https://dx.doi.org/10.22161/ijaers.6.1.15 ISSN: 2349-6495(P) | 2456-1908(O)

High PSNR based Image Steganography

Namrata Singh

Department of IT, R.C.E.W. Jaipur, Rajasthan, India
Email: namritayadav07@gmail.com
Guide Name: Sh. Vinod Todwal, Assistant Professor (IT), RCEW, Jaipur, Rajasthan, India

Abstract*—*Steganography is a method for inserting digital data within a different digital medium like text, pictures, sound signals, or film signals, while not exposing its occurrence in the medium. Information safekeeping is an essential necessary domain in correspondence medium over the web system. In this paper, working for improve the performance of Image Steganography. Results are showing comparison in between DCT-SVD and LWT-DCT-SVD. PSNR of proposed methodology is high as compare to DCT-SVD.

Keyword—-Steganography, DCT, LSB-DCT, threshold, PSNR, Chaos, PWLCM, FLD, LWT-DCT-SVD.

I. INTRODUCTION

Today, overall need for the purpose of protecting all the digital information had becomes a very essential topic. Steganography is a work which is a combination of work steganos and graphos which means hidden writing. This is the secret of information with other carriers such as videos, images, graphics and documents for the purpose of getting the stego object as it won't be affected after the insertion. By this method, only receivers will understand if there is any secret message and can get it back. Steganography can be divided into two domains, frequency and spatial [1]. For first domain, modifications can be made for the pixels of the real image. Secret image is added directly in the pixels. Second domain, will have the carrier image which can be transformed from spatial domain into the frequency domain with the help of the techniques like domain transformation. The hidden message is then put into all these pixels. Second domain, in which all the carrier images are transformed with the coefficient with cover for forming the stego image [1,2]. Frequency domain can have different advantages, as it's more robust than the spatial technique, it can tolerate the shrinking, cropping, image manipulation etc. [1,2,3]. As there are different transformation which are used in the map for signaling it into frequency domain. [3] all the top methods which are used in literature are DFT or Discrete Fourier Transform, DWT or Discrete wavelet Transform or DCT Discrete Cosine Transform. [1,3]

Many metrics are there which are used for the purpose of evaluating the steganography method, which are MSE or Mean Square Error, PSNR or Peak Signal to Noise Ratio, SSIM or Structural Similarity Index, and the capacity along with the robustness and securities. [1,2] Robustness is ability of the stego image which is hidden against different attacks with security as the inability of the adversary for detecting the hidden image which are accessible only for the authorized users. [5] Steganalysis can be used for the purpose of detecting all the secret information [5]. Images which are digital can be mostly transmitted with the help of the internet along with multimedia information. This is why the importance is for the purpose of protecting them. There are many different types of images which can be easily covered with Bitmap File Format (BMP), Graphics Interchange Format (GIF), Joint Photographic Experts Groups (JPEG) images. All the research are mostly about the BMP images. It can also be studied that steganopraphic ways which embed message in LSB or Least Significant Bit of the DCT coefficient. All the embedding can be completed by two methods, random and sequential. Problems with sequential is the vulnerability, secret messages can be very easily detected. Another proposed improvement is of the technique that is applied in the literature of LSB and DCT with the threshold, it can also hide the data at random location which are based on threshold. [7] Problem with limited capacity which is related to taken threshold. It can also be broken without any problem as you discover this threshold. This is why the overall purpose of these paper is to provide a very novel image DWT way for the high embedding capacity and provide more security for the purpose of using the chaotic generator for the Piece Wise Linear Chaotic Map or PWLCM.

For the purpose of hiding any hidden data in the image, which is present in the big variety of steganography technique some of the available data is a lot more complex if compared with others and they have their own respective weak and strong points. Other application are there which can need complete invisibility for the secret information, there are some others which can need a big secret for the hidden data. In such cases Steganography will exploit human precipitation, most of the human senses are not worked for looking for the files which have the required information for the secret data which in in them, as there are some programs available which can do Steganalysis which is detecting the use of the Steganography. Most

https://dx.doi.org/10.22161/ijaers.6.1.15 *ISSN: 2349-6495(P) | 2456-1908(O)*

common uses of Steganography is for hiding a file inside some another file. When all the information of the file is secret in the carrier file, then data can be normally encrypted with the help of password.

