International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Steganography for Secure Data Transmission and Reception and Stegoanalysis

Jyoti Ashok Thange[1], Kailas Aade[2]

[1]G.H.Raisoni College of Engineering Ahmednagar,Pune University, India

[2]Professor, G.H.Raisoni College of Engineering Ahmednagar,Pune University, India

Abstract: ***This paper introduces the steganography, it means hiding secure information and stegoanalysis. In Steganography message data is hiding behind cover data. Now a day's number of techniques are available for hiding information such as Least Significant Bit (LSB), Discrete cosine transform (DCT), Discrete Fourier transform (DFT) and Discrete wavelet transform (DWT). The data content may be in text, audio, video or image. Basically this paper focuses on image steganography. Due to steganography it is possible to communicate between two authorized parties. This is the part of Steganography. But sometimes, it is necessary to find secure data from un-authorized parties to save our nation from terrorist hence next part of project is stegoanalysis. In stegoanalysis two types of analysis are done that is subjective analysis and objective analysis.***

Keywords: PSNR, MSE, TEXTURE, VSNR, luminance, contrast, correlation, standard deviation, entropy, histogram, LSB, DCT, DFT, DWT

1. Introduction

The secret communication between two known parties is the today's necessary thing for that purpose steganography is necessary. Steganography is nothing but communication is in invisible manner. The secret data is hiding behind the cover image using different techniques. The steganography word is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1] hence it is defined as "covered writing". In image steganography the secret data as well as covered data is image.

Today's world means computer world so that study of steganography is most important. Another technique for hiding information is Cryptography. It also used for secure communication but difference between Steganography and cryptography is cryptography keep the contents of a message secret from unauthorized parties and steganography keep the existence of a message secret[4]. Both of these techniques used to protect information from unauthorized parties but neither technology is perfect. So that for secure purpose steganography with double compression is necessary. The double compression means LSB with DCT, LSB with DFT, and LSB with DWT. Due to combination of two techniques means dual compression the information is more secure than the single compression and hackers and crackers does not decode the message easily. It reduces the risk of information leakage. [8] The security in the communication is the most important in business, industrial documents, military applications and personal use also.

Organization of this Paper is as follows. Section I include Introduction. Section II gives brief literature review of Section III gives the system development Section IV gives result Section V gives conclusion and Section VI gives future work.

2. Literature Review

From a long period the steganography is used. The invisible inks such as milk, vinegar, fruit juices or urine were used for secret communication. The secret message is written using these invisible inks, when these are heated then the message gets display which is easily readable it is the one type of the steganography used from long period.

Today's world Steganography technique is used in computers mostly on internet. In Steganography cover image and message image together used for secret communication and using networks as the channels the message sends securely. Steganography as well as cryptography both are used for sending the secret data but neither technology alone is perfect. The message used for secret communication is in the form of text, audio, video, image and combination of text plus image, audio plus image etc.

In this paper the information keep secure using different techniques such as LSB, DCT, DFT and DWT but for more secure purpose dual compression is used it means combination of LSB with DCT, DFT, and DWT is done.

Other part of this project is stegoanalysis. In this it is important to find out whether the message is secret or not. For that purpose two types of analysis are done,

1. Subjective analysis
2. Objective analysis

3. System Development

In cryptography technique one can easily guess that it contain the encrypted message to avoid this problem Steganography is used with different techniques. The Cover image plus message image produce stego image and stego image minus Cover image produces message image. The basic mathematical model of steganography is as shown in the below.

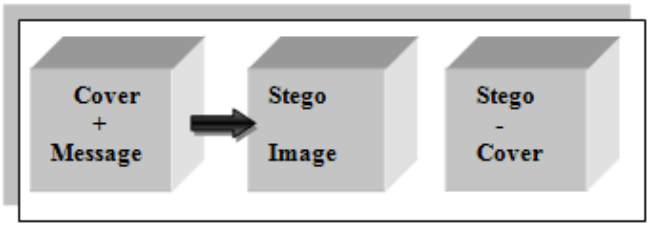
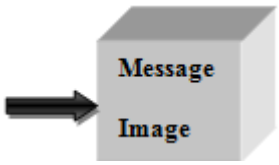


Figure 1: Graphical View of the Steganography system

The cover image acts as a carrier for the message image . The secret data is hide behind Image by the



steganographic techniques transfer add cover and secret message The obtained result is the stego-image is transferred from the sender's end to the receiver's end over the communication channel. At the receiver's end, the same steganographic algorithm works to extract the original secret data from the cover image.

