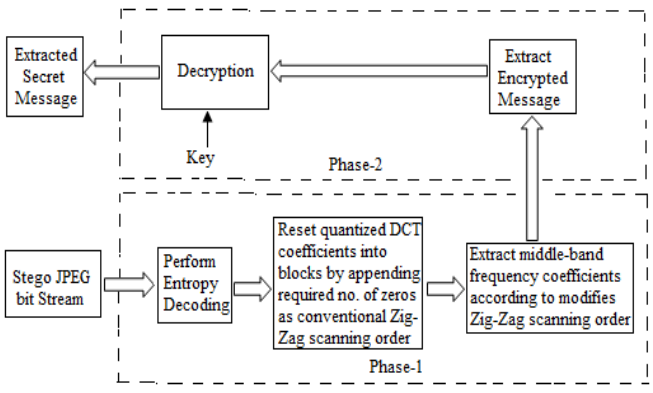


Figure 5. The block diagram of the extraction process.

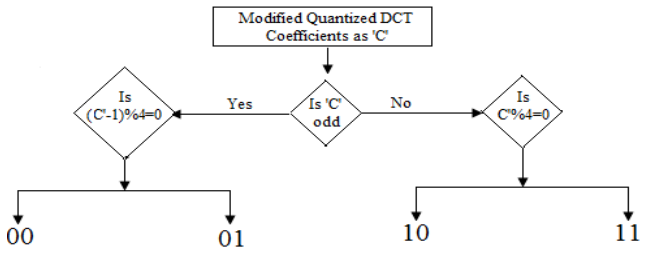


Figure 6. The tree representation of the extraction rules.

Table 2. 8×8 block of an image.

168	163	159	154	152	148	146	142
134	127	126	115	112	106	100	94
90	84	79	71	71	67	66	94
68	69	69	72	80	84	91	101
110	120	120	128	137	139	149	154
165	173	170	176	180	182	182	185
184	191	185	187	189	186	184	180
177	177	174	171	164	162	154	149

Table 3. DCT coefficients of 8×8 block of an image.

108.1.9	10.0	2.20	2.70	1.10	-4.10	-2.90	0.90
-196.0	23.8	8.40	2.60	1.60	3.006	3.60	4.90
168.7	62.2	-8.0	5.20	-3.0	4.10	2.50	-0.3
189.7	-27.8	-3.5	-1.9	1.0	-2.30	-3.7	-1.5
-19.1	-23.9	3.30	-3.3	1.90	0.30	0.2	-0.8
-0.8	-9.0	0.39	0.90	1.30	-1.50	-1.20	-0.50
-5.90	7.20	1.50	1.0	0.30	0.70	0.70	-1.30
5.40	3.10	-0.9	0.70	-1.2	0.20	-3.1	1.10

Table 4. Quantized DCT coefficients by using modified quantization table.

69	1	0	0	1	-4	-3	1
16	2	1	3	2	3	4	0
13	4	-1	5	0	4	0	0
15	-28	-4	-2	1	0	0	0
-29	-24	3	-3	0	0	0	0
-1	-1	0	0	0	0	0	0
-6	7	0	0	0	0	0	0
5	0	0	0	0	0	0	0

$$\text{Message} = (10100101101010101001001110101010100111)_2$$

Table 5. Modified quantized DCT coefficients after embedding the secret message.

68	1	0	0	1	-4	-4	1
17	2	1	3	3	3	4	0
12	5	-1	4	0	4	0	0
14	-26	-5	-3	1	0	0	0
-18	-24	4	-4	0	0	0	0
-1	-1	0	0	0	0	0	0
-4	7	0	0	0	0	0	0
6	0	0	0	0	0	0	0

4. Experimental Results

In this section, the experimental results are presented to evaluate the performance of the proposed steganography scheme. We have executed the proposed scheme on a set of standard grayscale test images, but in this paper, we have presented the simulation results for eight images of sizes 512×512 as shown in Figure 7 where the chosen image data set contents some promising varying texture property of the images. In steganography, the first concerned issue is preserving visually high- quality stego image. As in the proposed scheme, we are not embedding the secret message directly into the cover image, where the secret messages are embedded by modifying the quantized discrete cosine transformed coefficients of the cover image and these modified coefficients are further encoded by employing any suitable entropy encoding to obtain the compressed data set.

a) Lena. b) Tiffany. c) Barbara. d) Boat.

e) Goldhill. f) Mandrill. g) Peppers. h) Zelda.