Steganography can be usually confused by cryptography as there are two which are very same in a way that you need both to be protected for all the necessary information. The real difference in between the two is that Steganography will consist of hiding of data which is why it will appear in a way that no information is hidden in it. If any one sees the object in the hidden information, when the person will have absolutely no idea about the secret information, this is why the person will not use the decrypt information. In the image steganography, hidden communication can be achieved when you embed any message in the cover of the image which is used like a career for embedding the message in it and for generating the stego-image which is generated image which can be carrying the hidden message. It can also be very high security technique for any long data transmission.

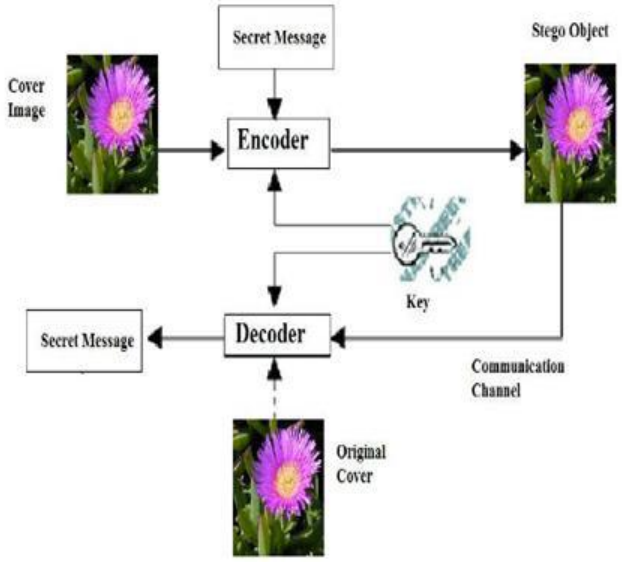

Fig 1:- Model of image Steganography

With the advancement of the computers and the expanding it can use in various area of work and life, all the issues of the information security can turn out to be very essential. One of the areas which are talked in the information security are the exchange of information with the help of cover media. In the end, there are many different methods like steganography, cryptography, coding and many more which can be used. Such methods of steganography are among the methods which has received a lot of attention in last few years. Main purpose of steganography is in the form of methods for converging all the media which is why other person will not have to notice the presence of this information. This are some of the main distinctions in middle of this method and some of the other methods which can convert exchange of data for example, when we consider cryptography, people can notice all the information by looking at the coded data as they are not be able to take this information.

II. LITERATURE REVIEW

Steganography has gained increasing importance, and have attracted lots of researchers 'attention. Many techniques have been developed. Deshpande et al., [8] explained the Least Significant Bit (LSB) embedding technique and presented the evaluation results for 2, 4 and 6 LSBs for a .png file and a .bmp file. The authors in [6] proposed a novel high capacity data embedding scheme that hides secret information in Discrete Cosine Transform Coefficients based on Average Covariance algorithm. The cover image covariance is computed to consider number of Most Significant Bits (MSBs) of payload to be embedded based on DCT coefficients. Kafri and Suleiman [9] have utilized the idea of the spatial steganography approach SSB-4 introduced by Rodrigues, Rios and Puech in 2003 [10] to propose a novel method which embed message bits in the 4^{th}bit of the successive non zero DCT coefficients of the low frequency region and modify the 1st, 2nd, 3rd and/or 5th bits to minimize the difference between the cover and the stegoimages. The 4th bit was chosen because it is the most significant bit which provides the minimum change in the pixel values. Since this approach uses significant bit, the hidden message resides in more robust areas and provides better resistance against the steganalysis [9, 10]. The authors in [5] proposed an image steganography technique based on combination of two transforms Integer Wavelet Transform and Discrete Cosine Transform. It used an assignment algorithm to select the best embedding locations of cover image to increase the visual quality of stego image and the system security. Recently, the idea of using chaotic systems has been noticed. Many chaos based steganographic methods have been discussed. MazharTayel et al., [3] proposed a new chaos steganography algorithm for hiding the confidential data based on discrete chaotic dynamic system. A logistic map chaotic generator is used to encrypt the secret message then embed the message randomly into the pixels least significant bits of the original image. [4] Presented Chaos based Spatial Domain Steganography using Most Significant Bit (MSB) that hides secret information in the spatial domain using LSB and MSB with a chaotic approach.

