

## A New Image Steganography Method using Message Bits Shuffling

<sup>1</sup>Prithwish Das, <sup>2</sup>Kushal Chakraborty, <sup>3</sup>Sayak Sinha, <sup>4</sup>Atanu Das

<sup>1,2,3,4</sup>Dept. of Computer Science and Engineering, Netaji Subhash Engineering College,

Techno City, Garia, Kolkata, West Bengal, India

<sup>1</sup>prithwish2007@gmail.com, <sup>2</sup>rony.kushal@gmail.com, <sup>3</sup>syksinha@gmail.com, <sup>4</sup>atanudas75@yahoo.co.in

Corresponding author: Atanu Das

<https://doi.org/10.26782/jmcms.2018.12.00001>

### Abstract

*Steganography has been considered as a technique of message hiding within another carrier multimedia data. Messages in the form of image (with embedded handwritten or typed texts) are often embedded in several ways within another image in image steganography. DCT based schemes are undertaken in the frequency domain methods in addition to usual plain text message embedding. Most of the message image hiding techniques embeds image bit string without considering any shuffling schemes to deal with the said string before embedding. Present work targeted to incorporate message hiding essentially with shuffled and re-shuffled bit strings in different ways prior to DCT operation. A new method has been proposed with these shuffling schemes to enhance the security level of the encryption. Investigations with the proposed image steganography method show that the new methods performed better than normal image steganography techniques without shuffling schemes. Performance of the proposed method is evaluated using Peak-Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). Results show that the shuffling bit steganography method outperformed the common DCT based schemes without shuffling.*

**Keywords :** Image Steganography, DCT, Message Bit Shuffling.

### I. Introduction

Since the rise of the internet technologies, digital media data can be transmitted conveniently over the internet. However, transmitted messages still have to suffer all kinds of security problems over the internet like unauthorized crossover. Different types of modern crypto systems have been evolving to protect the secret messages from illegal access by encoding the message before transmitting it over the network. However, the encrypted data exists in a meaningless form and may attract the intention of the interceptors to understand the secret messages. Steganography can be considered as the art and science of invisible communication. Steganography has

now become one of the important modern data hiding techniques. These methods hide the secret information (or message) in a cover carrier so that the presence of the embedded information is undetectable. Varieties of digital media platform such as image, audio, and video or a mix of these can be used as a cover carrier. Because of the insensitivity of the human visual system, cover carriers are widely chosen from digital images in most steganographic schemes, and are especially referred to as image steganography techniques.

Designing an image steganography technique consists of two parts – embedding (or message hiding) process and extracting (or message recovery) process. Within the cover image secret data is embedded and it forms a stego image. Secret data embedded into cover image are extracted will be using decryption algorithm. It may be noted that a pair of keys is used for both encryption and decryption process like other cryptography methods. If the both keys are same then the steganography is called symmetric, otherwise it is of asymmetric type.

Steganography methods uses uncompressed images with BMP extensions or compressed images with PNG extensions with lossless compressions because these offers large capacity to hide data since they contain much visually redundant information. The message hiding primarily started to take place from two approaches, namely spatial domain methods and frequency domain methods. Least significant bit replacement has been observed as mostly used spatial domain techniques where as DCT/DWT [IV], [VI], [XIII] based methods are major choice in the frequency domain. This work used BMP images to provide better capacity though a number of worked is noticed with JPEG images [VI], [XXI] where people think not to have hidden information due to less in memory size or capacity.

This work considered steganography methods where frequency domain methods were modified by integrating a new shuffling scheme. It may be noted that existing literature shows very little implementation of shuffling schemes except in [XVI], [XX] where the application fields are watermarking and general security. Introduction of shuffling schemes [V] can increase the complexity of message hiding and hence will increase the security potential of the hidden message because intruders will guess very little about the existence of hidden information inside. This work approached to hide information (message) inside an image by introducing a new shuffling scheme after DCT and quantization steps in line with [VI]. It is expected to provide more security by offering more inherent complexity of the shuffling scheme.

