High Capacity and lossless Steganography using Discrete Cosine Transform

Deepika kulshreshtha, Kamal kumar

***Abstract*— Digital data communication is an important part of everyone's life. Data communication has some problems such as internet security so to elude these problems, cryptography is among one of the methods. However, encryption results in a disordered and confusing message and can allure eaves droppers easily. The technique used to keep the contents of a message secret is called steganography. Proposed work consists of embedding technique, retrieval technique and algorithms. the confidentiality and data integrity are required to protect data in case of unauthorized access and this resulted in an explosive growth of the field of information hiding. To achieve this we propose following assumptions: To embed the payload in the cover image by exchanging LSB bits of cover image by the image of the payload. The combined image is called stego-object(s).To converting the stego-object from spatial domain to frequency domain using DCT. To compress the frequency domain stego-object using quantization and run length coding to generate a secure stego-object.**

***General Terms*—Lsb, Iinjection, Protocol, Generation, Tcp, Ip, Udp, significant Bit, signal-to noise ratio**

***Index Terms*— Steganography, Basic steganography Model, Basics of embedding , Steganography Classification.**

I. Introduction

1.1Introduction to steganography:

Digital data communication is an essential part of everybody's life. Data communications have some problems name as internet security, copyright protection etc. To ignore these problems, cryptography is one of the techniques. Moreover, encryption results in a disordered and confusing message and can attract snoopers easily. Steganography methods overcome this problem by hiding the secret information back of a cover media (video, audio or image) because the existence of information cannot be noticed by any attacker [1].The goal of steganography is to keep the existence of a message secret Steganography is concealed writing and is the technique of hiding confidential data within a cover media such that it does not catch the attention of an unauthorized person [2]. The most commonly used steganographic method was bit insertion method where the least significant Bit (LSB) of the pixel is modified and projected [3]. There are two things that need to be considered while designing the Steganographic system. (a) Unapparant: Human eyes cannot distinguish the difference between original and stego image. (b) Potential: The more data an image can bear the better it is. However large embedded data may degrade image quality significantly [4].

Deepika kulshreshtha, MVVEC, JAGADHRI
Kamal kumar, MVVEC, JAGADHRI

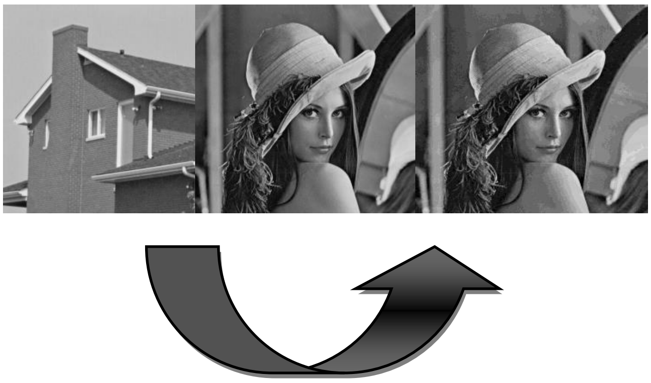


FIGURE 1.1 STEGANOGRAPHY

Digital steganography, or information-hiding schemes, can be characterized by making use of the theories of communication [5].The parameters of information secret, such as the number of data bits that can be hidden and the unseenable of the message and its resistance to removal, can be related to the characteristics of communication systems: potential, signal-to noise ratio (SNR), and jamming margin. The notion of capacity in data hiding specify the total number of bits secret and successfully recovered by the stego system.The signal-to noise ratio serves as a measure of invisibility, or detect ability.

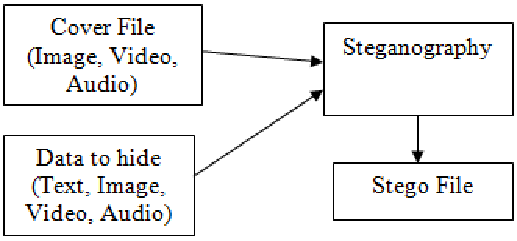


Figure 1.2: The Process of hiding Data

1.1.1 The four basic techniques used for Steganography are:

- **LSB method**: The LSB of bearer medium is directly inserted with the message bit. So LSB of the carrier medium contains the payload.
- **Injection:** Hiding data in segments of a file that are ignored by the processing application. Therefore ignore modifying those file bits that are adjacent to an end perfectly usable.
- **Substitution**: Replacement of the least significant bits of information that deduce the meaningful content of the original file with new data in a way that generates the least amount of deformation.
- **Generation**: Not like injection and substitution, this does not require an existing cover file but produces a cover file for the sole purpose of hiding the message.