III. DWT BASED STEGANOGRAPHY

Steganographic technique for hiding multiple images in a color image based on DWT. The cover image is

https://dx.doi.org/10.22161/ijaers.6.1.15 ISSN: 2349-6495(P) | 2456-1908(O)

decomposed into three separate color planes namely R, G and B. Individual planes are decomposed into sub bands using DWT.DWT is applied in HH component of each plane. Secret data are dispersed among the selected DWT coefficients using a private key. PSNR, capacity and correlation are major aspects in steganography. More specifically PSNR is demanded high, but it depends application to application. PSNR is inversely proportional to capacity, and directly proportional to correlation and vice-versa. During the study we found a problem that is of a proper combination of PSNR, capacity and correlation is required so that data can be sent through unsecure channel without fear of third party access. The results in the steganography mainly depend on secrete data. The larger value of the secrete data; affect more to the quality of stego image rather than smaller value of secret data.

A. Embedding Process both Cover Image&Secret Data by using DWT

During the proposed embedding process, perform DWT on both the cover image and the secret data by using the fusion process we get fused image. Apply IDWT on fused image to get a stego image. 1) Algorithm for proposed embedding process:

- Step 1: Read the cover image (i.e.Video) as C and segment the frame based on video file. Convert the pixel values Of cover image into a gray scale image as CG.
- Step 2: Apply image pre-processing and correction process to get a gray scale cover image.
- Step 3: Read the secret data(i.e. Text) as S. Apply image pre-processing and correction process to get a gray scale image as SG.
- Step 4:Apply transforms domain technique into cover gray scale image and secret gray scale image.
- Step 5: By applying 2D-DWT extract the approximation coefficients of matrix LL1 and detail Coefficients matrices LH1, HL1, HH1 of level 1 of the cover image as CG1.
- Step 6: By applying DWT extract the approximation coefficients of matrix LA1 and detail coefficient matrices LH1,HL1, HH1 of level 1 of the secret image as SG1.
- Step 7: Apply fusion operation on an image CG1 and SG1 and get merged image. Finally perform fused image with 2-DWT to form the stego image as ST.

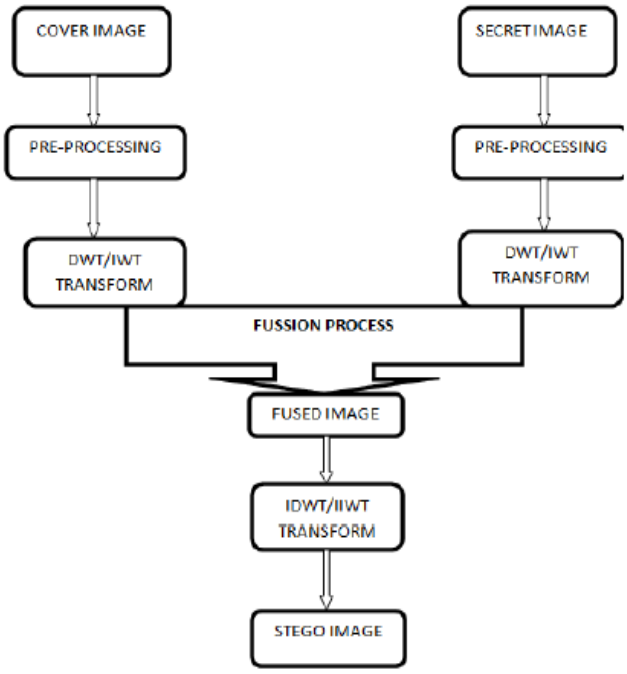

Fig 2:- Block Diagram of Embedding.

➢ *Extraction of Secret Image*

During the proposed extracting process, the recover stego image and known cover image were reconstructed with DWT transform domain and followed by the fusion process. Next, inverse transform IDWT was performed to rebuild the secret data. Finally the secret data is obtained, which is similar to the original secret image.