Rest of the paper is organized as follows. Section II presents a review of related literature. Section III presents the proposed methodology of encoding and decoding schemes. Section IV presents the experimental results with the proposed methods. The paper is ended with section V giving the conclusion of the present work.

## **II. Related Literature**

If secure information travelling over a network remains open, it becomes accessible to all and hence it will not remain secure. A variety of schemes is considered in the cryptography domain to hide a secure information inside another carrier normally within images namely with the nomenclatures watermarking [VIII], [XV], steganography [XVI] etc. Steganography is one of the data hiding techniques

where secure information gets embedded within another multimedia carrier usually within the images [VI]. Occasionally these conciliation techniques may not be sufficient to hide the data to be transmitted. These techniques are extended on those situation by including normal cryptographic methods (like DES, RSA etc) to improved the security schemes [II], [XIV]. Selection of container image may be another area to explore where [XVI] presented image classification schemes to optimize the efficiency of steganographic methods. Literature shows that the image steganography techniques are categorized in to four broad domains, namely, (1) spatial domain techniques (LSB replacement, LSB matching etc.), (2) transform or frequency domain techniques (DCT, FFT and DWT based methods), (3) spread spectrum techniques, (4) compressed domain techniques based on vector quantization, (5) distortion techniques, and (6) statistical techniques. First two categories are typically dominating as far as usage is concern among these four classes of methods, one is in the frequency domain and another is in the spatial domain [VII], [VIII], [XII].

LSB coding method [VII], [XVII] is noted to have major applications normally in the spatial domain where as DCT, DFT and DWT are used in the frequency domain. [XVI] demonstrated a Lucas sequence (in number theory) based method encapsulated under DCT based technique where as [VIII] considered an ordering strategy based on some snake scanning technique for making extension of the LSB method. [III] has also demonstrated a method incorporating pixel value differences to modify the LSB of the target image. The scheme also provides mechanism to get a layer structure revision of considered five pixels block wise. [XI] approached to increase the capacity of data hiding combining both the spatial and frequency domain techniques. It considered LSB with DWT for message hiding using FPGA platform to get required robustness and improved performances.

LSB based methods are easy to understand and implement compared to others where as frequency domain methods are complex as far as implementation is concern. Present work considered frequency domain methods specially incorporating DCT and quantization which are used in the JPEG based image compression steps. Chance of discovering the embedded message in this approach is comparatively lower than those with normal LSB based methods.

Someone interested to increase the security protection may opt for including more randomness under the scheme. Shuffling of data may be one of the ways of increasing randomness while dealing with LSB based schemes. Shuffling means rearrangement which is conducted by permutations. A few numbers of message hiding and security schemes have been noticed in the literature where the techniques are incorporated with some mechanism of message data shuffling within the schemes [VIII], [X] of message data encapsulation. [V] presented a very good demonstration on the theories of shuffling from its basic concepts to real applications. These shuffling schemes are mainly applied in watermarking and other security enhancement techniques. Few applications of such shuffling schemes are noticed in the LSB based methods [VIII], [X]. Even those shuffling schemes are found to get applications in the public key based encryptions methods and not in plain message hiding schemes. These shuffling schemes are not yet noticed to have applications in the image steganography methods

especially with DCT based schemes. This gap of application of the shuffling schemes in image steganography has been explored in this present work.

### III. Proposed Methodology

Steganographic techniques hide the secret messages in the cover carrier so that the presence of the embedded information becomes almost untraceable. Variety of digital media such as text, image, audio, and video can play the role as a cover carrier. Cover carriers are widely chosen from digital images in most steganographic schemes because of the insensitivity of the human visual system. The present scheme considered messages to get shuffled before it is embedded in the image encoding scheme incorporating DCT and quantization.

Present work first selects a carrier image. Then the text message is typed and converted to a message image (bit streams). This message image is considered for shuffling operation choosing optimum block length. After shuffling operation, this message image is embedded within the carrier image while steganographic operation is undertaken. On the other hand, first carrier image is undergone the extraction operation to get the hidden message image. This extracted message image is then passed through inverse shuffling operation to get the readable message image.

