International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Review of Comparative Evaluation : Image Steganography

Anjani Kumar

Cluster Innovation Centre, University of Delhi, Delhi, India

ABSTRACT

The main aim of this paper is to develop some algorithms for hiding the information in digital image that will not be predictable by the attacker except the recipients. Here, we have studied here two methods of spatial domain steganography and frequency domain steganography each and then hides the information to produce stego-image having property of robustness to visual and statistical attacks. Finally, comparisons are shown between the signals for the detection features.

Keywords: Steganography, LSB, DCT, Stego, JSteg, PSNR

I. INTRODUCTION

Steganography is an art and science of hiding information used for intelligence bureau, defence agencies etc., based applications [1]. Properly executed steganography allows a huge amount of data to be hidden in a file, (image, video, audio etc.) without making detectable changes to file. It can apply in different types of data, such as text, images, audio, and video.

Steganography can be of many types depending on the cover medium like Video Steganography, Audio Steganography, and Image Steganography etc. Image Steganography is vastly used because of popularity of digital image transmission on the internet. Image Steganography use redundancy of digital image to hide the secret information. It may be categorized into two categories namely spatial and frequency domain.

In case of spatial domain, the secret message or information are embedded in the pixels of image directly. In case of frequency domain, the secret image is first transformed to frequency domain, and then the messages are embedded into it.

II. METHODS AND MATERIAL

Information embedded in spatial domain can be subject to losses if the image undergoes any visual attack like compression, cropping etc. To improve upon this, we embed the information in frequency domain such that the secret information is embedded on the significant frequency components while higher frequency components are omitted. Frequency transform is first applied on the image then data is embedded by changing the values of the transformation coefficients accordingly.

A. LSB Substitution

Least Significant Bit (LSB) embedding is a simple procedure, which embeds the data into the cover so that it cannot be detected by a casual observer. This technique works as by replacing some of the information in a given pixel with information from the data in the image [2]. While it is possible to embed data into an image on any bit plane, LSB embedding is performed on the least significant bit(s), thus minimizes the variation in colors that the embedding creates. For example, embedding through LSB changes the color value by one. Embedding into the second bit plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel.

B. Distortion

Distortion techniques require the knowledge of the original cover image for decoding the hidden message. A sequence of modifications is applied to the cover image to get a stego-image in such a way that it corresponds to a specific secret message for embedding [3]. Receiver computes the differences with respect to the original cover image to determine modifications made by sender, which corresponds to the secret message.

Using a similar approach as in LSB, the sender first chooses l different cover pixels he wants to use for information transfer, where l is the length of the secret message. Such a selection can do again using pseudorandom number generators or pseudorandom permutations. If both communication partners share a stego-key k usable as a seed for a random number generator, they can create a random sequence k1… kl(m) and use the elements with indices for information transfer.

$$J_1 = k_1$$
$$J_i = j_{i-1} + k_1,\ i \geq 2$$

Thus, the distance between two embedded bits is determined in a pseudo random manner. Since the receiver has access to the seed k, which is used as a key and knowledge of the pseudorandom number generator, he can reconstruct k_i and therefore the entire sequence of element indices j_i. To encode a 0 in one pixel, the sender leaves the pixel intensity unchanged; to encode a 1, he adds a random value x to the pixel's color. Although this approach is similar to a substitution system, there is one significant difference, the LSB of the selected pixel do not necessarily give secret message bits. No cover modifications are needed when coding a 0. Furthermore, x can be chosen in a way that better preserves the cover's statistical properties. The receiver compares all l(m) selected pixels of the stego-object with the corresponding pixels of the original cover. If the i^{th} pixel differs, the i^{th} message bit is a 1, otherwise a 0. Here, we have taken the value of x as 1 so that minimum variation from cover image will be produced. We defined a middle level of pixel value, such that if the pixel value is greater than this value then x is added to pixel value otherwise x is subtracted from the pixel value. In this way, the high PSNR will be produced.