- Step 1: Receive the stego image. Perform a 2-D DWT at the level of both stego image and known cover image.
- Step 2: Apply fusion process on both stego image and cover image to get fused image.
- Step 3: Separate the wavelet coefficients and take inverse IDWT of the fused image to reconstruct the secret image.
- Step 4: Select the 4 bit privacy key to decrypt the secret information.
- Step 5: Calculate the statistical parameters such as Mean square Error (MSE), Peak signal to noise ratio (PSNR),Capacity, Entropy Mean of the stego image.

https://dx.doi.org/10.22161/ijaers.6.1.15 *ISSN: 2349-6495(P) | 2456-1908(O)*

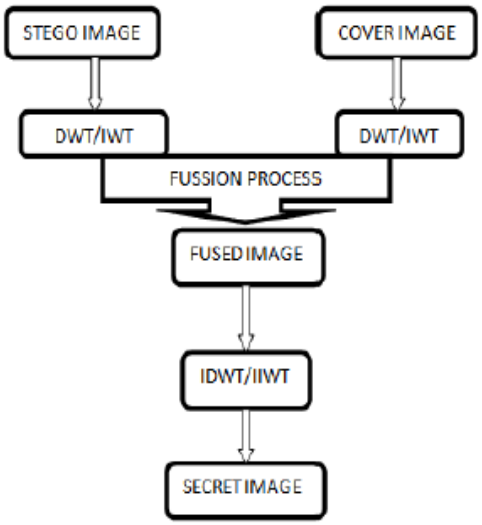

Fig 3:- Block Diagram of Extraction

➢ *DCT – SVD based Image Stegaography*

❖ *Embedding Process*

The steps of embedding process are as following:

- Read the cover and the secret image.
- Convert the secret image to 1-D binary vector.
- Divide the cover into 8□8 blocks and working from left to right, top to bottom, apply the 2D DCT transformation to each block.
- Use the described chaotic generator to provide a long sequence of l bits.
- Extract from the generated sequence the coordinates (X,Y) that represent the locations of the transformed DCT coefficients in which the secret image will be embedded as illustrated in the example below. The first k bits represent X, the following k bits represent Y and so on.

.....1010.....1110.....1101.....010.....

X Y X Y

- Replace the LSB of these defined coefficients with the MSB of the secret data.
- Apply 2D Inverse DCT to get the final stego image. Sharing the initial conditions of the chaotic generator and the secret image size with the receiver, he will generate the same random sequence, and apply the extraction algorithm.

B. Extraction algorithm

The steps of the secret image extraction applied by the receiver are:

- Read the stego image.
- Divide the stego image into 8□8 blocks and apply 2D DCT on each block.
- Generate the same random sequence from the chaotic generator and extract the positions of DCT coefficients that hide the secret data.
- Extract the LSB of the defined coefficients.
- Construct the secret image.

IV. PROPOSED METHODOLOGY

Introduce a novel video steganography algorithm in the wavelet domain based on the KLT Ourproposed steganography is divided into the following four phases.

A. Lifted Wavelet Transform (LWT)

LWT is lifted DWT. It simply lifts the coefficients of DWT. DWT contains the up and down sampling. So through filtering attacks there is a possibility of loss of information. While in LWT there is no up and down sampling [1] it contains Split, Predict and Update so there is no loss of information. It also overcomes the problem of rounding of DCT and DWT [3] because of split, predict and update stages of LWT. LWT decompose the image into four sub bands as shown in the figure 1. They are called as an approximation component (LL), vertical component (LH), horizontal component (HL) and diagonal detail (HH). Where the first letter indicates whether it is the low pass (L) or high pass (H) filtered along the columns (vertically) and second letter represents whether it is low pass (L) or high pass (H) filtered along the rows (horizontally). In decomposing, row wise and column wise down sampling is done so image is divided into two bands and again two bands respectively and finally decompose into four bands.

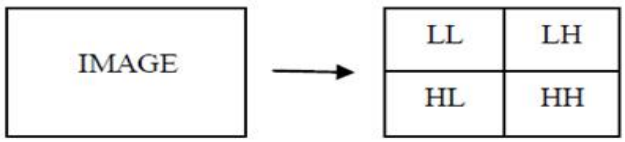

Fig 4:- Decomposing of Image by LWT

In comparison with other wavelet transforms reconstruction of the image by LWT is good, because it is increases the smoothness and reduces aliasing effect. It requires less memory and less computational cost almost half of DWT. LWT reduces loss in information, increases intactness of embedded watermark in the image and helps to increase the robustness of watermark [3].