Figure 7. The Cover images used in our experiments.

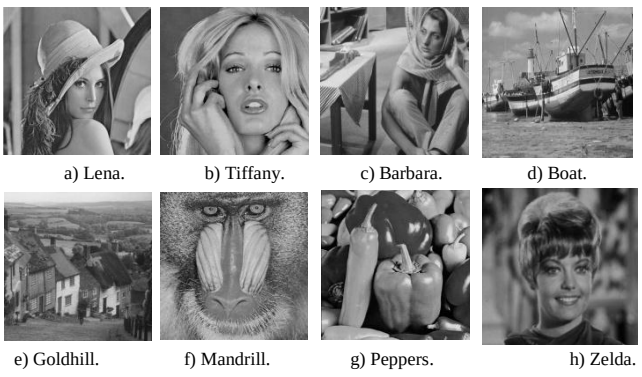
This compressed data set is considered as a compressed version of the stego image where the receiver can extract the secret message from the compressed data set. Since the opponent can access the compressed data set from the public channel; in this case after decompression process if the opponent obtains a highly visual quality meaning full image data from the compressed data set then it will fulfil the goal of the steganography. Figure 8 shows visually high quality reconstructed images from the stego JPEG bit-stream where the human visual perception is not capable to distinguish between the reconstructed stego image and the corresponding original image. We also computed the Peak Signal to Noise Ratio (PSNR) for stego-images to show the effectiveness of the proposed scheme over some other related steganographic schemes. The comparative detail in terms of PSNR values are presented in Table 6. The proposed scheme achieved reasonably good PSNR values compared to the existing related works. The second important issue of the steganography is to preserve the high embedding capacity of the secret message without distorting the cover media significantly. In the proposed scheme, two bits encrypted message are embedded into each permissible quantized DCT coefficients. Table 7 shows the comparative study of the proposed scheme with some existing related JPEG based steganography schemes in terms of embedding capacity or estimation. It can be revealed that the proposed scheme has higher embedding capacity than the existing schemes. In addition, we have also studied the histogram analysis and chi-square family attacks under the statistical steganalysis. In steganography, the objective of histogram analysis is to show the disparity between the original cover image and the stego-image. In this paper, the histogram analysis is carried out especially

in two domains, i.e., in the spatial domain and in transform domain respectively. In the spatial domain, a histogram is statically representation of an image to show the visual impression of the distribution of the pixel values. The height of histogram at a particular interval of pixel shows the frequency density of that interval. In case of transformed domain, we basically plot the occurrence of quantized DCT coefficients of the stego- media to exhibit the histogram. Since the proposed scheme is the improvement of the Liu et al. scheme, so in this paper, we have presented the histogram analysis regarding the proposed work of Liu and Liao [12] Figure 9 depicts the histograms of the reconstructed images obtained from the compressed JPEG bit stream. It can be observed that the histogram obtained from the proposed scheme is almost similar to the original cover image. The histograms obtained from the transformed domain are presented in Figure 10 where it conveys that less distortion occurred in the proposed scheme compared to the Liu and Liao [12] scheme. Chi-square attack is mainly found in LSB based steganography where it detects the existing of the secret message from the stego-image based on the variation of the Pair of Values (PoVs) in the stego-image. The variation of PoVs for any image is observed in the following manner. Suppose X_k and Y_k are the occurrence of the frequency for pixel value $2k$ and $2k+1$ respectively, for $k=0, 1, 2,..., 127$. Now if D_k denotes the difference of pixels values for $2k$ and $2k+1$ of any image, then D_k is computed from Equation (2).

$$D_k = abs(X_k - Y_k) \quad (2)$$

Where $abs(\bullet)$ implies the absolute value.

We have plotted the values of D_k for Lena image as well as for the stego-image obtained from the different steganography schemes as shown in Figure 11. It can be observed that the variation of D_k for both the cover image and the stego-image obtained from the proposed scheme are almost similar. So the proposed method can resist the chi-square attack. A comparative study has been given as shown in Table 8 to show the superiority of the proposed scheme over other mentioned schemes.



a) Lena. b) Tiffany. c) Barbara. d) Boat.

e) Goldhill. f) Mandrill. g) Peppers. h) Zelda.