C. JPEG-JSteg

JPEG steganography is more important and popular because stego-image produced by these techniques are robust to compression. In this technique secret data is embed after quantization phase of JPEG compression. Only significant quantized DCT coefficients are modified according to secret bits. Remaining steps are similar to JPEG compression [4]. In this way, stego-image is produced in ".jpg" format directly. The basic flow diagram of embedding and extraction process is given in figure 1 and 2:

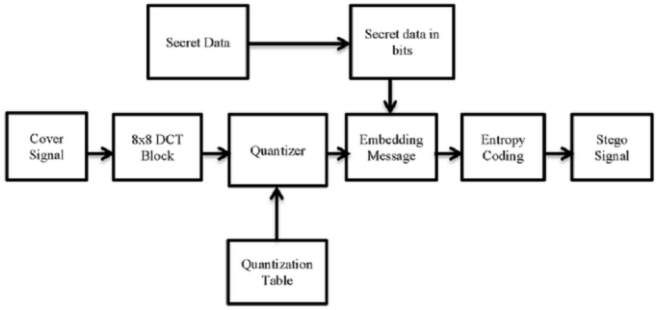

Figure 1. Block diagram of embedding process of JPEG Steganography.

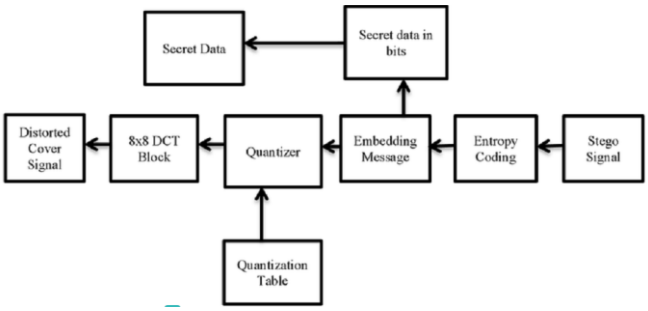

Figure 2. Block diagram of extraction process of JPEG Steganography.

There are some JPEG steganography techniques such as JSteg, Steghide, Outguess, F3, F4, and F5. In this paper, we have implemented JSteg and modified version JSteg DCT algorithm, in which secret message bits are, embedded in LSB of quantized DCT coefficients whose values are not 0, 1, or -1. Its execution steps are described briefly as follows. First, JPEG partitions a cover image into no overlapping blocks of 8x8 pixels, and then it uses DCT to transform each block into DCT coefficients. The DCT coefficients are scaled according to the quantization table. The embedding sequence employed in JPEG – JSteg is in the zigzag scan order. After embedding the secret message in each block, JPEG – JSteg uses Huffman coding, Run Length coding, and DPCM of

JPEG entropy coding to compress each block. Finally, JPEG – JSteg obtains a JPEG stego-image. The message capacity of JPEG – JSteg is limited. If there are many quantized coefficients equal to 0, 1, or 1, then the message capacity of JPEG –JSteg will be decreased. Besides, in DCT transformation, most important coefficients are located around the low frequency part. JPEG – JSteg modifies the quantized DCT coefficients right in the low frequency part. Therefore, the image quality of JPEG – JSteg is degraded, especially when the cover image undergoes a high compression ratio. The DCT is given as:

$$F(u,v) = \frac{1}{4}C(u)C(v) \cdot \sum_{x=0}^{7}\sum_{y=0}^{7}\left[f(x,y)\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right]$$

In this equation x , y , u , v ϵ {0 , 1 , … , 7} , f (x,y) is the particular pixel color space component , C (u) = 1/2 if u=0 and otherwise C (u) = 1.

D. DCT Replacement

The process of embedding data in this proposed algorithm is the same as JSteg algorithm in the first step, the only difference is in manipulation of coefficients. First step is to divide the cover image into the 8x8 blocks, and then each block is transformed to the DCT (frequency) domain. Similar to the JSteg algorithm, DCT coefficients are sorted in the increasing frequency order by zig-zag ordering method. So they stand in the frequency positions 0 to 63, the zero frequency is called DC and the rest are AC coefficients. Unlike the JSteg algorithm, which is applied on all AC coefficients, in this method the embedding, is done only on the n middle frequencies. Therefore, the visual quality of image can be improved after changing the DCT values in comparison to JSteg algorithm. As such, no bordering is there between middle and high frequencies. Here according to the experimental result of the algorithm, the last 15 coefficients are chosen as high frequency components and the other coefficients except the DC are named middle frequencies. Starting from the first coefficient in the middle frequencies area, the LSB of each coefficient is replaced with secret message bits. In this algorithm, parameter b is defined as the number of bits, which can be embedded in each coefficient [5].

