A Comparative Analysis of Steganographic Data Hiding within Digital Images

P. Rajkumar
Caledonian College of Engineering
P.O Box 2322
CPO Seeb 111
Oman

R. Kar
National Institute of Technology
Durgapur
India

A. K. Bhattacharjee
National Institute of Technology
Durgapur
India

H. Dharmasa
Caledonian College of Engineering
P.O Box 2322
CPO Seeb 111
Oman

ABSTRACT

A huge deployment of effective steganography by several techniques with varying degrees of payload, peak signal to noise ratio (PSNR), robustness, perceptual transparency and so on has been evidenced. Steganography has been effective as an alternative to cryptography and has been projected to the forefront of digital security by the explosive growth in computational power, security awareness and through widespread intellectual pursuit. The current techniques for Steganography reviewed include substitution method such as least significant bit (LSB) and transform domain methods such as discrete cosine transform (DCT) and discrete wavelet transform (DWT). In this paper, the techniques involved with LSB, DCT and DWT are analyzed with the proper use of the performance metrics and then the techniques have been modeled by computer simulations. The results from simulation indicate that the LSB technique, although easy to implement and encode and having good payload capacity, is easily prone to statistical attack, since the histogram plots are revealing the data hidden within. On the other hand, transform domain techniques are more robust to statistical attacks but at the cost of reduced payload.

General Terms

Digital Security, Computational Power, Statistical attacks, Robust Algorithms.

Keywords

Steganography, Payload, PSNR, Histogram LSB, DCT, DWT, Steganalysis.

1. INTRODUCTION

Communication mechanisms have evolved a lot since the dawn of the human society. The onslaught of multimedia, World Wide Web (WWW) and the internet has enabled a massive explosion in the availability of visual means of presenting and preserving data in the form of animations, real-time audio clips, images, videos and holograms with equal access for all. As more and more transactions are conducted digitally, new needs, issues and opportunities arise. At times, there is a preference that only the intended recipient has the ability to decipher the contents of the communication. There is a need to keep the message secret. Although, encryption can be used to mask the meaning of a communication, instances exist where we would prefer that the entire communication process not be evident to any observer, keeping the communication a secret [1]. In this case we want to hide the matter. Here the difference between Cryptography and Steganography becomes evident, with the latter being a subtle means of hiding messages in various types of media. The Greek definition of Steganography roughly translates to "hidden writing." Digital Steganography is the art of hiding information through digital content in the internet. The 21st century has witnessed a massive proliferation in the utilization of Data Hiding techniques in digital imagery. The two broad techniques are Steganography and Watermarking. Messages can be hidden inside all sorts of cover information such as text, images, audio, video, making web pages an elemental means of action. These base images, texts or audio are referred to as cover and the result of combination of the cover and the message to hide is called stego. The most important property of a cover source is the amount of data that can be stored inside it, without being perceptible to an observer. When a cover is distorted, it will be suspicious and may be checked more meticulously. A cover with a secret message inside can easily be spread over the WWW or in newsgroups. Steganographic techniques can be used to hide the existence of communication within cover data, which is just a carrier of secret information. On the other hand, Watermarking gives significance to the cover works and the data hidden is of small, fixed size. Steganography can be used to hide information within innocuous images, like a weather map that conceals the existence of the communication [2]. The weather map is made available on an open channel for anyone to access, but only the intended recipient is aware of the hidden information and has the ability to extract it from the image. Modern Steganographic methods, which conceal the existence of communication, are needed to exploit contemporary modes of information exchange [3]. Measures of performance for these methods are needed to compare specific algorithms and determine appropriate uses. In Steganographic communication, it is found that capacity bounds for the message depend upon the actual data-hiding technique. It is pertinent therefore to maximize the payload or capacity, provide allowance for error-free recovery of embedded data, and provide resilience to removal, whilst concealing the existence of the embedded information from the observer. The applications of Steganography in military applications include spread spectrum and meteor scatter radio which gives various combinations of resistances to detection. Other applications include medical safety, indexing of voice mails etc. Steganographic methods can be classified into Spatial Domain Embedding and Frequency Domain Embedding. Spatial Domain Embedding comprises of the LSB method in which the least significant bits of the cover object are used to embed the message to be communicated secretly. As the resulting change in color is insignificant, the hidden image goes undetected by human vision. This technique enables high capacity embedding without rendering any significant changes to the cover image. The selection of LSBs could be random using a stego-key or could be confined to the noisy areas i.e., areas with large color variation of the image so as to generate least suspicion. The selection of LSB's could be done using a stego-key when security is the priority. Although the LSB method is a high capacity embedding technique, it leaves behind statistical evidences making it vulnerable to attacks [17]. The most popular methods under Frequency Domain Embedding are the Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). In DCT method, the image is first transformed to frequency domain which results in coefficients. The Discrete Cosine coefficients of hidden image are used for embedding the hidden message into the cover image such that the distortion is minimum and no significant changes in the statistical features of the Stego image with respect to cover image occur. In DWT method, the image is decomposed based on frequency components into detailed and approximation bands, also called the sub-bands. Detailed band contains vertical, horizontal and diagonal bands. The total Information of the image is present in the approximation band. Hence the payload is normally embedded in the detailed band and rarely in the approximation band. In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect [4]. Another approach combines spread spectrum communication, error control coding and image processing to hide information in images [11]. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. The modern approach uses Genetic Algorithms [6], which offers immunity measures. Steganalysis [4,5] is the art of attacking the covert data in images and has also been very popular among researchers. The goal of Steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information. The classical "Prisoner's Problem" [17] is used to provide benchmarking. The rest of the paper is structured as follows: Section 2 does a literature review of the existing Steganographic methodologies practiced. Section 3 focuses on the Analysis of the techniques. Section 4 provides the Simulation results and finally Section 5 concludes with proper inference.