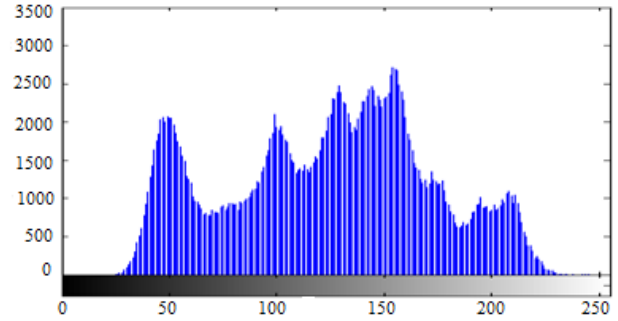
Figure 8. Reconstructed stego images by our proposed scheme.

Table 6. The PSNR values of various steganography schemes.

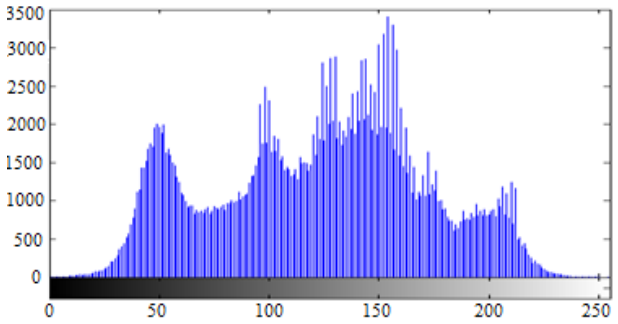
Cover Image	Method					
	JSteg [9]	F5 [22]	OutGuess [14]	Chang *et al.* [4]	Liu and Liao [12]	Proposed
Lena	36.36	36.94	36.37	33.84	35.67	39.09
Peppers	35.45	35.86	35.32	32.98	34.75	37.59
Boat	35.67	36.13	35.47	33.29	34.53	38.74
Barbara	32.51	32.83	32.10	31.13	26.41	34.27
Goldhill	33.02	35.40	35.12	31.78	33.03	37.17
Zelda	38.31	38.32	38.22	36.45	37.64	40.86
Mandril	27.86	28.13	27.89	27.63	23.25	30.10
Tiffany	35.93	36.36	35.81	33.12	35.07	35.29
Average	34.39	35.00	34.54	32.53	32.54	36.64

Table 7. Comparisons of various steganography schemes in terms of embedding capacity.

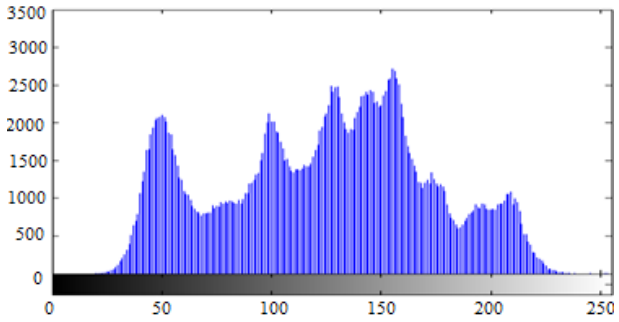
Cover Image	Method					
	JSteg [9]	F5 [22]	OutGuess [14]	Chang *et al.* [4]	Liu and Liao [12]	Proposed
Lena	32998	33026	16375	104578	44131	104578
Peppers	33295	34074	17016	110750	46346	110750
Boat	38374	38506	19105	105578	50042	105578
Barbara	45363	45513	22699	105600	59229	105600
Goldhill	45196	45505	22639	125176	60890	125176
Zelda	27557	27630	13724	89514	37086	89514
Mandril	75751	75837	37867	152302	98989	152302
Tiffany	31674	31516	15729	118184	43300	118184
Average	41267	41451	20644	113960	55001	113960



a) Histogram of original image.

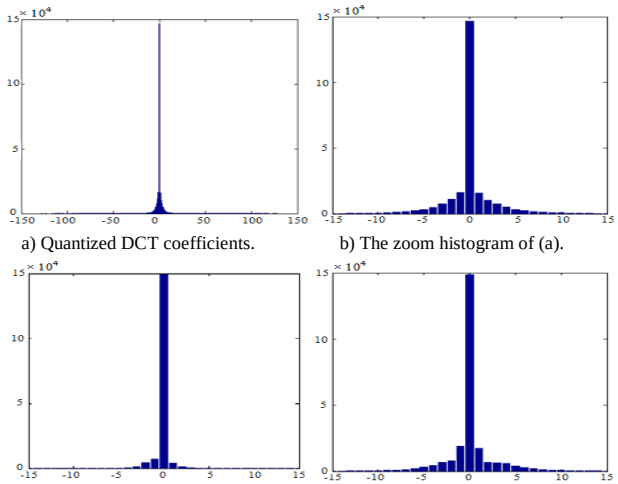


b) Histogram of the stego- image obtained From Liu and Liao [12] scheme.



c) Histogram of the stego- image obtained from the proposed scheme.