For experimental setup, we have the following information available:

E. Dataset

The MATLAB tool is used to implement and simulate four-steganography techniques - JSteg and DCT replacement of transform domain and LSB and Distortion of spatial domain steganography. The dataset consists of several color images have taken from camera, which results for various color cover image for the different hidden information. The various simulation parameters are as in Table I:

Table I. Simulation parameter setup

Cover image pixel size (N x N x3)	N=256, 512, 1024
Secret text file size (kb)	1.5
Image type	Tiff, jpg
Simulation Tool	MATLAB 7.13.0.564
Pseudo Random Number Generator	MATLAB rng with key 2

F. Embedding Load

It is the size of the secret information that can be embedded in cover image (file) without corrupting the integrity of the cover image. It can be represented in bytes or bit per pixel (bpp). It depends upon the characteristics of cover image and the embedding algorithm used. The Table II shows the average embedding capacity of the 4 techniques for cover images for different resolutions:

Table II. Embedding capacity in the four techniques

Image Size	LSB Substitution Steganography	Distortion Steganography	Jsteg Steganography	DCT Replacement Steganography
256x256x3	23437	23437	157	4563
512x512x3	93750	93750	610	17339
1024x1024x3	393216	393216	3136	60687

III. RESULTS AND DISCUSSION

In this section, we have only taken two metrics, based on that it is easy to see the visual discrimination between the signals clearly.

A. MSE

The mean squared error (MSE) of an estimator (of a procedure for estimating an unobserved quantity) measures the average of the squares of the errors or

deviations—that is, the difference between the Estimator and what is estimated. Given a noise free M x N monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Mean Square error for different techniques with a fixed payload of size 3171 bytes for 256x256, 12864 bytes for 512x512 and 50736 bytes for 1024x1024 with different collection of images has been calculated in Table III:

Table III. MSE with different techniques

Image Size	LSB Substitution method	Distortion method	Jsteg method	DCT replacement method
256x256x3	0.1847908	0.001758	0.7001165	0.0176913
512x512x3	0.1147956	0.001099	0.5509096	0.0167923
1024x1024x3	0.3309332	0.001632	0.3509783	0.1639457

We can analyse from the results that MSE for spatial domain techniques is very less than that of for transform domain technique where the lossy compression step of JPEG compression i.e. Quantization is performed in the embedding process and hence very large MSE is produced and quality of cover image degraded more.

B. PSNR

It is the measure of quality of the image by comparing the cover image with the stego-image. High PSNR indicates good perceptual quality of stego-image. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Usually the images with PSNR value less than 40, will be extremely ruined and cannot be compared with the original image. The results of PSNR for all the techniques are in following Table IV:

Table IV. PSNR values with different techniques

Image Size	LSB Substitution	Distortion Steganography	Jsteg Steganography	DCT Replacement
256x256x3	55.4659	75.6791	49.6791	65.6532
512x512x3	57.5315	77.7203	50.7203	65.5209
1024x1024x3	52.9334	75.7986	52.6790	63.8368

C. Histograms

Histogram measures of the number of occurrence of pixels with respect to particular pixel value. During embedding pixel value changes hence number of pixel having a particular value changes. These changes can be used to detect steganography. We take histograms for the flower color image with size of (512x512) for all the four the techniques separately.