1.2 Basic Steganography Model:

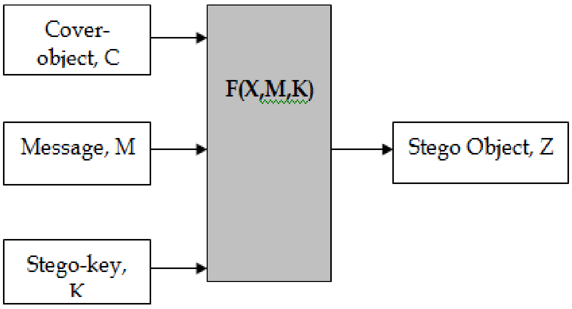


Figure 1.3: Basic model for steganography

Message is the data that the sender wishes to keep it confidential. It can be plain text, cipher text, other image, or anything that can be implanted in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which assure that only recipient who knows the corresponding decoding key will be able to separate the message from a cover-object. The cover-object with the secretly embedded message is then named as Stego-object. Retrieving message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used through the encoding process. The original image may or may not be required in most applications to extract the message [6].
There are several suitable carriers below to be the cover-object:

- Network protocols name as TCP, IP and UDP
- Audio that applying digital audio formats such as wav, midi, avi, mpeg, mpi and voc
- File and Disk that can hides and include files by using the slack space
- Text such as null characters, just alike morse code containing html and java
- Images file name as bmp, gif and jpg, where they can be both color and gray-scale [7].

In general, the information hiding process separate redundant bits from cover-object. The process consists of two steps:

1. Identification of duplicate bits in a cover-object. Redundant bits are those bits that can be modified without corrupting the quality or destroying the unity of the cover-object.
2. Embedding process then selects the subset of the redundant bits to be exchanged with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits [8].

1.3 The Basics of embedding:

In embedding process, a key is often needed This can be in the pattarn of public or private key so you can cryptograph the secret message with your private key and the recipient can decode it using your public key. In this way, it minimizes the chance of a third party attacker getting hold of the stego object and decoding it to find out the confidential information.

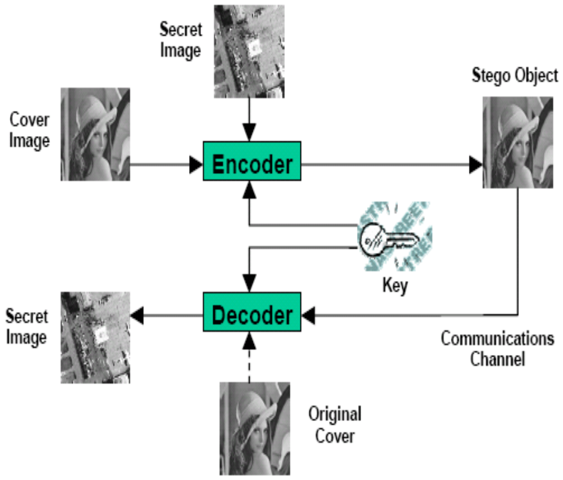


Figure 1.4: Generic form of image steganography.

After passage through the encoder, a stego object will be produced. A stego object is the original cover object with the secret information implanted inside it. This object should look almost identical to the cover object otherwise a third party attacker can see contained information. Having produced the stego-object, it will then be sent off via some transmission channel, such as email, to the intended recipient for decoding it. The recipient must decode the stego object in order to view the confidential information. At last, the decoding process is reverse of the encoding process. It is simply the separation of secret data from a stego object.