The cover image and the message image combination is nothing but stego-image. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image and if we subtract cover image from stego image we get message image i.e. secret message.

3.1 Least Significant Bit (LSB)

Basically 8-bit or 24-bit files are used to store image in digital form and it produces the colored representation of the pixels these colors are derived from three primary colors such as red, green and blue. Each primary color is represented by 8-bit and 8-bit is equal to 1-byte. So each pixels required 24 bit. In this technique the only least significant bits are used for hide data, due to embedded data is undetectable to human eye. This is known as Least Significant Bit.

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1.

The LSB based Steganography is one of the steganographic methods, used to hide the secret data into the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS : (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
240 : 011110000
RESULT: (00100110 11101001 11001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

3.2 Discrete Cosine Transform (DCT)

DCT is one of the steganographic techniques to hide the data. DCT coefficients are used for JPEG compression. It divides the image into DCT coefficient and transforms a signal from the spatial domain into the frequency domain. It can separate the image into three categories high, middle and low frequency components.

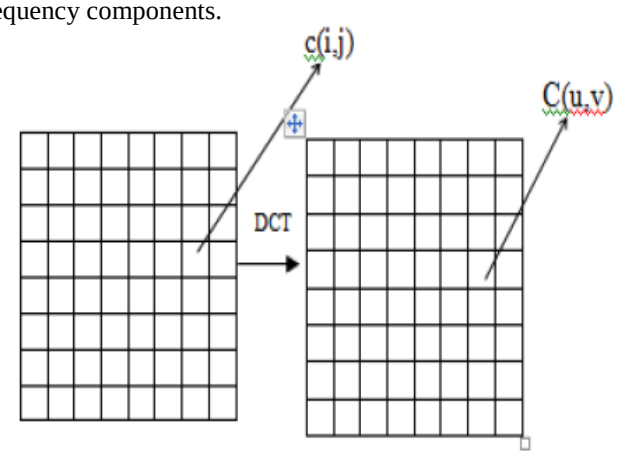


Figure 2: Discrete Cosine Transform of An Image

DCT is used in steganography for image. Image is broken into 8×8 blocks of pixels which are working from left to right, top to bottom; the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients. For DCT with block size (M _N), the connection between the spatial domain image pixels X(i; j) and the transform domain coefficients Y (u; v) is

Y (u; v) is

$$Y(u,v) = \frac{2c(u)c(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} X(i,j) \cos\left[\frac{(2i+1)u\pi}{2M}\right] \cos\left[\frac{(2j+1)u\pi}{2N}\right]$$

$$where\ u = 0,1, \ldots . M-1, v = 0,1, \ldots \ldots N - 1, and$$

$$c(k) = \begin{cases} \frac{1}{\sqrt{2}}, & if\ k \\ 1, & otherwise \end{cases}$$

$$= 0,$$

3.3 Discrete Fourier Transform (DFT)

The relationship between the spatial/temporal domain signals, f[n], and their corresponding transform in the frequency domain, F[k], is

$$F[k] = \sum_{n=0}^{M-1} f(n) . W_M^{kn}$$

Where $W_{M=e^{-j2\pi r/M}}^{r}$

For digital image, the 2D DFT can be defined as

$$Y(u,v) = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} X(i,j).W_M^{ju}.W_N^{jv}$$

The DFT of an image is always complex valued. This leads to the magnitude and phase representation for the image

$$M(u,v) = |Y(u,v)|$$
$$\emptyset(u,v) = \prec Y(u,v)$$

3.4 Discrete Wavelet Transform (DWT)

The field of Discrete Wavelet Transforms is a recent one and also one of the technique for steganography The Discrete Wavelet Transform (or DWT), is an orthogonal function applied to a finite group of data. Functionally, it is very similar to the Discrete Fourier Transform, in that the transforming function is orthogonal. In wavelet transform the image is converted from a spatial domain into frequency domain. The link between the spatial/temporal domain signals, f(t), and the DWT of f(t), d(k; l), is

$$f(t) = \sum_{k=-\infty}^{\infty}\sum_{l=-\infty}^{\infty} d(k,l)2^{-\frac{k}{2}}\Psi(2^{-k}t - 1)$$

Where Ψ (·) denotes the mother wavelet.