1) Histograms of spatial domain techniques

For spatial domain techniques, we have to take 3 histograms each for red, green and blue color plane. Hence 3 histograms of cover image, 3 histograms for stego-image and 3 differences are to be taken for analysis of one technique. Below in the figure 3 and figure 4 are the representation of the results for both the spatial domain techniques here the x-axis is the different color values and y-axis is showing the number of occurrence:

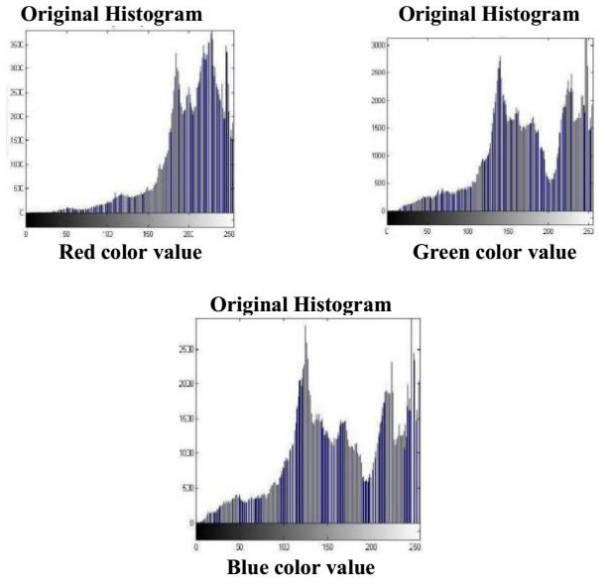

Figure 3. Cover image histograms for red, green and blue color plane respectively

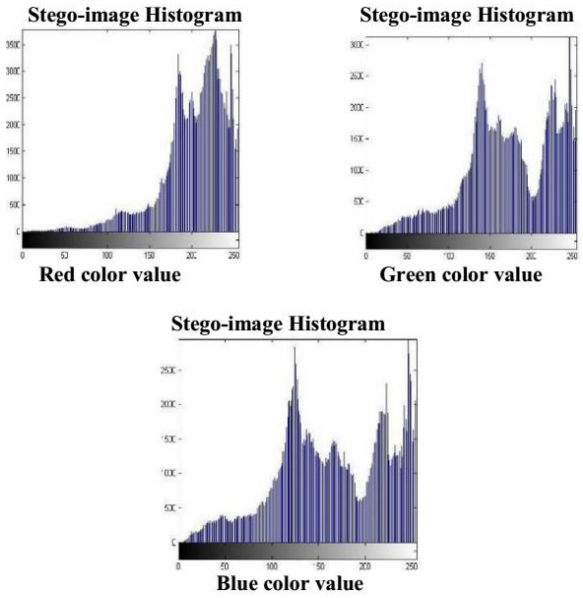

Figure 4. Stego-image histograms for red, green and blue color plane respectively

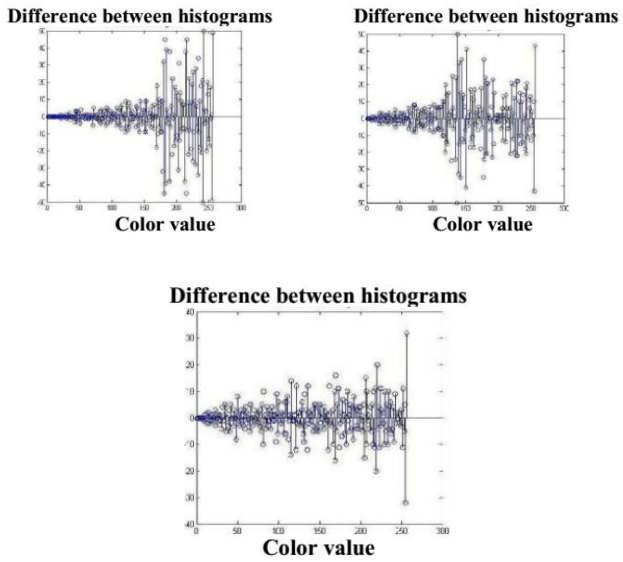

Figure 5. Difference between histograms of Cover image and Stego-image for red, green and blue color plane with secret file of 5 kb and (512 x 512 x 3) Cover image

We see that histogram of cover image and stego-image seems to be similar but by plotting difference between the two we can analyze the change in statistical properties of cover image in the figure 5 above (where x-axis is color value and y-axis is difference of occurrence). As the size of secret file increases the difference is increases which are shown in figure 6.