1.4Steganography Classification:

When we talk of digital steganography, we mean to call that, digital media's like Image, Audio /Video, Protocol are used as innocent covers for hiding secret confidential messages. Figure 1 shows the four main categories of file formats that can be used for steganography. [9]

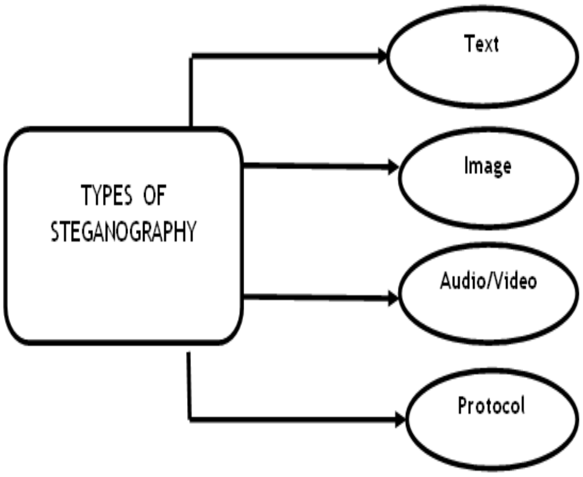


Figure1.5: Different types of Steganography

1.4.1 Hiding Information in Text:

Information can also be concealed in text files. The most popular method was to hide a secret message in each nth letter of each word of a text message [9]. A variety of various techniques exist of hiding data in text files. Text steganography having digital files is not used very frequently since text files have a very small amount of redundant data.

1.4.2. Hiding information in images:

Images are very famous cover source for digital steganography because of the large amount of redundant bits exists in the digital representation of an image. This paper will stresses on hiding information in images in the next sections.

1.4.3. Hiding Information in Audio Files:

Audio files can also be used for hiding secret data. One different method unique to audio steganography is masking, which exploits the features of the human ear to hide information unnoticeably. A slight but audible sound becomes inaudible in the presence of another louder audible sound [9].This property generates a channel in which to hide information. The larger size of meaningful audio files frame them less popular to use than images [10].

1.5 Different Image Steganography Techniques:

1) LSB (Least Significant Bit) method

It is one of the most usual and easiest methods for message hiding. In this method, message is concealed in the least significant bits of image pixels [11] .Changing the LSB of the pixels does not introduce great difference in the image and thus the stego image looks alike to the original image. In case of 24-bit images three bits of pixel can be used for LSB substitution as every pixel has separate components for red, green and blue [12].

Advantages:
1.) Simplest and contended to implement.
2.) Chances of message placing are 100%.
Drawbacks:
1.) Not vulnerable to different attacks.
2.) Invader can easily guess and change the LSB's of the image pixels, thus original message gets destroyed[13].

2) Masking and Filtering

Basically, this method is used for 24-bit and grey scale images. It is similar to placing watermarks on the image [12]. Steganography only hides the information where as watermarks becomes part or attribute of the image [13]. This method is more robust than LSB in terms of some image processing like - compression, cutting which makes it ideal in lossy JPEG images. Masking images includes changing the luminance of the masked area.

Advantages:
1.) Immune to image manipulation
2.) Durable technique
Drawbacks:
This method is mostly used for only 24 bit and grayscale images [11].

II. RELATED WORK

The research work performed in this field by different researchers is presented as follows:

Gowtham Dhanarasi et.al [1] in this paper a block complexity analysis for transform domain image stegonagraphy is invented. The algorithm proposed here acts on the wavelet transform coefficients which embedded the confidential data into the original image. The technique implemented which are efficient of producing a secret-embedded image that is identical from the actual image to human eye. This can be attained by retaining integrity of the wavelet coefficients at high capacity embedding. This development to capacity-quality trading –off interrelation is analyzed in detailed and experimentally explained in the paper.

Inderjeet Kaur et.al [2] The technique proposed in this paper is a integration of steganography and watermarking which provides copyright preventive to the information being transmitted confidentially. The suggested technique is a transform domain based method with the aid of segmentation and watermarking (TDSSW). It is noticed that the proposed technique comes up with fine PSNR (Peak Signal to Noise Ratio) and enhanced Security.