https://dx.doi.org/10.22161/ijaers.6.1.15 *ISSN: 2349-6495(P) | 2456-1908(O)*

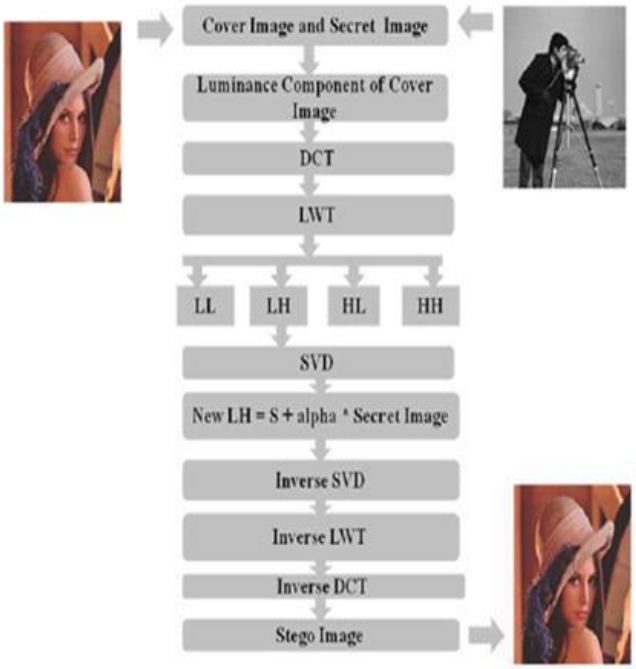

Fig 5:- Embedding Model

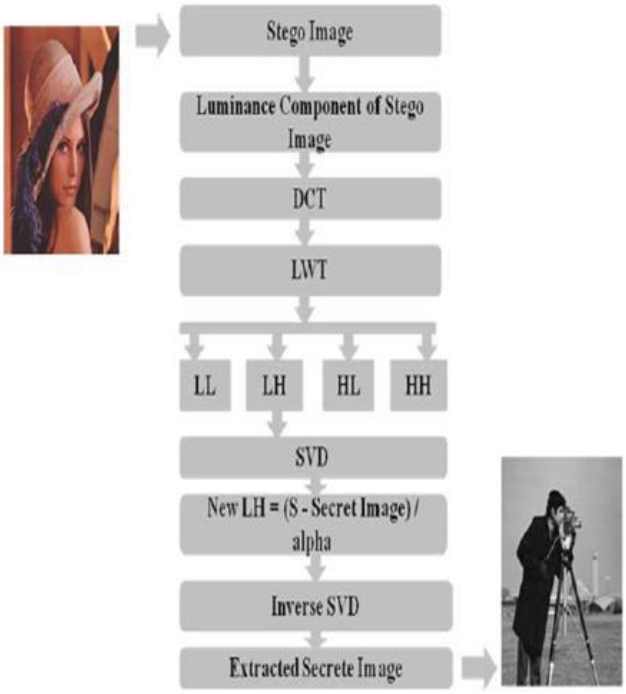

Fig 6:- Extraction Model

V. RESULTS

In the Result session, comparing the performance of the results. In this chapter, compare the Steganogrpahy method.

A. DWT-SVD Based Image Steganography

For hide the secret message DCT-SVD based Image Steganography method is using. Figure 7 is showing the Original cover Image in which secret image will hide.

Fig 7:- Original Cover Image

Fig 8:- Secret Image

Figure 8 is showing the Secret Image which we have to hide in the Original Cover Image . For image hiding , use DCT-SVD method.

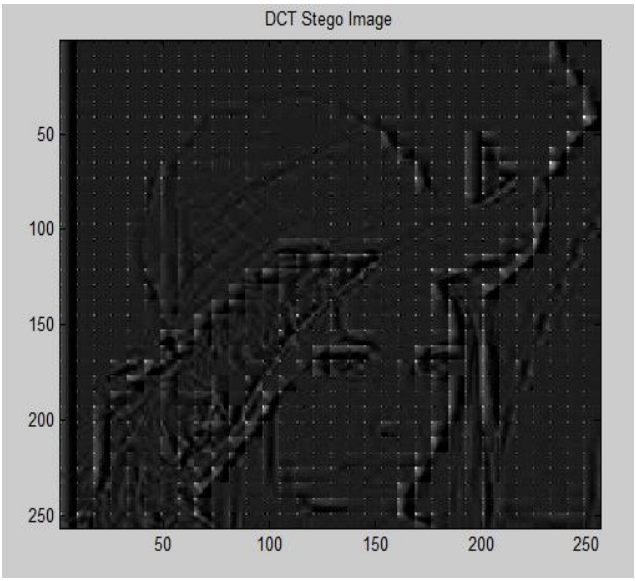

Fig 9:-Stego image

Figure 9 is showing the Stegoimage, which is receive by apply DCT-SVD based methodology. Stego image hide the secret image.