2. LITERATURE REVIEW

Shih *et al.* [1] has made a review of existing data hiding mechanisms to come up with performance metrics to compare the image Steganographic techniques. The capacity or payload measure is a much important performance metric. The rate of success is in terms of hiding and recovery of significant amount of payload within digital images without being detected by an observer. One has to set the upper and the lower Steganographic capacity bounds and work to achieve a new bound for the capacity of the channel. Shih *et al.*[3] considered spatial domain techniques such as Least Significant Bit (LSB) embedding, LSB matching and pixel value differencing and inferred that these techniques provide a very high Payload or Capacity and they fail visual inspection and the LSB algorithm is computationally efficient and it takes less time to do the embedding. The PSNR of the data hiding is also the highest. The main disadvantage is that they can easily be attacked by statistical detection methods, and so they don't offer much immunity.

Kharrazi *et al.* [2] elaborated upon data hiding using Transform domain techniques. The Discrete Cosine Transform (DCT)-based technique provides very robust data hiding and is quite immune to basic attack, but the drawback is lesser Capacity, lesser PSNR and takes more computational time. Wavelet based Image hiding is a superior transform domain technique in the sense that it is not much affected by statistical attacks. It offers better resilience to message removal. But the problem is it is computationally time consuming, takes less payload and also it fails visual inspection in some cases. The other techniques which are not in spatial or transform domains techniques such as spread spectrum methods can be applied to steganography with goals of high payload, reliable recovery, and robustness to removal and imperceptibility. Shih *et al.* [1] has propounded that since the rounding error problem with lossy techniques limits the capacity of message, a Genetic Algorithm (GA) approach is envisaged, which may result in increased efficiency. The GA approach also has the added advantage of providing immunity to conventional attach. Raja *et al.* [6] have applied the Discrete Cosine Transform and Discrete Wavelet Transform to the payload. Genetic Algorithm is used to generate many stego-images based on Fitness functions; one of these which give least statistical evidence of payload is selected as the best stego image to be communicated to the destination. It is perceived to have an improvement in BER, PSNR and embedding capacity. Cheddad *et al.* [8] has performed a comprehensive review of the existing steganographic techniques with detailed recommendations. Atabyl *et al.* [10] have analyzed the DWT embedding process to enable robust data hiding.

3. ANALYSIS OF SYSTEM

3.1 Steganographic data hiding system

As shown in figure 1, the Steganographic system comprises of a stego system encoder that accepts the cover image, the message to be hidden and the optional key to generate the stego image that is identical to cover image as per the human visual systems (HVS). The encoder implements the algorithm for Steganographic data hiding, whether it be substitution technique or transform technique. The cover can be transmitted via a channel or uploaded to the internet. At the other end the decoder works on the stego image with the optional key to extract the hidden message.