Shuffling Schemes:

Shuffling is introduced from the concept the cards or any other items distribution or arrangement. Normally we consider permutation of number of cards or items while dealing with shuffling issues. The permutation theories are very rich in mathematical statistics and used in many areas of science and technology specifically in the case of modeling uncertainties. Uncertainties increases with the underlying randomness. Increasing randomness is a fundamental requirement of increasing securities issues so that the decoding time increases sufficiently with the increase of randomness. Shuffling schemes are introduced [VIII], [X] in this cryptography and steganography domain because of these reasons. The bit strings are shuffled to induce randomness artificially in this security domain. The shuffling scheme consists of the following two parameters:

1. One is for q-shuffle (q)
2. Block size (B)

B and q are two key numbers in the proposed algorithms for encryption and decryption. B and q perform an important role in both the cases. In case of encryption, direct shuffling is used where inverse shuffling scheme is used for decryption algorithm. Direct shuffling results are straight away dependent on those key parameters. Moreover, proper implementation of inverse shuffling is impossible without knowing B and q in the receiver end and hence decrypted message will be erroneous in case of improper inverse shuffling.

The shuffling scheme considered in this work is inherited from that taken in to account while dealing with shuffling of bit string in delta network of multi-processor architecture in [IX]. The scheme of shuffling and inverse shuffling are elaborately explained below.

A q-shuffle of B objects is denoted by S where q is some positive integer given by  $q=2k$  where  $k=1, 2, 3, \dots$ . Then S is the permutations with q indices  $\{0, 1, 2, 3, \dots, q-1\}$ . The formula for shuffling is given below:

$$S(i) = \begin{cases} q * i \text{ mod } (B - 1) & \text{for } 0 \leq i < B - 1 \\ i & \text{for } i = B - 1 \end{cases} \quad (1)$$

Let message bits are stored into a 1D array (M). Assume length of message is 16 and store the values according to followings order.

$$M[0:15]=\{10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25\}.$$

Here we divide the message into 2 blocks. Each block length is 8. At first apply shuffling to the first block and then repeat the same thing for 2nd block. Assume L indicates the length of message. B represents the length of each block. N means number of blocks, i.e.  $N = L/B$ ;

Take an example, where  $L=16, B=8, q=4$ . So,  $N=2$ .

4 shuffle of 8 objects are presented below:

$$S(0) = 4 * 0 \text{ mod } 7 = 0$$

$$S(1) = 4 * 1 \text{ mod } 7 = 4$$

$$S(2) = 4 * 2 \text{ mod } 7 = 1$$

$$S(3) = 4 * 3 \text{ mod } 7 = 5$$

$$S(4) = 4 * 4 \text{ mod } 7 = 2$$

$$S(5) = 4 * 5 \text{ mod } 7 = 6$$

$$S(6) = 4 * 6 \text{ mod } 7 = 3$$

$$S(7) = 7$$

The following figure 1 illustrates an example of a 4 shuffle of 8 objects. In the above example only shuffling of first block is shown.

Similarly, for inverse shuffle  $q' = \frac{B}{q}$

The formula for inverse shuffle is given below:

$$S(i) = \begin{cases} q' * i \text{ mod } (B - 1) & \text{for } 0 \leq i < B - 1 \\ i & \text{for } i = B - 1 \end{cases} \quad (2)$$

For an example, 2 shuffle ( $q' = 2$ ) of 8 objects are given below:

$$S(0) = 2 * 0 \text{ mod } 7 = 0$$

$$S(1) = 2 * 1 \text{ mod } 7 = 2$$

$$S(2) = 2 * 2 \text{ mod } 7 = 4$$

$$S(3) = 2 * 3 \bmod 7 = 6$$

$$S(4) = 2 * 4 \bmod 7 = 1$$

$$S(5) = 2 * 5 \bmod 7 = 3$$

$$S(6) = 2 * 6 \bmod 7 = 5$$

$$S(7) = 7$$

The following figure 2 illustrates an example of a 2 shuffle of 8 objects.