https://dx.doi.org/10.22161/ijaers.6.1.15 *ISSN: 2349-6495(P) | 2456-1908(O)*

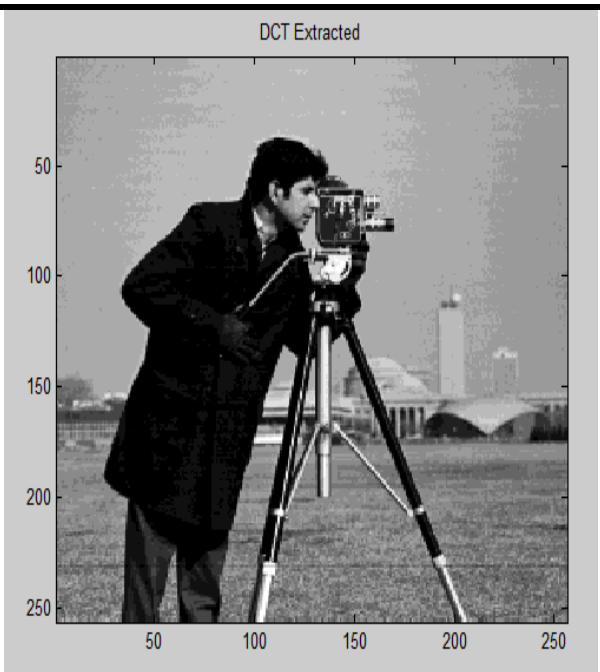

Fig 10:- Reconstruct Secret image

Figure 10 is showing the Reconstructed Secret image by apply DCT-SVD based Image Steganography.

B. Comparison Table

Table.1: Comparison Table

	PSNR
DCT-SVD	42.71
LWT-DCT-SVD	51.93

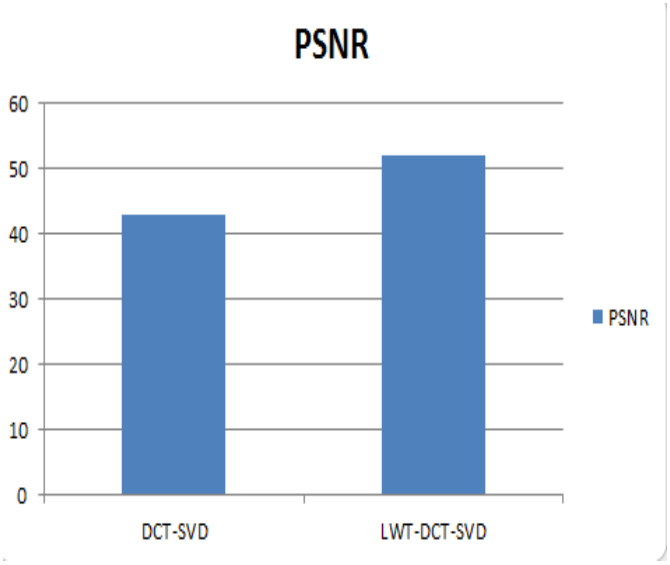

Fig 11:- For hide the secret message DCT-SVD based Image

Steganography method is using. Figure 11 is showing the Original cover Image in which secret image will hide.

VI. CONCLUSION

Image steganography technique is useful for security of confidential data over Internet. In this proposed work a new concept of Steganography has been introduce. Previous method will create difficulty for an unauthorized person to determine presence of secret massage. For improve the performance, show three parameters PSNR, MSE and NCC . PSNR, NCC is getting increase and MSE is getting decrease for the Proposed Methodology as compare to DWT-SVD Methodology.