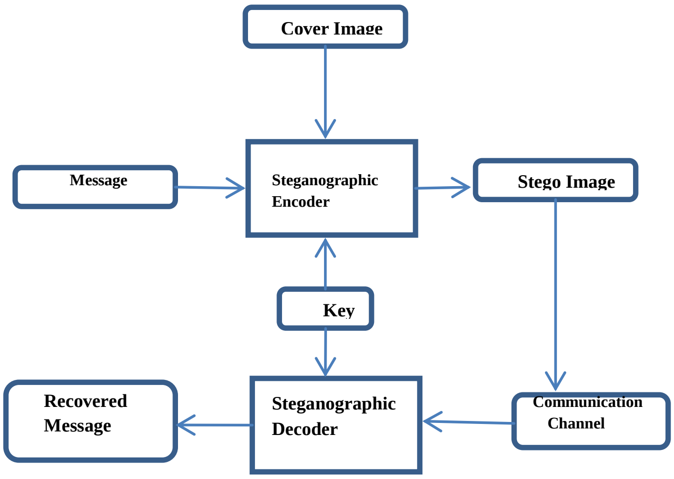

Fig 1 Steganographic data hiding system

3.2 Least Significant Bit (LSB) data hiding

Least significant bit (LSB) substitution is a simple approach to embed information in a cover image. The least significant bit of some or all of the bytes inside an image is interchanged with a single bit of the secret message. A 24-bit image represents each pixel by three bytes. So it is possible to embed three bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example representation for 3 pixels of a 24-bit image can be as follows:

- (00101101 00011100 11011100)
- (10100110 11000100 00001100)
- (11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

- (00101101 00011101 11011100)
- (10100110 11000101 00001100)
- (11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only 3 bits needed to be changed according to the embedded message. On the average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye and thus the data hiding is successful. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference. In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed [8]. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key. In its simplest form, LSB makes use of BMP images, since they use lossless compression, but other formats can also be used. Generally embedding can also be done up to the 4th LSB instead of confining to just the LSB, but at the cost of more visual distortion to the cover image. Again proper trade-off between the payload and cover image distortion is necessary.

3.3 Discrete Cosine Transform (DCT) method

The schemes of the second kind embed the secret data within the cover image that has been transformed using DCT (Discrete Cosine Transform). The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data. Tseng and Chang in [14] proposed a novel steganography method based on JPEG. The DCT for each block of 8×8 pixels was applied in order to improve the capacity and control the compression ratio.

Let I(x,y) represent a gray scale cover-image with x = 1,2,…….,M and y = 1,2,…….,N. This M × N cover image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of the L = M×N / 64 blocks. The mathematical definition of DCT is:

Forward DCT:

$$F(u,v) = C(u).C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y).\cos\left(\frac{(2x+1)u\pi}{2N}\right).\cos\left(\frac{(2x+1)u\pi}{2N}\right) \quad (1)$$

if u=v=0, C(u)=C(v)=√1/N; otherwise C(u) =C(v) =√2/N,

Inverse DCT:

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u).C(v).F(u,v).\cos\left(\frac{(2x+1)u\pi}{2N}\right).\cos\left(\frac{(2x+1)u\pi}{2N}\right) \quad (2)$$

3.4 Discrete Wavelet Transform (DWT) method

Many practical tests propose to use the Wavelet transform domain [10] for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information-Hiding system features. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain.

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or bi-orthogonal scalar or multi-wavelets. The DWT used in this paper is implemented using the functions available with MATLAB with haar wavelet. The 2-D DWT leads to a decomposition of approximation coefficients at level *j* in four components which are, the approximation at level *j+1*, and the details in three orientations (horizontal, vertical, and diagonal).

3.5 Performance Metrics

For data hiding, the main objectives are that the embedded data must be imperceptible to the observer, and it should have maximum payload possible. It is difficult to quantify how imperceptible embedded data is. In the case of image steganography, the typical observer's detection resources include the HVS and computer analysis. The imperceptibility of the embedded data is indicated by illustrating the original image and its counterpart with embedded data so that their visual differences, if any, can be determined. The relationship between the display and the human visual system (HVS) can be best expressed by mathematical relationships of Image Quality Measures [2] on the basis of the fact that Steganographic schemes leave statistical evidence that can be used to quantify the hidden content in the stego image relative to the cover image. The IQMs based on pixel distance include Average Distance (AD) and Euclidean Distance (L2), while IQMs based on correlation of the content of the images include Structure Content (SC), Normalized Cross-Correlation (NCC) and finally IQMs based on mean square error include

Normal Mean Square Error (MSE) and Peal Signal to Noise Ratio (PSNR). Let the original image's pixels be represented as C(i,j) and the stego image pixels as S(i,j) for fixed image size of M x N. Then the following equations [1] can be used to estimate the IQMs.