G. Arun Karthick et.al [3]this paper gives a new scheme which is hybrid in nature, combines two distinct domains.1) Steganography (Integration of Image + cryptography) and 2) Image Fusion – combining two images. Steganography implant the digital data message along with the media file where digital information may be text, image or hybrid. Although both Cryptography and steganography are integrated to provide security in some criteria yet advanced system of security is required to share information without any interference. To remove the real world problem a novel algorithm called StegFuse is proposed in this paper where cryptography and steganography is implemented on two various images, after implementing steganographic technique both the images are force to image combination in order to get the fused image. Wavelet transform is applied on both the image during fusion. Conventional cryptographic techniques are used for encryption of digital data and steganographic algorithms are used to conceal the encrypted data in the images.

S.Shanmugasundaram[4] The proposed method uses both Cryptography and Steganography to enhance the security of the message. The secret message is first encrypted using RSA algorithm and then randomized using OAEP. This encoded message is then embedded in the bitmap cover image using frequency domain approach. For embedding the encrypted message, initially skin tone regions of the cover image are detected using HSV (Hue, Saturation, Value) model. Thereafter, a region from skin detected area is selected, which is known as the cropped region. In this cropped region secret message is embedded using DD-DWT (Double Density Discrete Wavelet Transform). DD-DWT overcomes the intertwined shortcomings of DWT (like poor directional selectivity, Shift invariance, oscillations and aliasing). Hence the image obtained after embedding secret message (i.e. Stego image) is far more secure and has an acceptable range of PSNR. The terms of PSNR and robustness against various noises (like Poisson, Gaussian, salt and pepper, rotation, translation etc.).

Inderjeet Kaur et.al [6] The technique proposed is a combination of steganography and watermarking (TDSSW) which provides copyright security to the information being transmitted secretly over communication channel. The suggested technique is a transform domain based technique. At end it was noticed that the proposed technique comes up with good PSNR (Peak Signal to Noise Ratio) value and enhanced Security.

2.1 PROPOSED WORK

2.2 PROBLEM FORMULATION

The rising possibilities of modem transmission need the special means of security especially on computer networking. The network security seems more important as the number of data being exchanged on the Internet increases. So, the confidentiality and data integrity are necessary to protect data against unauthorized access and this resulted in an explosive growth of the field of information hiding. Information secret techniques are receiving much attention today due to fear of encryption services getting illicit and copyright owners who want to track confidential and intellectual property, copyright safety against unauthorized access and use in digital materials (music, film, book and software) through the use of digital watermarks. Advance security is not prolonged by the password protection but it is gained by hiding the presence of the data which can only be done by Steganography.

Proposed Work

In proposed work we do the following assumptions: Cover image, payload object (confidential message) are raw images of any arbitrary size. The LSB's of cover image is used to embed the payload. Let, Cover image be A: Cover image (A), B be the hidden image: Hidden Image (B), C be the stego-image: Stego image (C) Input: Cover Image (A) and a Hidden Image (B) Output: Encoded Stego Image(S) Repeat: Read first byte of A and B, Execute LSB (), Compute DCT (), Perform Quantization (), Copy the output as stego image.

III. RESULTS AND ANALYSIS

MATLAB is used as simulator to execute the techniques of steganography. MATLAB provides highly computing environment and advanced in-built function for image processing. An image is nothing but a matrix or set of matrices which define the pixels value of the image, That a grey scale value in black and white images, and Red, Green and Blue or Hue, Saturation and Intensity values in color images. imread function in MATLAB is used for taking input image. graythresh fun computes a global threshold (level) that can be used to convert an intensity image to a binary image with im2bw. A level is a normalized intensity value that lies in the range [0, 1].

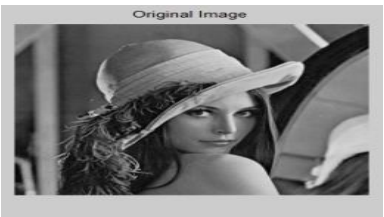


Figure 4.1 Original Image

Description: This is our cover Image in which we have to embed our secret image.

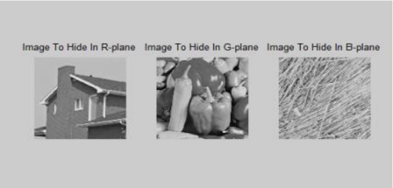


Figure 4.2 Message to be hidden.