Figure 9. Results on Lena image.



a) Quantized DCT coefficients. b) The zoom histogram of (a).

c) Quantized DCT coefficients after applying Liu and Liao [12]. d) Quantized DCT coefficients after applying the proposed scheme.

Figure 10. The histogram of Lena image.

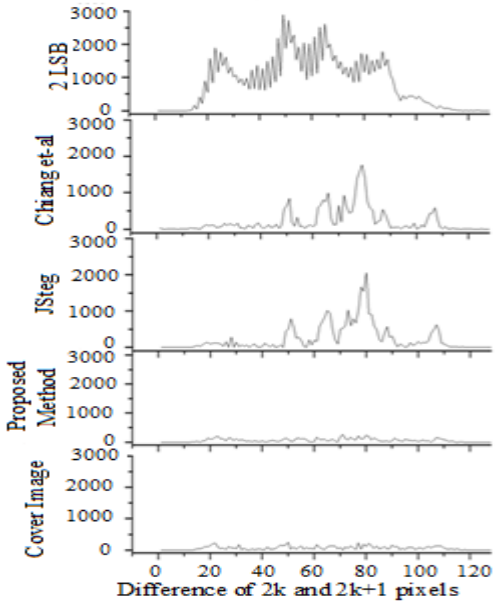


Figure 11. Frequency Vs difference of pixel value between 2k and 2k+1 for Lena image.

Table 8. Comparative study table.

Schemes	Various Parameters			
	Resistant to Chi-square	Capacity (in bits) per coefficient	Average PSNR > 35db	Resistant to Shrinkage effect
JSteg [9]	×	1	×	√
OutGuess [14]	√	$\frac{1}{2}$	×	√
F5[22]	√	1	√	×
Chang *et al.*[4]	×	2	×	×
Liu and Liao [12]	√	1	×	√
Proposed	√	**2**	√	√

5. Conclusions

In this paper, we have proposed a JPEG cover image based steganography with high visual quality along with high embedding capacity stego image. To improve the embedding capacity, we have used modified quantization table that increases the number of non-zero middle-band quantized DCT coefficients of every 8×8 blocks and two bits of encrypted secret message bit sequence are embedded into each permissible quantized DCT coefficients. In the proposed scheme, to maintain the visual quality of the reconstructed stego image, the encrypted secret message bit sequence is embedded into the middle-band quantized DCT coefficients according to the modified zigzag scanning order. Experimental results further demonstrate that the proposed scheme provides high quality reconstructed stego- image from the JPEG stego-image and is capable to withstand various statistical attacks. To show the effectiveness of the proposed scheme, the proposed scheme is compared with some other related existing methods such as JSteg, F5, OutGuess, Chang *et al*.[4] scheme and Liu and Liao 12] scheme and satisfactory results have been found.

References

[1] Ataby A. and Naima F., "A Modified Higy Capacity Image Steganography Technique Based on Wavelet Transform," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 358-364, 2010.

[2] Atee H., Ahmad R., and Noor N., "Cryptography and Image Steganography using Dynamic Encryption on LSB and Color Image based Data Hiding," *Middle-East Journal of Scientific Research*, vol. 23, no. 7, pp. 1450-1460, 2015.

[3] Chan C. and Cheng L., "Hiding Data in Images by Simple LSB Substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469-474, 2004.

[4] Chang C., Chen T., and Chung L., "A Steganographic Method based upon JPEG and Quantization Table Modification," *Information Sciences*, vol. 141, no. 1-2, pp. 123-138, 2001.

[5] Chanu Y., Singh K., and Tuithung T., "A Robust Steganographic Method based on Singular Value Decomposition," *International Journal of Information and Computation Technology*, vol. 4, no. 7, pp. 717-726, 2014.

[6] Chen P. and Lin H., "A DWT Based Approach for Image Steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275-290, 2006.

[7] Chen W., Chang C., and Le T., "High Payload Steganography Mechanism using Hybrid Edge Detector," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3292-3301, 2010.