$$AD = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}([S(i,j) - C(i,j)]) \qquad (3)$$

$$SC = \sum_{i=1}^{M}\sum_{j=1}^{N}([C(i,j)])^2 / \sum_{i=1}^{M}\sum_{j=1}^{N}([S(i,j)])^2 \qquad (4)$$

$$NK = \sum_{i=1}^{M}\sum_{j=1}^{N}([C(i,j)].[S(i,j)]) \quad / \sum_{i=1}^{M}\sum_{j=1}^{N}([S(i,j)])^2 \qquad (5)$$

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}([S(i,j) - C(i,j)])^2 \qquad (6)$$

$$\mathrm{PSNR} = 10 * \log_{10}\left(\frac{255 * 255}{\mathrm{MSE}}\right) \qquad (7)$$

4. SIMULATION RESULTS

Simulation was carried out using the main techniques of steganography applied to simple gray scale images such as Baboon, Lena, Cat, and so on. In the first experiment, LSB technique was used to hide a message within the image as indicated in Fig 2. The message was an arbitrary string of 72 characters and the statistics of the simulation are indicated below in Table 1. The extraction process correctly produced the same string. As clearly shown in Fig 2, the stego is identical to the cover and hence fails the HVS detection, but the histogram plot reveals the differences. The "pair effect" as referred to in [8] is clearly evidenced in the stego image histogram. This effect is observed due to the usage of the modulus operator, but cannot be generalized. The modulus operator used in the embedding process acts as a means to generate random locations to embed data and as the number of bit planes increase the effect is very evident. The embedding process was applied for LSB and up to 4th LSB resulting in varying statistical indications. The embedding time is naturally longer for the latter and the MSE figures are larger with corresponding lesser values of PSNR.

Table 1 Test results for sample LSB Embedding

Sl. No	**Characteristic or Metric**	**Numeric al value**
1.	Number of Ascii characters Hidden	72
2.	Number of Bits Hidden:	576
3.	Number of Bits Space Available for Hiding	262144
4.	Utilization	0.21973 %
5.	Mean Square Error (MSE)	0.5012
6.	Peak Signal to Noise Ratio (PSNR)	51.1304
7.	Normalized Cross-Correlation	0.9965
8.	Average Difference	0.5001
9.	Structural Content	0.9867
10.	Normalized Absolute Error	0.0039

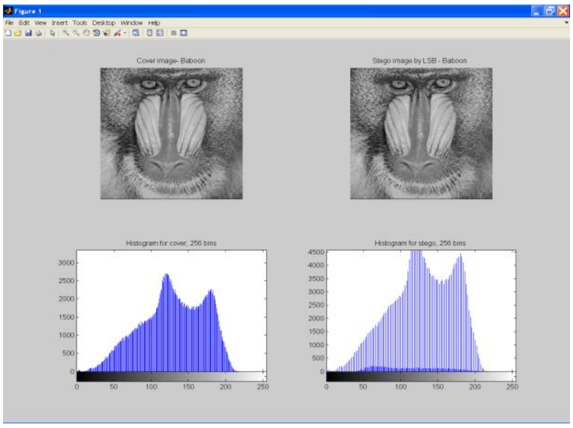
Figure 1
File Edit View Insert Tools Desktop Window Help
Cover image- Baboon
Stego image by LSB - Baboon
Histogram for cover, 256 bins
3000
2500
2000
1500
1000
500
0
0
50
100
150
200
250
Histogram for stego, 256 bins
4500
4000
3500
3000
2500
2000
1500
1000
500
0
0
50
100
150
200
250

Fig 2 Test results for LSB Embedding

The second set of experiments used the DCT embedding approach, whereby the cover images was initially segregated into 8 x 8 blocks of pixels and DCT was performed on each block with message hiding being done in the LSBs of the resulting non-zero coefficients. The stego image was got by inverse DCT approach and the results are depicted in Fig 3 as well as Table 2. Here the substitution was performed in the frequency domain. The same hidden message of 72 characters was used in this experiment. The stego is identical to the cover and also the stego histogram plot closely resembles the histogram of the cover, hence eliminating first order statistical detection. But the resulting PSNR figures are lesser than that of the substitution approach and also arbitrarily increasing the length of the hidden message produces error and corresponding distortions, clearly indicating the use of lesser payloads with this approach. Computation times are higher as expected.