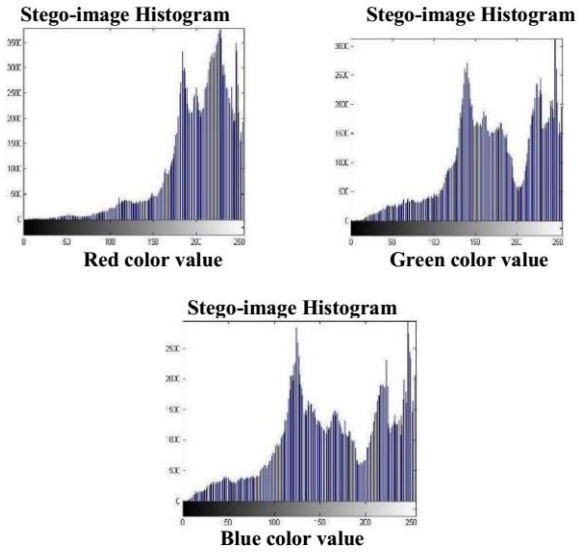

Figure 6. Stego-image histograms for LSB substitution method for red, green and blue color plane

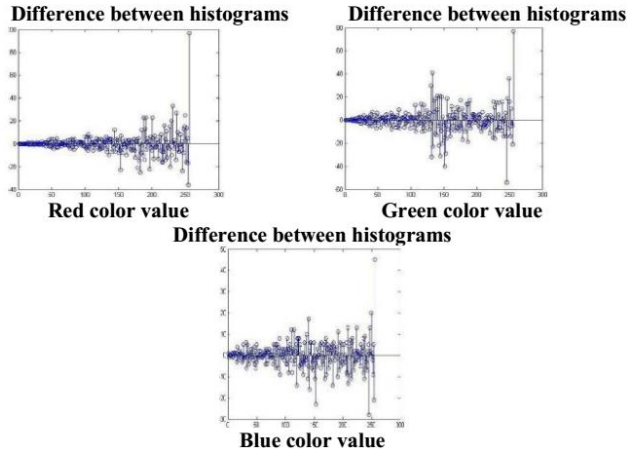

Figure 7. Difference between histograms of Cover image and Stego-image for 3 color plane with 512 x512 cover image

We see that difference between histograms by distortion technique is lesser than LSB substitution technique with same cover image and secret data file, which has been shown in figure 7.

2) Histograms of Transform domain techniques

For transform domain techniques quantized coefficients are used for calculation of histogram instead of pixel value. After data embedding progress in the cover image, the number of pixels with the same brightness level in the spatial histogram, and also number of DCT coefficients in the coefficient histogram will be changed. Because of the symmetrical property of Fourier transform, the images which are chosen as a cover media will have the symmetrical histogram. This means that the coefficient have equal abundance

around a central axis in the form of positive and negative values. After applying the steganography algorithm on the image, this symmetrical property in coefficient histogram will be eliminated, and this can be an indication of hiding something in the image. The more the outlet histogram of an algorithm is close to the original image, the algorithm have more efficiency and more robustness against the statistical attacks.

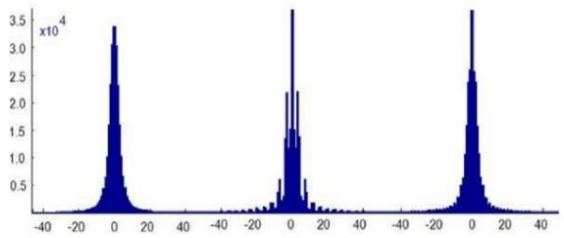

Figure 8. DCT Coefficient histogram for (a) Cover image (b) JSteg steganograhy (c) Replacement algorithm

As it can be seen in the above figure 8, the original histogram for cover image has a symmetrical structure. The results of JSteg and replacement algorithms are shown in figure (8-b) and figure (8-c). It can be seen that structure of figure (8-b) is different from the original one. However histogram of figure (8-c) which is the result of replacement histogram is more similar to the cover image histogram. Because of this similarity, detection of secret data, in replacement method, is more difficult against the steganography attacks is higher than the JSteg algorithm.