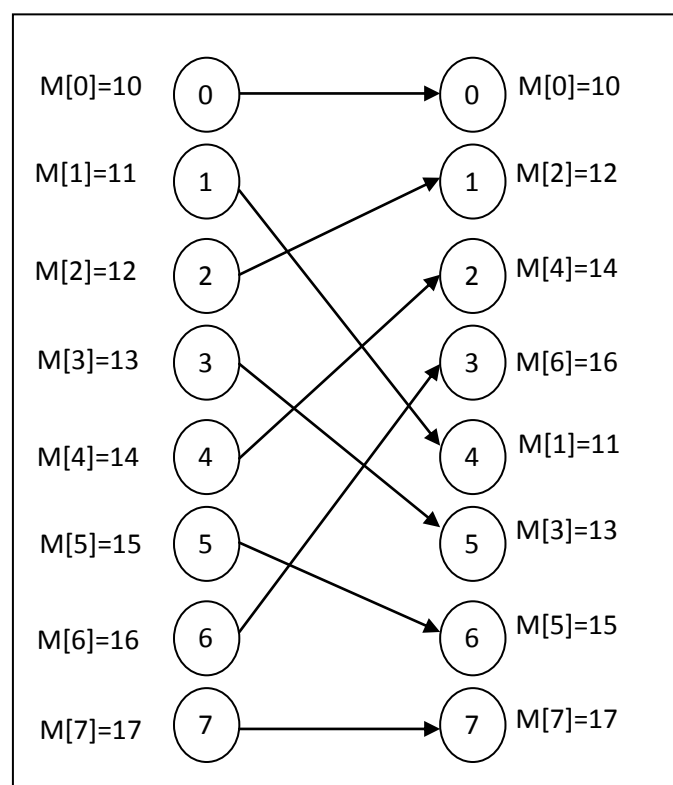


Fig 1. Shuffling operation

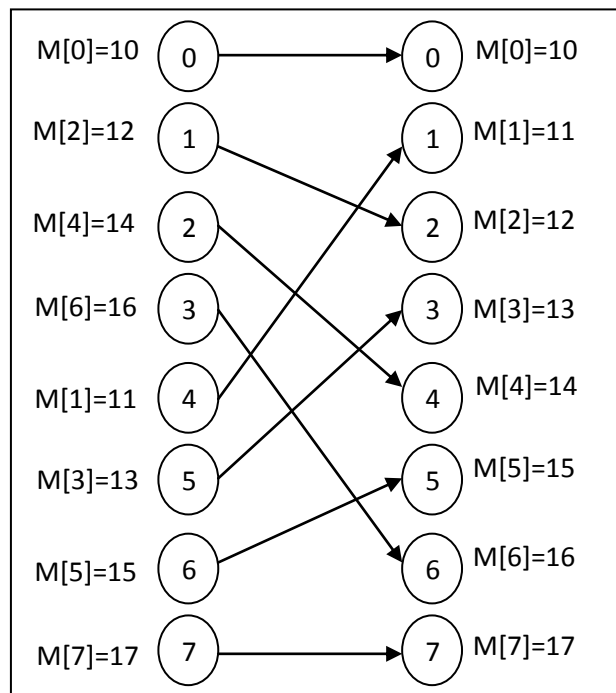


Fig 2. Inverse shuffling operation

**Steganography Algorithms:**

The following figure 3 presents the message embedding techniques with the help of a block diagram for easy understanding.