Table 2 Test results for DCT Embedding

Sl.No	**Characteristic or Metric**	**Numerical value**
1.	Mean Square Error	7.0277
2.	Peak Signal to Noise Ratio	39.6627
3.	Normalized Cross-Correlation	0.9998
4.	Average Difference	9.1553e-005
5.	Structural Content	1
6.	Normalized Absolute Error	0.0042

The third experiment used the DWT approach and the data hiding was done within the coefficients of the pixels and the complete details are depicted in Fig 4 and Table 4. The histogram plots are identical as that of the cover.

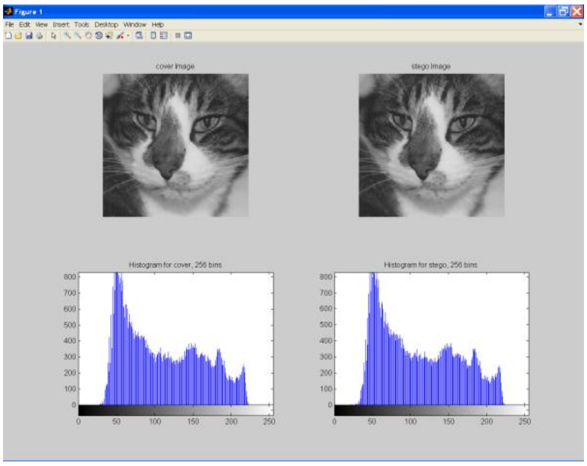
Figure 1
File Edit View Insert Tools Desktop Window Help
cover image
stego image
Histogram for cover, 256 bins
Histogram for stego, 256 bins
800
700
600
500
400
300
200
100
0
0
50
100
150
200
250

Fig 3 Test Results-DCT Steganography

Table 4 Test results for DWT Embedding

Sl.No	**Characteristic or Metric**	**Numerical value**
1.	Mean Square Error	0.1326
2.	Peak Signal to Noise Ratio	56.9044
3.	Normalized Cross-Correlation	1
4.	Average Difference	1
5.	Structural Content	1
6.	Normalized Absolute Error	9.7853e-005

From the simulation results run on several images, it is found that generally the LSB approach is very useful for very large payloads that can be embedded within bmp images, but the statistics are easily evident by means of histogram plots. The transform domain techniques prevent detection of the statistics in the frequency domain, although they generally do not support very large payloads like the LSB method, due to the constraints of hiding within the coefficients.

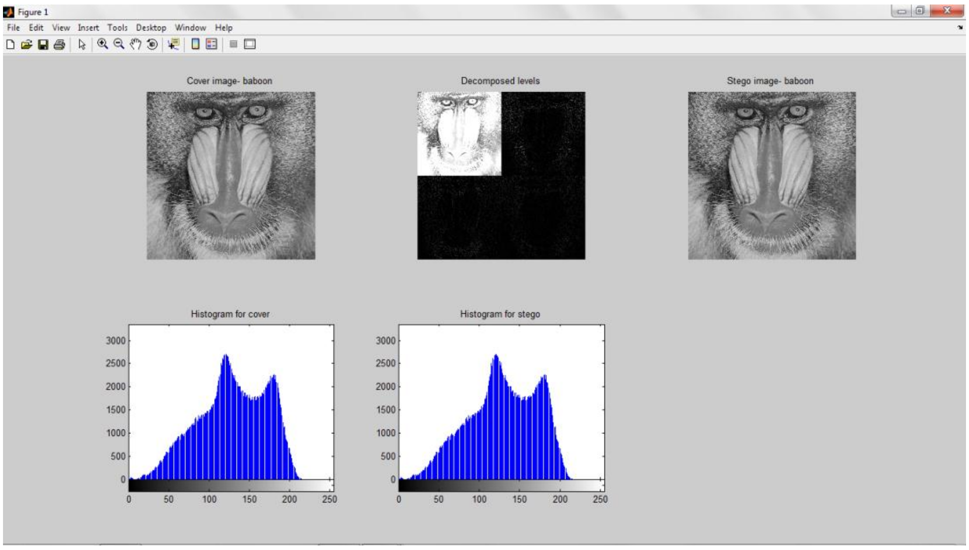

Fig 4 Test Results-DWT Steganography

5. CONCLUSION

This comparative analysis has presented a background discussion on the major algorithms of steganography used within digital images. The standard techniques of spatial domain such as LSB as well as transform domain techniques, DCT and DWT have been analyzed at length. It is found that the LSB technique enables more payload and larger PSNR, but the resulting stego image is more susceptible to statistical attacks as revealed by the histogram plots. Generally, it is inferred that transform domain mechanisms are not too susceptible to attacks, especially when the hidden message is not too large. This is due to the reason that the alteration of coefficients in the transform domain requires to keep distortion at a minimum at the price of lesser message hiding. So it is evident that transform domain mechanisms have lower payload compared to spatial domain algorithms. In essence, there is always a trade-off between robustness and payload. The future work would focus on applying optimization techniques to locate the specific pixels within the cover image to be used for data hiding with the goal of minimizing easy detection of the first order and second order statistics of the stego images.