The Wavelet Transform is the simplest wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

Figure 3: DWT Band

4. Result

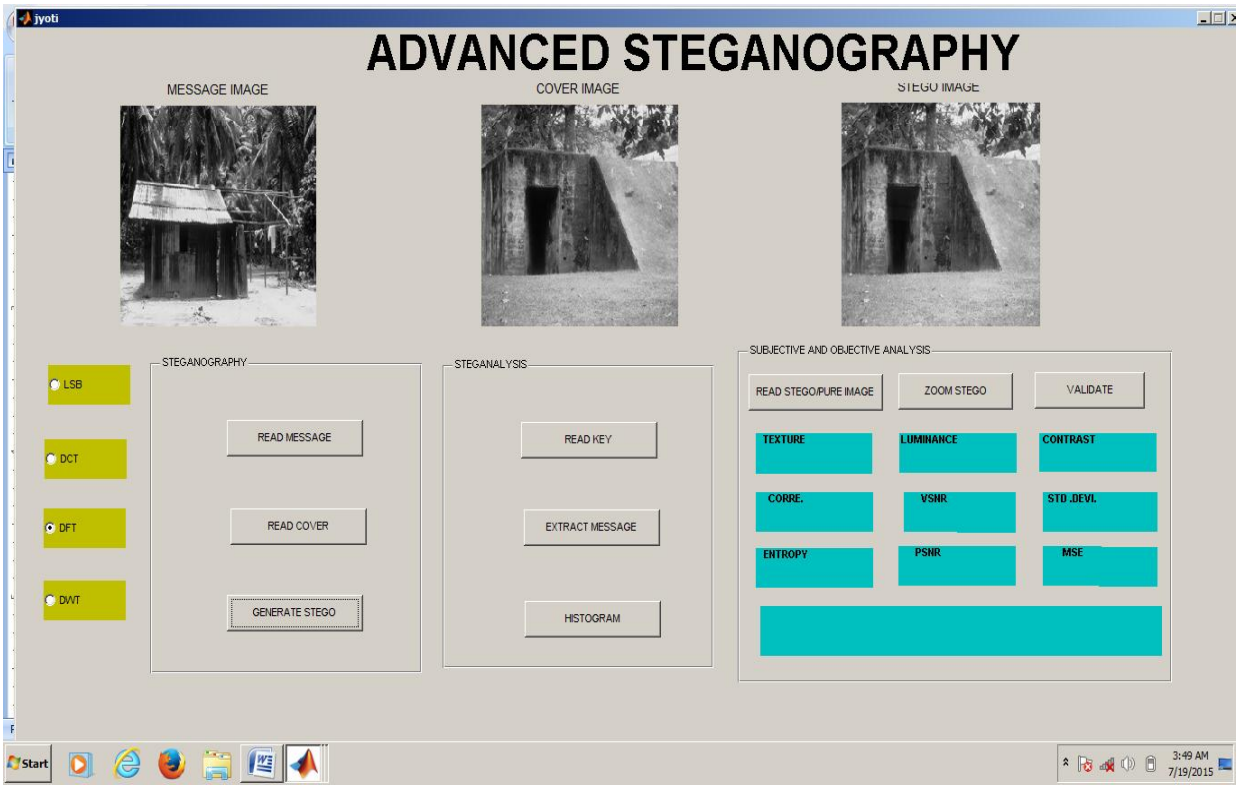


Figure 4: Steganography Part

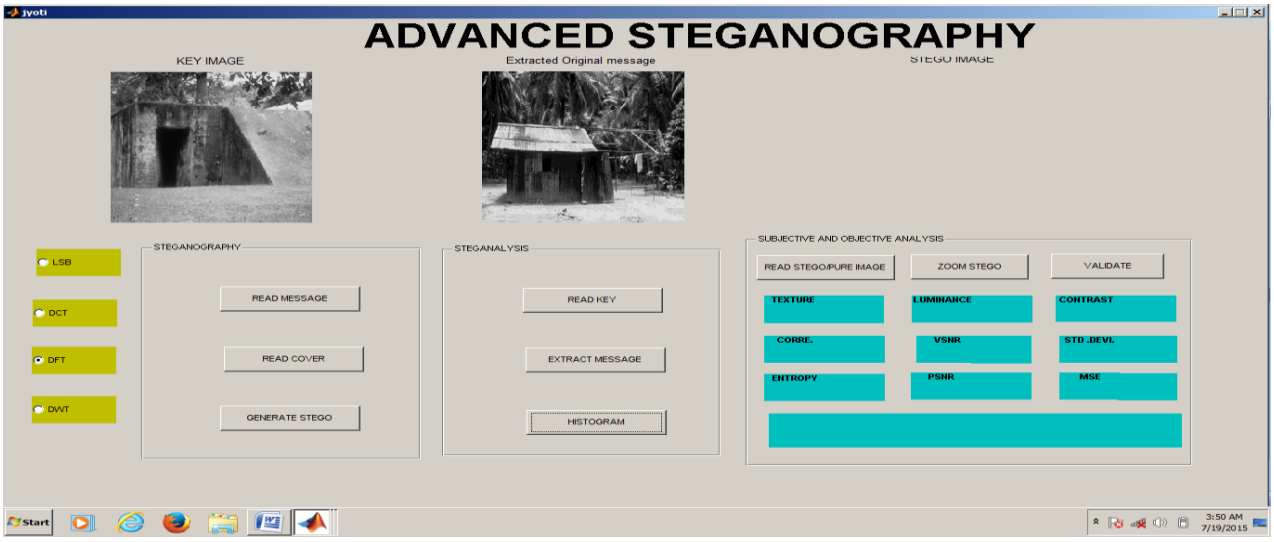