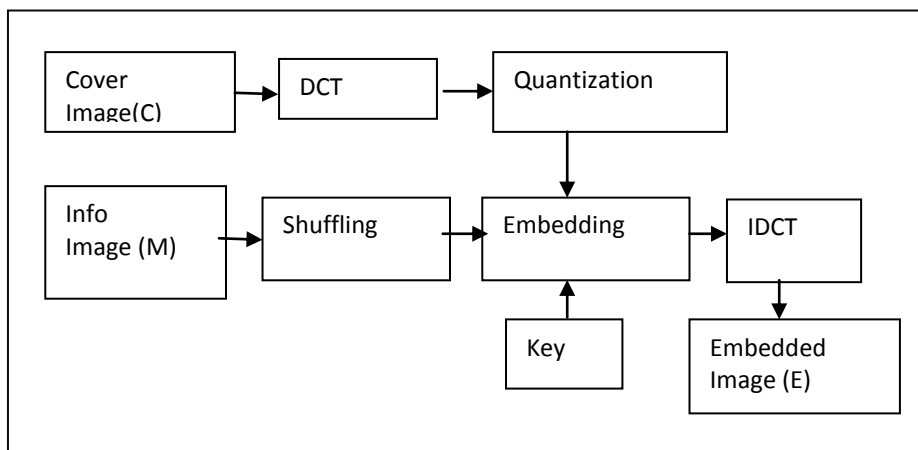


Fig 3. Block diagram of message embedding

The following figure 4 presents the message extraction techniques with the help of a block diagram for easy understanding.

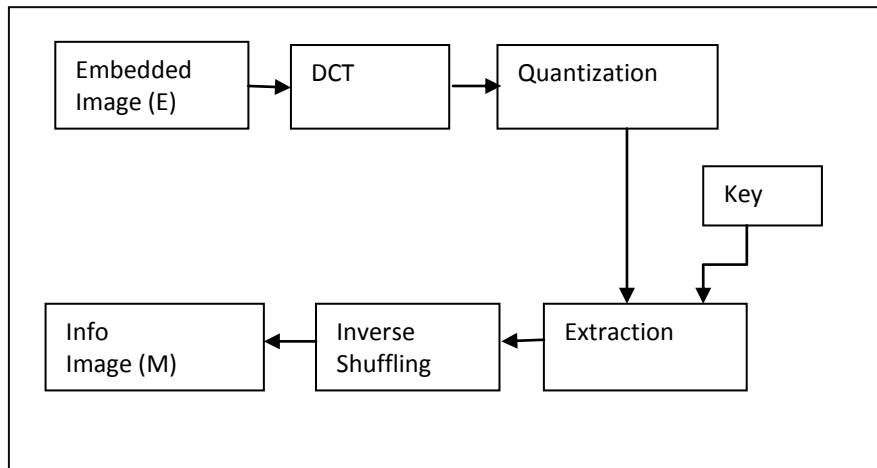


Fig 4. Block Diagram of Message Extraction

The following algorithms 3.1 and 3.2 present the technique of message encapsulations and extractions respectively

Algorithm 3.1: Message Embedding Algorithm

- Step 1: Take two images as input; cover-image (C) and the information-image (M).
- Step 2: Divide the C into 8x8 blocks.
- Step 3: Transform the pixel values of each block into DCT coefficients by applying DCT.
- Step 4: Round of the DCT values by dividing it by the quantization matrix (viz. Q90).
- Step 5: Divide the M into k number of fixed size blocks of length b.
- Step 6: Apply said shuffling scheme (given in the above section A) in each block of M and treat this as shuffled-M.
- Step 7: Hide (at LSB of DCT coefficients) the shuffled-M into the result matrix of step 4 except +1, -1 and 0 values as DCT co-efficient.
- Step 8: Perform IDCT on the result matrix of step 7 and get the embedded image (E).

Algorithm 3.2: Message Extraction Algorithm

- Step 1: Take E (embedded image) as input.
- Step 2: Divide E into 8x8 blocks.
- Step 3: Transform the pixel values of each block into DCT coefficients by applying DCT.
- Step 4: Round of the DCT values dividing it by the same quantization matrix (used in embedding algorithm).