Description: These are the secret images that need to be hidden in RGB plane.

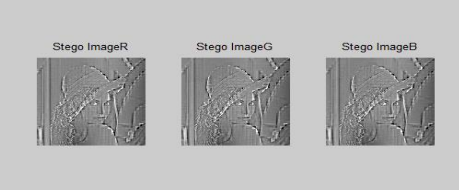


Figure 4.3 Stego image obtained

Description: Stego Image obtained after embedding the secret image inside cover medium.

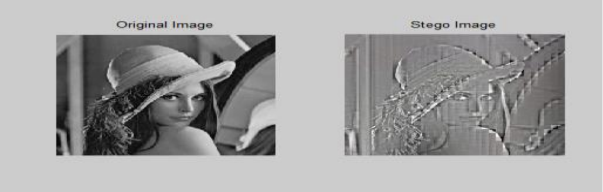
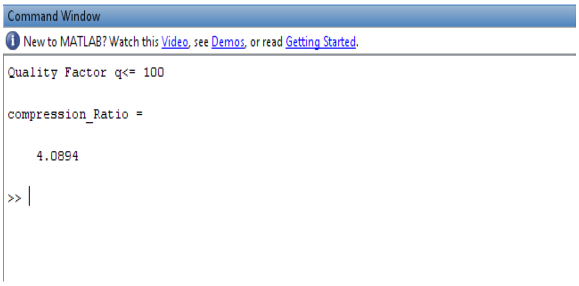


Figure 4.4 Comparison of Original image and stego image from proposed work.



```
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

Quality Factor q<= 100

compression_Ratio =

    4.0894

>> |
```

Figure 4.5 Quality Factor

Description: Image quality measurement between original image and compressed image.

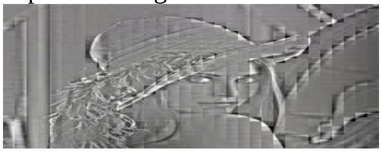


Figure 4.6 Resulted Image

Description: After applying DCT compression the resulted image is shown in figure.

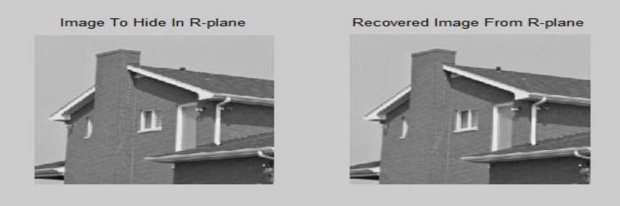


Figure 4.7 Recovered image from R-plane.

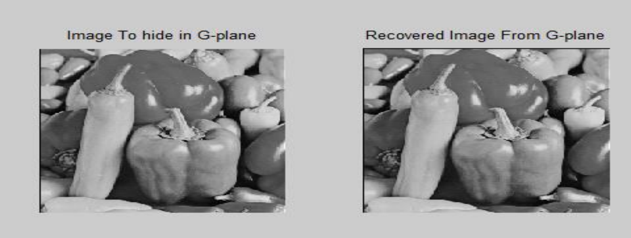


Figure 4.8 Recovered image from G-plane.

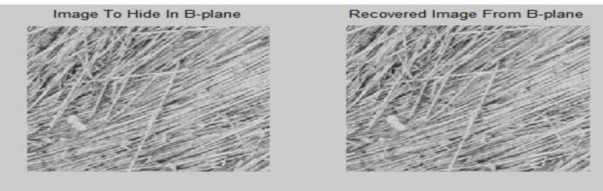


Figure 4.9 Recovered image from B-plane.

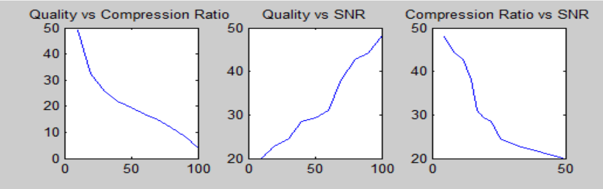


Figure 5.10 Comparison between Quality vs Compression ratio, Quality vs SNR, Compression ratio vs SNR.