6. ACKNOWLEDGMENTS

This work is part of the first author's PhD research which is under the staff development program of the Caledonian College of Engineering, Oman and National Institute of Technology, Durgapur, India.

7. REFERENCES

[1] Frank Y.Shih, “Digital Watermarking and Steganography- Fundamentals and Techniques”, CRC Press 2008.

[2] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, “Performance study of common image steganography and steganalysis techniques”, Journal of Electronic Imaging 15(4), 041104 Dec 2006.

[3] Mohammad Ali Bani Younes and Aman Jantan, “ A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.

[4] Hany Farid,” Detecting Steganographic Messages in Digital Images”, Department of Computer Science Dartmouth College Hanover NH 03755. Department Notes. http:// www.cs.dartmouth.edu/farid/ publications/tr01.pdf

[5] Ismail Avcıbas, Nasir Memon and Bülent Sankur, *“*Steganalysis Using Image Quality Metrics”, IEEE Transactions on Image Processing, Vol. 12, No. 2, February 2003.

[6] K.B. Raja, Kiran Kumar K., Satish Kumar N., Lakshmi M.S., Preeti H.,Venugopal KR., and Lalit M. Patnaik, “Genetic Algorithm Based Steganography Using Wavelets”, Lecture notes in Computer Science. P. McDaniel and S.K. Gupta (Eds.): ICISS 2007, LNCS 4812, pp. 51–63, Springer-Verlag Berlin Heidelberg.

[7] R.Amirtharajan, R.Akila, P.Deepika, “A Comparative Analysis of Image Steganography”, International Journal of Computer Applications (0975-8887) Volume 2 – No.3, May 2010.

[8] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current methods”, Elsevier, Signal Processing 90 (2010) 727-752.

[9] Digital Image Steganography – A Gentle Overview, Pradeep Kumar Saraswat and RK Gupta, International Journal of Computer Science and Information Technology, Vol. 2 (2), 2012, 129-136

[10] Ali Al-Ataby1 and Fawzi Al-Naima2, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, the International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010

[11] Lisa M. Marvel, Charles T. Retter, Charles G. Boncelet Jr.: Hiding Information in Images. 396-398 Proceedings of the 1998 IEEE International Conference on Image Processing (ICIP-98), Chicago, Illinois, October 4-7, 1998. IEEE Computer Society, 1998, ISBN 0-8186-8821-1, Volume 2

[12] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen,” IEEE Computer magazine, *February* 1998, pp. 26-34.

[13] Johnson, N. F., Jajodia, S. Steganalysis of Images Created Using Current Steganography Software. [online] 1998.
Available at http://www.jjtc.com/ihws98/jjgmu.html.

[14] Johnson, N. F., Jajodia, S. Steganalysis: The Investigation of Hidden Information. [online] 1998 September.
Available at http://www.jjtc.com/pub/it98a.htm.

[15] Wikipedia - The Free Encyclopedia. Steganalysis. [online] 2004 May. Available at http://en.wikipedia.org/wiki/Steganalysis.

[16] Petitcolas, F.A.P., Anderson, R., Kuhn, M.G., "Information Hiding - A Survey", July1999, URL:http://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf

[17] Ingemar J. Cox, Mattew L.Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Second Edition, Elsevier, Morgan Kaufmann Publishers Series in Computer Security, 2008.

[18] B.B Zaidan, A.A Zaidan, Alaa Taqa, Fazida Othman, “Stego – Image Vs Stego-Analysis System”, International Journal of Computer and Electrical Engineering, Vol. 1, No. 5, December 2009.

[19] Lifang Yu, Yao Zhao, Rongrong Ni and Ting Li, “Improved Adaptive LSB Steganography based on Chaos and Genetic algorithm”. EURASIP Journal on Advanced in Signal Processing 2010.

[20] Rafael C.Gonzalez, Richard E. Woods, Steven L.Eddins, “Digital Image Processing Using MATLAB’ Pearson Education, 2004.