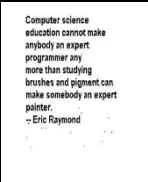
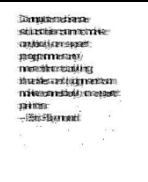


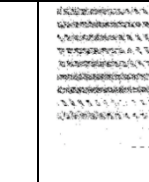
Step 5: Extract (from LSB of DCT coefficients) the shuffled-M from the result matrix of step 4 except +1, -1 and 0 values as DCT co-efficient.

Step 6: Perform said inverse-shuffling scheme (presented in section A) on the extracted values to get the correct form of M.

#### IV Experimental Results

Before reporting the quantitative performance of the proposed method, the question of choosing appropriate block size in the considered methods has been tried to be resolved. In case of embedding, the block size should be at least within certain limit to make it suitable for the hidden data. Following table 1 presents the quality of expected degradation of message image after considering shuffling operation with various block length. We have considered block length of 8, 16, 32, 64 and 128 for this particular example reported below.

**Table 1. Extracted message images with different block length**

4 shuffle Block length=8	4 shuffle Block length=16	4 shuffle Block length=32	4 shuffle Block length=64	4 shuffle Block length=128
				

It is observed that the message image is identifiable as text data up to 128 block length and this become almost indistinguishable beyond that block length. Moreover it appears as some kind of texture. So suggested optimum block length for this purpose are 128 and above to get desired shuffling performance. The following investigations reported below used block length of 128 in light of these results.

The above scheme is run on a set of carrier images and a number of secret message images. Some of the results are shown below. A slight variation in the results may be perceived depending on the size and quality of the cover image and the message image. The following figure 5 and figure 6 present the two sample cover images in the present experiment under consideration.



Fig 5. Cover Image (1)



Fig 6. Cover Image (2)

The following table 2 presents the results of the experiment during embedding and extraction. Second, third, fourth and fifth column of the said table demonstrates the qualitative appearance of the cover images, message images, stego images and extracted message images respectively. From these input-output images, it is observed that almost no qualitative degradation is noticed due to message hiding operations considered. This was also happened for the considered standard images in the image processing domain as well as for other images captured through camera operators. Though the degradation quality is considerably high for images other than those given here but they are comparable with those cases.

**Table 2. Extracted images with different quality**

Exp. No.	Cover Image	Message Image	Stego Image	Extracted Message Image
1.				
2.				
3.				
4.				

For comparing the quantitative performance of the proposed method, this work used the so called metric PSNR values. Peak-signal-to-noise ratio (PSNR) is a performance measurement for carrier image distortion, the well-known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics is applied to the Stego images. The said performance is compared with the method without shuffling that is the method with the DCT operation only. Following standard formula is considered for calculation of PSNR values in the present work.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [f(i,j) - f'(i,j)]^2$$

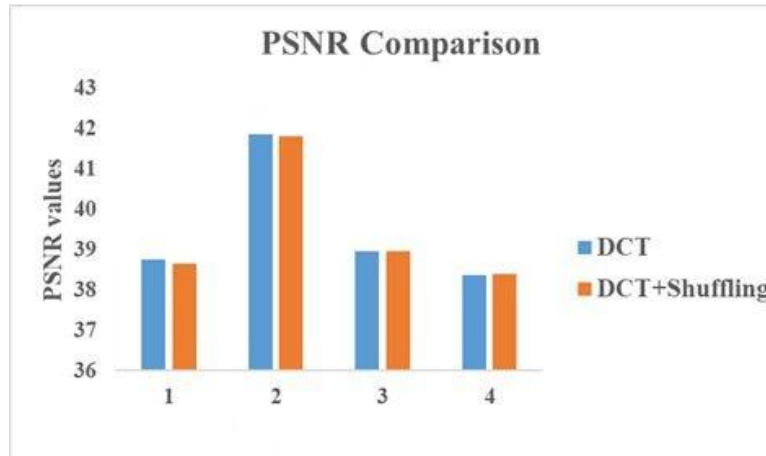
$$PSNR = 10 \text{ Log}_{10} \left[ \frac{255^2}{MSE} \right]$$

Here M is the Image height and N is the image width. i and j two indices.