IV.CONCLUSION

Spatial domain techniques are easy means to embed data, but these are terribly sensitive to even little cover modifications. Hence the size of stego-image cannot be reduced. An attacker can simply apply signal processing techniques in order to destroy the secretly embedded information totally. In several cases even the minute changes resulting out of lossy compression systems results in total information loss. On the other hand transform domain methods hide messages in significant areas of the cover image which makes them even more robust for attackers, such as compression, cropping, and some image processing. So lossy compression e.g. JPEG compression can be implemented and size of stego-image can be significantly reduced. But it has a disadvantage that only slight data can be embedded in the cover image. The capacity of embedding of Jpeg steganography is very low than spatial domain techniques. The spatial domain techniques results in high perceptual quality, high PSNR, and high embedding capacity but lacks in providing robustness. On the other hand transform domain provide robustness while providing very less embedding capacity, low PSNR and low perceptual quality.

V. REFERENCES

[1] Judge J.C. (2001): Steganography: past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/stenganography/552.php.

[2] Cheddad Abbas, Condell Joan, Curran Kevin, and Kevitt Paul Mc (2010): Review Digital image steganography: Survey and analysis of current methods‖ in Journal Signal Processing Volume 90 Issue 3, March, Pages 727-752.

[3] Zaidan A.A., Zaidan B.B., and Jalab Hamid.A (2010): " A New System for Hiding Data within (Unused Area Two + Image Page) of Portable Executable File using Statistical Technique and Advance Encryption Standared ", International Journal of Computer Theory and Engineering (IJCTE), 2010, Vol. 2, No. 2, ISSN:1793-8201, Singapore

[4] Wallace, G. K (1991): The JPEG Still Picture Compression Standard, Communications of the ACM, Vol. 34, No. 4.

[5] Sheisi Hossein, Mesgarian Jafar, and Rahmani Mostafa (2012): Steganography: DCT Coefficient Replacement Method and Compare With JSteg Algorithm, International Journal of Computer and Electrical Engineering, Vol. 4, No. 4

[6] Kurak, C., and McHughes J (1992): "A Cautionary Note on Image Downgrading," in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, pp.153¬159.

[7] Bender, W., Gruhl D., and Morimoto N (1996): Techniques for data hiding, IBM Systems Journal, Vol. 35, No. 3&4.

[8] Jamil, T. (1999): Steganography: The art of hiding information is plain sight, IEEE Potentials, 18:01.

[9] El-Emam N.N (2007): Hiding a large amount of data with high security using steganography

algorithm, Journal of Computer Science 3 (2007) 223-232.

[10] Ibrahim R. and Kuan T.S (2010): Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, pp. 144-148.

[11] Provos N., Honeyman P (2003): Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) 32–44.

[12] Raja K.B., Chowdary C.R., Venugopal K.R., and Patnaik L.M. (2005): A secure image steganography using LSB, DCT and compression techniques on raw images, in: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP'05, Bangalore, India, 14–17 December 2005, pp. 170–176.

[13] Johnson N.F., Katzenbeisser S.C. (2000): A survey of steganographic techniques, in: S. Katzenbeisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood.

[14] Elbireki, Majdi Farag Mohammed, M. F. L. Abdulah, and Ali Abdrhman M. Ukasha. "Adopting a Robust Watermarked I'm age against Cyber Security Threats Using DCT and Ramer Method", 2014 5th International Conference on Intelligent Systems Modelling and Simulation, 2014.

[15] Vijayakumar, P., V. Vijayalakshmi, and G. Zayaraz. "An Improved Level of Security for DNA Steganography Using Hyper elliptic Curve Cryptography", Wireless Personal Communications, 2016.

[16] Chin-Chen Chang, Tung- Shou Chen, Lou – Zo Chung. "A steganographic method based upon JPEG and quantizat ion table modification", Information Sciences, 2002