Figure 5: Stegoanalysis with histogram

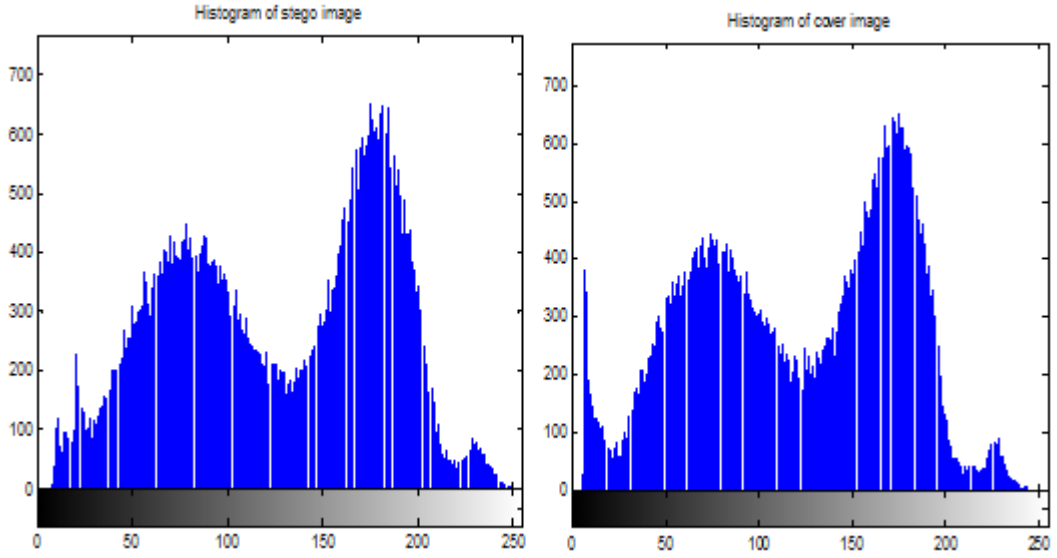
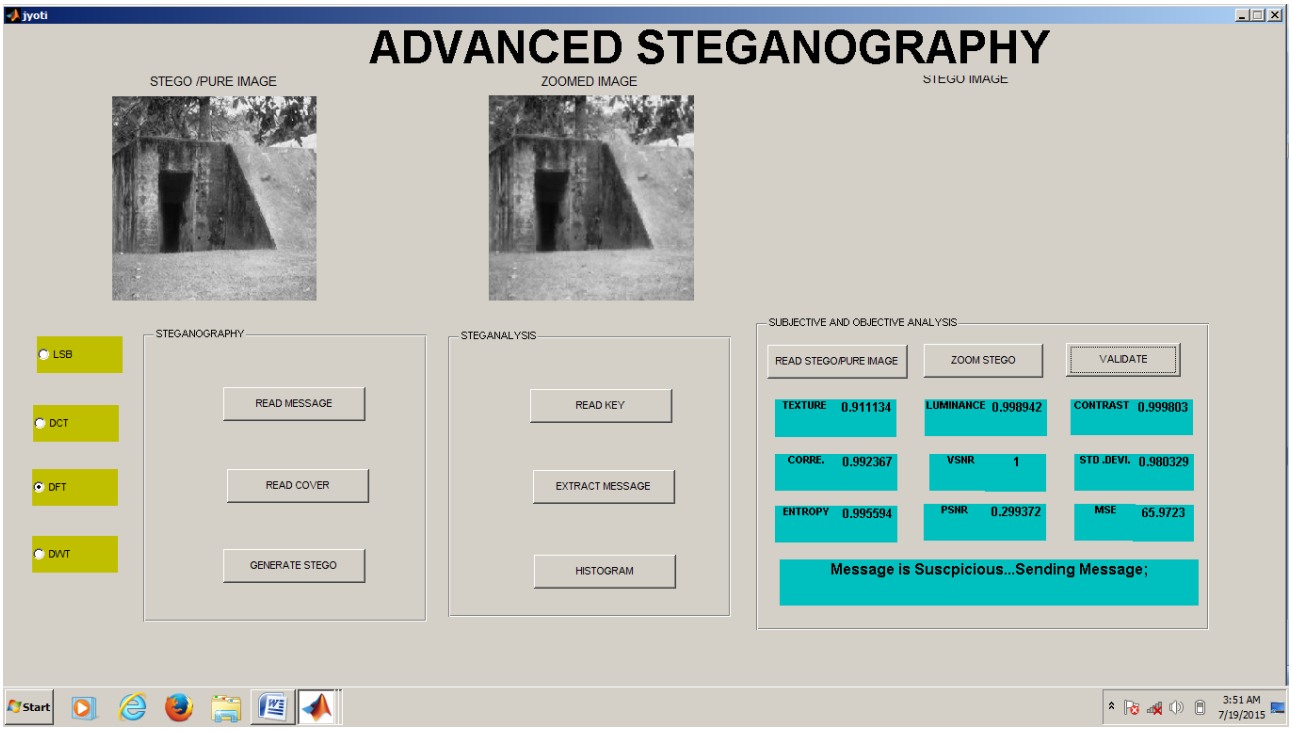