Table 3 and figure 7 present those PSNR values for methods with and without Shuffling operation

**Table 3. Comparison of PSNR values**

Experiment No.	PSNR (DCT)	PSNR (DCT+Shuffling)
1	38.7431	38.6588
2	41.8776	41.8045
3	38.9666	38.9710
4	38.3760	38.3954



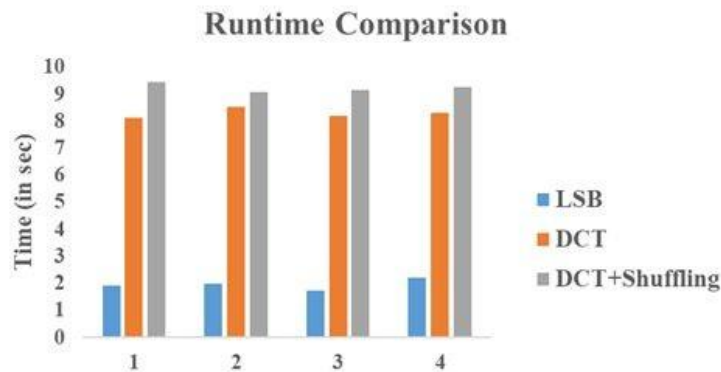
**Fig 7. PSNR value comparison**

From those results we may claim that these methods provided PSNR values or performance comparable and very similar. It is obvious that Shuffling schemes will offer higher randomness and hence increase higher chance of not to be discoverable. From this perspective, we may conclude that the proposed method is better than the methods without incorporating shuffling schemes.

Next investigation is to compare the performance of the proposed method with respect to extraction time. Following table 4 presents the comparison of the proposed method with standard methods LSB and DCT in the spatial and frequency domain of steganography. Figure 8 presents graphical representation of the data in the table 4.

**Table 4: Comparison of runtime**

Exp. No.	LSB	DCT	DCT+Shuffling
1	1.906	8.128	9.447
2	2.006	8.531	9.083
3	1.735	8.212	9.142
4	2.199	8.294	9.280



**Fig 8. Runtime Comparison**

From the above figure 8, is observed that time required for extraction is comparable for the proposed method with that of other standard methods. Moreover, the Shuffling scheme enforces to satisfy extraction time requirements higher than the time requirements for simple DCT based methods without shuffling. So we can claim that the proposed method is efficient with respect to its desired purpose.

## V. Conclusion

A novel steganography method has been proposed and implemented in this work by using a shuffling scheme normally found to have applications in the computational methods. The proposed method improves the encryption efficiency by using the shuffling schemes. It provides improved efficiency because of non-maintenance of array index table. In any random embedding method, one index table needs to be sent to the receiver which remained an extra burden. Proposed methods tried to overcome this burden by undertaking only two parameters viz. block length and the type of shuffle (example: 2 shuffle, 4 shuffle, 8 shuffle, ..., 2n shuffle). So the proposed method offers same level of security with minimum bit transaction. The considered block length for shuffling of message image bit string is expected to be more than 128 to get desired shuffling performance. The variations of shuffling

J.Mech.Cont.& Math. Sci., Vol.-13, No.-5, November-December (2018) Pages 1-15  
schemes and considerations of more complex schemes incorporating chaos theories may increase the efficiency of the technique under consideration.

Both qualitative and quantitative comparisons have been taken in to account to prove that the proposed method is outperforming and is superior to its predecessor standard methods. Investigations with different types of standard images show that the noise level (PSNR) found within acceptable limits. The said performance may vary with choice of image types. Present work advocates the use of more sophisticated shuffling schemes for enhancing the level of security under steganographic methods.