Description:

1. Quality Vs Compression ratio: Image quality is the measure of how accurately our image matches the source image. Generally as the quantity of compression increases, quality decreases.

2. Quality Vs Signal to Noise Ratio: SNR parameter controls the sharpness of the restoration result. It compares the level of desired/ wanted signal to the level of background noise. At 100% quality we get 48% SNR.

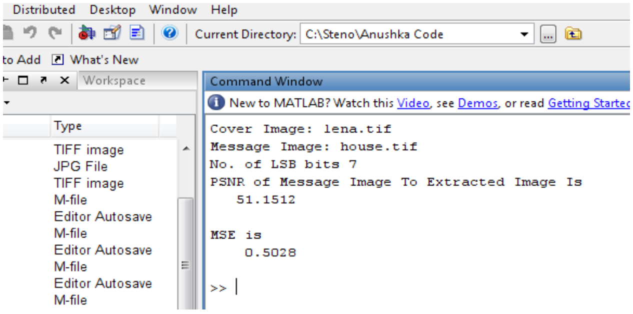
3. Compression ratio Vs SNR: The Compression ratio is used to measure the ability of data compression by relating the size of the image being compressed to the size of original image.

Parameters	Quality Vs C.R		Quality Vs SNR		C.R Vs SNR	
Proposed Technique	10	48.01	10	21.1323	48.6150	20.1456
	20	31.25	20	23.6137	31.2000	21.0690
	30	24.654	30	24.5698	24.4013	23.6085
	40	21.967	40	29.6853	20.3065	27.1459
	50	18.46	50	30.3815	18.30264	28.3178
	60	17.87	60	32.145	17.3715	33.0008
	70	13.900	70	37.1801	14.8800	39.9078
	80	10.425	80	44.8435	10.8078	42.5900
	90	7.518	90	46.32	7.1067	45.2185
	100	4.8721	100	49.12	3.6798	48.5055

Table 4.1: Parameters comparison between different image quality measurements**.**

5.1 Calculating PSNR and MSE:

Comparative analysis of LSB based & DCT Based steganography has been done on basis of parameters like PSNR & MSE on different images and the results are assessed. If PSNR ratio is high then images are best of quality.



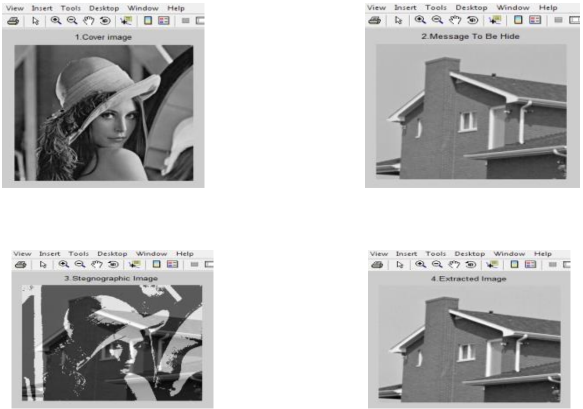
```
Cover Image: lena.tif
Message Image: house.tif
No. of LSB bits 7
PSNR of Message Image To Extracted Image Is
   51.1512


MSE is
    0.5028

>> |
```

Figure 4.11 Calculating PSNR and MSE between original image and stego image.

Description: After applying substitution method the PSNR and MSE is calculated.
Resulted Output:-



Result analysis:
From the above images we have concluded that Steganography is very efficient technique. Without compromising quality factor we can compress our image. The mean square error comes out to be zero.

IV. CONCLUSION AND FUTURE SCOPE

The objective of steganography is to communicate secretly using open channel. The technique proposed here is To develop an image based steganography framework to enhance security & quality of payload object. The stego image obtained was to be made secure by applying Huffman compression. Image quality is the measure of how accurately our image matches the source image. Generally as the amount of compression increases, quality decreases. SNR parameter controls the sharpness of the restoration result. It compares the level of desired/ wanted signal to the level of background noise. At 100% quality we get 48% SNR. The Compression ratio is used to measure the ability of data compression by comparing the size of the image being compressed to the size of original image. Comparative analysis of LSB based & DCT Based steganography has been done on base of parameters like PSNR & MSE on different images and the results are evaluated. If PSNR ratio is high then images are best of quality. After applying this technique we conclude that Steganography is very efficient technique. Without compromising quality factor we can compress our image. The mean square error comes out to be zero.