[8] Fridrich J., Goljan M., and Hogea D., "Steganalysis of JPEG Images: Breaking the F5 Algorithm," *in Proceedings of 5th International Workshop Information Hiding, Springer*, Noordwijkerhout, pp. 310-323, 2002.

[9] Upham D., "Jsteg Steganographic Algorithm,"

Available on the internet ftp://ftp. funet. fi/pub/crypt/steganography, Last Visited, 1999.
[10] Kanan H. and Nazeri B., "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality based on A Genetic Algorithm," *Expert Systems with Applications*, vol. 41, no. 14, pp. 6123-6130, 2014.
[11] Lee C. and Chen H., "A Novel Data Hiding Scheme based on Modulus Function," *Journal of Systems and Software*, vol. 83, no. 5, pp. 832-843, 2010.
[12] Liu C. and Liao S., "High-Performance JPEG Steganography using Complementary Embedding Strategy," *Pattern Recognition*, vol. 41, no. 9, pp. 2945-2955, 2009.
[13] Nissar A. and Mir A., "Classification of Steganalysis Techniques: A Study," *Digit Signal Process*, vol. 20, no. 6, pp. 1758-1770, 2010.
[14] Provos N., "Defending Against Statistical Steganalysis," *in Proceedings of the 10th USENIX Security Symposium*, Washington, pp. 323-336, 2001.
[15] Stalling W., *Cryptography and Network Security Principles and Practice*, Pearson Education, 2007.
[16] Stinson D., *Cryptography Theory and Practice*, Chapman and Hall, CRC Publisher, 2006.
[17] Subhedar M. and Mankar V., "Current Status and Key Issues in Image Steganography: A Survey," *Computer Science Review*, vol. 13-14, pp. 95-113, 2014.
[18] Trappe W. and Washington L., *Introduction to Cryptography with Coding Theory*, Pearson Publisher, 2005.
[19] Wang R., Lin C., and Lin J., "Hiding Data in Images by Optimal Moderately-Significant-Bit Replacement," *Electronics Letters*, vol. 36, no. 25, pp. 2069-2070, 2000.
[20] Wanga K., Lub Z., and Hua Y., "A High Capacity Lossless Data Hiding Scheme for JPEG Images," *Journal of Systems and Software*, vol. 86, no. 7, pp. 1965-1975, 2013.
[21] Westfeld A. and Pfitzmann A., "Attacks on Steganographic Systems," *in Proceedings of 3rd International Workshop on Information Hiding*, Dresden, pp. 61-76, 2000.
[22] Westfeld A., "F5- A Steganographic Algorithm: High Capacity Despite Better Steganalysis," *in Proceedings of the 4th International Workshop on Information Hiding, Springer*, Pittsburgh, pp. 289-302. 2001.
[23] Wu D. and Tsai W., "A Steganographic Method for Images by Pixel-Value Differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613-1626, 2003.
[24] Yeh H., Gue S., Tsai P., and Shih W., "Wavelet Bit-Plane based Data Hiding for Compressed Images," *International Journal of Electronics and Communications*, vol. 67, no. 9, pp. 808-815, 2013.
[25] Yu X., Wang Y., and Tan T., "On estimation of Secret Message length in JSteg-like Steganography," *in Proceedings of the 17th International Conference on Pattern Recognition*, Cambridge, pp. 673-676, 2004.
[26] Zhang T. and Ping X., "A Fast and Effective Steganalytic Technique Against JSteg-like Algorithms," *in Proceedings of the ACM Symposium on Applied Computing*, Melbourne, pp. 307-311, 2003.

Arup Kumar Pal is currently working as an Assistant Professor in the Dept. of CSE, ISM Dhanbad, India. He did his Ph.D in CSE from ISM Dhanbad in 2011. His main research interest includes Vector Quantization, Image Compression, Image Cryptosystem, Steganography, Watermarking and CBIR.

Kshiramani Naik is currently working as a full time Research Scholar in the Dept. of CSE, ISM, Dhanbad, India. She received her BE in CSE and M.Tech in CSE from BPUT Rourkela and NIT Rourkela respectively. Her research interest includes Image Cryptosystem, Steganography and Watermarking.

Rohit Agarwal is currently working as an Assistant Professor at the Dept. of CSE, JSS ATE Noida (U.P.) India. He has completed his M.Tech degree in Computer Application from the ISM Dhanbad in 2013. His research interests include Digital Image Processing and Numerical Linear Algebra.