## References

- I. A. ElSayed, A. Elleithy, P. Thunga and Z. Wu, "Highly secure image steganography algorithm using curvelet transform and DCT encryption", Proc. of Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, pp. 1-6. May, 2015
- II. A. Jawed and A. Das, "Security Enhancement in Audio Steganography by RSA Algorithm", Int. Journal of Electronics and Communication Technology, Vol.: 6, Issue:1, spl-1, pp. 139-142, Jan 2015
- III. A. K. Gulve and M. S. Joshi, "A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution", Int. J. of Image, Graphics and Signal Processing, Vol.: 7, No. 5, pp. 66-74, 2015, DOI: 10.5815/ijgisp.2015.05.08
- IV. B. G. Banik and S. K. Bandyopadhyay, "Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT", Proc. of IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 400-405, 2015
- V. B. Mann, "How many times should you shuffle a deck of cards", Topics in Contemporary Probability and Its Applications, Vol.:15, pp. 1-33, 1995
- VI. C. C. Chang, T. S. Chen and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification", Information Sciences, Vol.: 141, Issue: 1, pp. 123-138, 2002
- VII. E Walia, P Jain and N Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, 10(1) (Ver 1.0), pp. 4-8, April 2010
- VIII. F. Yonggang, "A novel public key watermarking scheme based on shuffling", Proc. of IEEE International Conference on Convergence Information Technology-2007, pp. 312-317, 2007
- IX. K. Hwang and F. Briggs, Parallel processing and computer architecture, Me Graw Hill 164, 1984

- X. K. Peng and B. Feng, "A shuffling scheme with strict and strong security", Proc of Fourth IEEE International Conference on Emerging Security Information Systems and Technologies (SECURWARE), 2010
- XI. K. S. Shete, M. Patil and J. S. Chitode, "Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA", Int. J. of Image, Graphics and Signal Processing, Vol.: 8, No. 6, pp. 48-56, 2016. DOI: 10.5815/ijigsp.2016.06.06
- XII. L. Guo, J. Ni, W. Su, C. Tang and Y. Q. Shi, "Using statistical image model for JPEG steganography: uniform embedding revisited", IEEE Transactions on Information Forensics and Security, Vol.: 10, Issue:12, pp. 2669-2680, 2015
- XIII. M. Bilal, S. Imtiaz, W. Abdul and S. Ghouzali. "Zero-steganography using DCT and spatial domain", Proc. of 2013 ACS Int. Conf. on in Computer Systems and Applications (AICCSA), IEEE, pp. 1-7, May, 2013
- XIV. M. Zamani, A. A. Manaf, R. B. Ahmad, A. M. Zeki and S. Abdullah, "A Genetic Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology, 2009
- XV. M. Zamani, A. A. Manaf, R. Ahmad, F. Jaryani, H. Taherdoost, S. S. Chaeikar and H. R. Zeidanloo. "A novel approach for genetic audio watermarking", Journal of Information Assurance and Security, Vol.: 5, pp. 102-111, 2010
- XVI. P. Das, S. Ray and A. Das, "An Efficient Embedding Technique in Image Steganography Using Lucas Sequence", International Journal of Image, Graphics & Signal Processing, Vol.: 9, Issue: 9, pp. 51-58, 2017
- XVII. S. Chandran, and K. Bhattacharyya, "Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography", Proc. of IEEE Int. Conf. on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015
- XVIII. S. Hemalatha, U. D. Acharya, A. Renuka and R. K. Priya, "A Secure Color Image Steganography in Transform Domain", International Journal on Cryptography and Information Security (IJCIS), Vol. 3, Issue: 1, March 2013
- XIX. S. Lahiri, P. Paul, S. Banerjee, S. Mitra, A. Mukhopadhyay and M. Gangopadhyaya, "Image steganography on coloured images using edge based Data Hiding in DCT domain", Proc. of 2016 IEEE 7<sup>th</sup> Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1-8, October 2016
- XX. S. S. Jaber, H. A. Fadhil, A. Khalib, I. Zahereel and R. A. Kadhim, "Survey on Recent Digital Image Steganography Techniques", Journal of Theoretical & Applied Information Technology, Vol.: 66, Issue:3, pp. 714-728, 2014
- XXI. W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard, Van Nostrand Reinhold, New York, 1993