Figure 6: Histogram of cover image and stego image



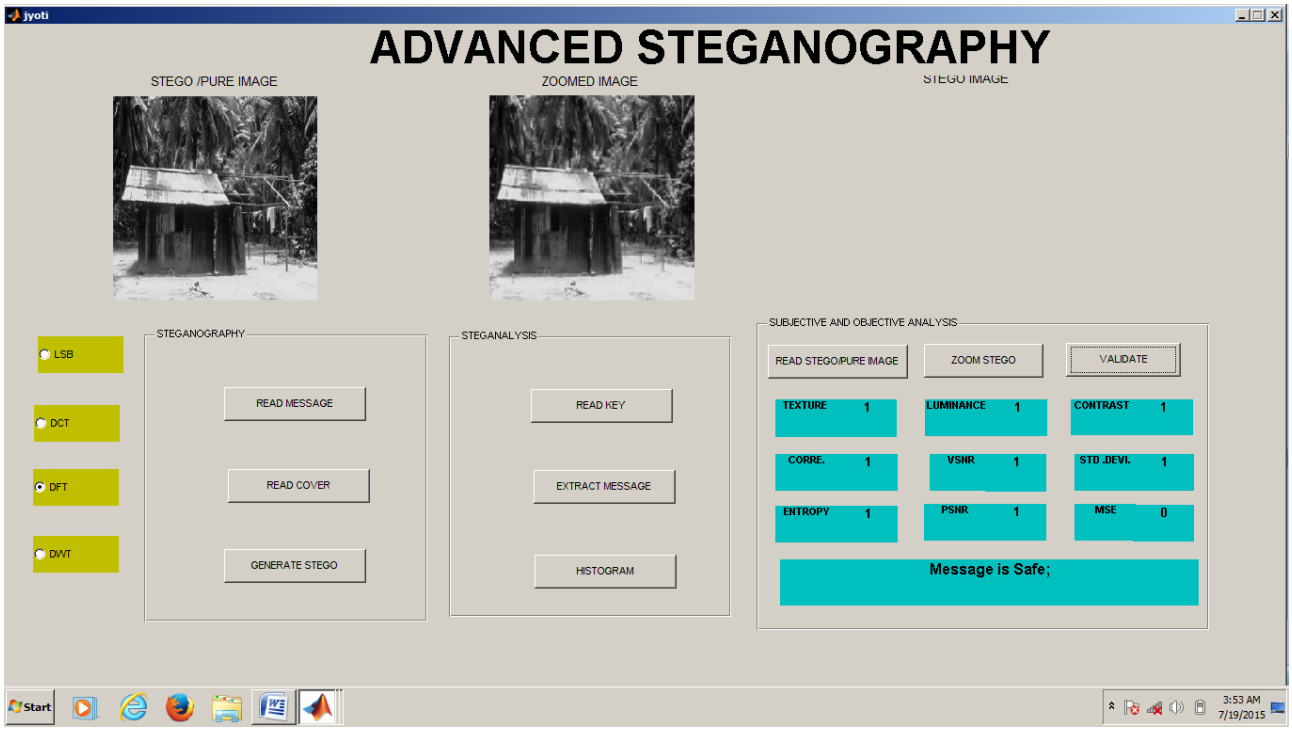


Figure 7: Subjective and Objective analysis.

5. Conclusion

As steganography is one of the data hiding techniques which is more widely used but in this project it basically focus on double compression so that it has more advantages than the other invented techniques. Due to double compression no one crack the data easily without knowing the key. This is the one part of project that is steganography. And another part is stegoanalysis. It is important part to save our country from terrorist for that purpose stegoanalysis is done. There are two categories of analysis that are subjective analysis and objective analysis. This is important to find out whether the information content secret data or not. This is the most robust method for steganography and stegoanalysis.

6. Future Work

1. In audio with image Steganography techniques can be implement
2. In video with image Steganography techniques can be implement
3. We can also improve this project for defense purpose.
4. In text with image Steganography techniques can be implement
5. We can embed voice recoganization system in our project.

References

[1] Hardik Patel, PreetiDave ”Steganography Technique Based on DCT Coefficients” International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717.

[2] Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt “Digital image steganography: Survey and analysis of current methods” Signal Processing 90 (2010) 727–752 Accepted 18 August 2009.

[3] Mehdi Kharrazi, Husrev T. Sencar, and NasirMemon “Image Steganography: Concepts and Practice” Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201, USA fmehdi, taha, memong@isis.poly.edu.

[4] L. Y. POR, B. Delina “Information Hiding: A New Approach in Text Steganography” 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008.

[5] Qian Wang Mechanical Engineering Penn State University “MATLAB Tutorial” MATLAB Fundamentals Plotting Figures, M-files, ODE Solver, Building Control Systems, Time Response, Root Locus, Frequency Response / Bode Plot SIMULINK.

[6] Soumyendu Das, Subhendu Das, BijoyBandyopadhyay, SugataSanyal “Steganography and Steganalysis: Different Approaches” soumyendu.das@gmail.com, subhendu.das@gmail.com.

[7] Amitava Nag, SushantaBiswas, DebasreeSarkar&ParthaPratimSarkar “A Novel Technique for Image Steganography Based on DWT and Huffman Encoding” amitava.nag@aot.edu.in, biswas.su@gmail.com.

[8] RajkumarYadav “ Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters” Assistant Professor U.I.E.T, M.D.U, Rohtak – 124001 (Haryana) rajyadav76@rediffmail.com, Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870.