V. REFERENCES

[1] GOWTHAM DHANARASI, Dr.A. Mallikarjuna Prasad," IMAGE STEGANOGRAPHY USING BLOCK COMPLEXITY ANALYSIS", Vol. 4, No.07, July 2012.

[2] Inderjeet Kaur,Rohini Sharma, Deepak Sharma," TRANSFORM DOMAIN BASED STEGANOGRAPHY USING SEGMENTATION AND WATERMARKING", Volume 4, Issue 1, January 2013.

[3] G. Arun Karthick,K. Kavitha, V. Sivakumar, D. Surender," A HYBRID METHOD FOR COVERT COMMUNICATION USING STEGANOGRAPHY AND IMAGE FUSION", May, 2014**.**

[4] S.Shanmugasundaram," A Highly Secure Skin Tone Based Optimal ParityAssignment Steganographic Scheme Using DoubleDensity Discrete Wavelet Transform", Volume 4, Issue 3, March 2014.

[5] K B Raja, R.K.Chhotary, K.B.Shiva Kumar," Coherent Steganography using Segmentation and DCT", IEEE 2010.

[6] Amitava Nag, Sushanta Biswas, A Novel Techniques for image steganography based on DWT and Huffman Encoding", IJCSS, Vol(4): Issue (6).

[7] Hniels Provos & Peter Honeyman,"Hide & Seek :An Introduction to Steganography" ,IEEE Computer Society Pub-2003. 2.

[8] D. Bhattacharyya, J. Dutta, P. Das, R. Bandyopadhyay, S. K. Bandyopadhyay, and T. Kim, "Discrete Fourier Transformation Based Image Authentication Technique," in *Proc. 8th IEEE International Conference on Cognitive Informatics*, 2009, pp. 196-200.

[9] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, "A New Image Steganography Technique", IEEE- 978-1-4244-2108-4/08/$25.00 © 2008.

[10] Y. V. Rao, S. S. Rao, and N. R. Rekha, "Secure Image Steganography Based on Randomized Sequence of Cipher Bits," in Proc. IEEE Eighth International Conference on Information Technology: New Generations, 2011, pp. 332-335.

[11] Blossom kaur1, Amandeep kaur2 and Jasdeep singh,"Steganographic approach for hiding image in dct domain"International Journal of Advances in Engineering & Technology, July 2011.

[12] Anjali A. Sheju and Umesh L. Kulkarni . A Secure Skin Tone based Steganography Using Wavelet Transform International Journal of Computer Theory and Engineering, Vol.3, No.1,February, 2011, 1793-8201.

[13] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul,(2008), "Securing Information Content using New Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management.

[14] Majunatha R. H. S. and Raja K B, (2010), "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), Vol. 3: Issue (6) pp 462-472.

[15] Saraireh S. and Benaissa M., (2009), "A Scalable Block Cipher Design using Filter Banks and Lifting over Finite Fields" In IEEE International Conference on Communications (ICC), Dresden, Germany.

[16] El Safy, R.O, Zayed. H. H, El Dessouki. A, (2009), "An adaptive steganography technique based on integer wavelet transform," ICNM International Conference on Networking and Media Convergence, pp 111-117.

[17] Piyush Marwaha, Paresh Marwaha, (2010), "Visual Cryptographic Steganography in images", IEEE, 2nd International conference on Computing, Communication and Networking Technologies.

[18]Johnson, N.F and Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Journal, February 2008.

[19]Blossom kaur1, Amandeep kaur2 and Jasdeep singh,"Steganographic approach for hiding image in dct domain"International Journal of Advances in Engineering & Technology, July 2011.

[20] J.R. Krenn, "Steganography and Steganalysis",January 2004.Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs,"Implementation of LSB Steganography and its Evaluation for Various Bits", 2004.