VII. FUTURE WORK

In the future, we can work for the Research Limitation. According to the limitations, we are working only for Image Steganography. In the Future we can work at Audio and Video based Steganography. According to the Second limitation, we are working for PSNR, Correlation and Contrast parameters only. In the future we can work for the MSE parameter also. According to the third limitation, in this Research we are working only at gray Scale image. In the Future, we can work for the Color images also.

REFERENCES

[1] S. Bhattacharyya,. "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier." Journal of global research in computer science 2, no. 4 (2011).

[2] S. Saejung, A. Boondee, J. Preechasuk, and C. Chantrapornchai, "On the comparison of digital image steganography algorithm based on DCT and wavelet," in Computer Science and Engineering Conference (ICSEC), 2013 International, 2013, pp. 328–333.

[3] M. Tayel, H. Shawky and A. E. S. Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data," 14th International Conference on Advanced Communication Technology, pp. 208 – 212, 2012.

[4] N. Sathisha, G. N. Madhusudan, S. Bharathesh, K. B. Suresh, K. B. Raja and K. R. Venugopal, "Chaos based Spatial Domain Steganography using MSB", International Conference on Industrial and Information Systems(ICIIS), pp. 177-182, 2010.

[5] N. Raftari and A.-M. E. Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT," in 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2012, pp. 295–300.

[6] N. Sathisha, K. Suresh Babu, K. B. Raja, K. R. Venugopal and L. Patnaik, "Embedding Information In DCT Coefficients Based On Average Covariance"

https://dx.doi.org/10.22161/ijaers.6.1.15 *ISSN: 2349-6495(P) | 2456-1908(O)*

International Journal of Engineering Science and Technology (IJEST), 3 (4), 3184-3194. 2011.

[7] A. Danti, and P. Acharya. "Randomized embedding scheme based on DCT coefficients for image steganography." IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition (2010).

[8] D. Neeta, S. Kamalapur and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for various Bits" in Digital Information Management, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349

[9] N. Kafri and H. Y. Suleiman, "Bit-4 of frequency domain-DCT steganography technique," in First International Conference on Networked Digital Technologies, 2009. NDT ,09, 2009, pp. 286–291.

[10] J. M. Rodrigues, J. R. Rios, and W. Puech. "SSB-4 System of Steganography using bit 4." In 5th International Workshop on Image Analysis for Multimedia Interactive Services. 2004.

[11] B. Bakhache, J. M. Ghazal, and S. E. Assad, "Improvement of the Security of ZigBee by a New Chaotic Algorithm," IEEE Syst. J., vol. Early Access Online, 2013.

[12] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision," Comput. Phys. Commun., vol. 153, no. 1, pp. 52– 58, Jun. 2003.

[13] S. Tao, W. Ruli, and Y. Yixun, "Perturbance based algorithm to expand cycle length of chaotic key stream," IEEE Electron. Lett., vol. 34, no.9, pp. 873–874, Apr. 1998.

[14] E. Walia, P. Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, April, 2010, Vol. 10, pp. 4-8.

[15] S. K. Mutt and S. Kumar, "Secure image steganography based on Slantlet transform," in Proceeding of International Conference on Methods and Models in Computer Science, 2009. ICM2CS 2009, 2009, pp. 1–7.

[16] Y. Wang and P. Moulin, "Optimized Feature Extraction for Learning- Based Image Steganalysis, "IEEE Trans. Inf. Forensics Secur., vol. 2, no. 1, pp. 31–45, Mar. 2007.

[17] D. Caragata, S. El Assad, B. Bakhache, and I. Tutanescu, "Secure IP over Satellite DVB Using Chaotic Sequences". Engineering Letters journal. Volume 18, number 2, 2010, pp. 135-146.

[18] Nitin Jain, Sachin Meshram, Shikha Dubey ," Image Steganography Using LSB and Edge – Detection Technique ", International Journal of Soft Computing and Engineering (IJSCE) , Volume-2, Issue-3, July 2012.

[19] Kazi Azizuddin Rafiuddin1, Chetan Kumar," Improvement in LSB Image Steganography using Message Partitioning ", International Journal of Recent Research and Review, Vol. VI, Issue 3, December 2013.

[20] Amanpreet Kaur, Sumeet Kaur," Image Steganography Based on Hybrid Edge Detection and 2k Correction Method ", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 2, February 2012.