Implementation of Image Steganography in Image by using FMM nested with LSB Substitution

Praneeta Dehare[1]
M.E. (CTA) Scholar: Department of Computer Science and Engineering
SSGI, SSTC Bhilai
Bhilai (C.G.), India
praneeta0511@gmail.com

Padma Bonde[2]
Sr. Associate Professor: Department of Computer Science and Engineering
SSGI, SSTC Bhilai
Bhilai (C.G.), India
pjyash2004@yahoo.com

***Abstract*—**Steganography allows intended recipients to communicate secretly, where steganography is a technique of hiding secret information inside an appropriate multimedia carrier e.g. Image, Audio, and Video files. In today's era data information available electronically, so these information can be transmitted over wireless communication. The data information can leak from the medium if it is not secured. So, the main goal of steganography is to communicate very securely. In this paper image steganography has been used where a secret image hide into an image called cover image and both images get embedded by using two techniques. The first technique called Five Modulus Method (FMM) and second is LSB substitution method. Both these techniques applied on images separately while embedding the secret image into cover image. In embedding process, secret image is horizontally divided into two equal parts. The first upper half part embedded by applying FMM algorithm and second lower part of secret image embedded through LSB substitution. A private stego-key also used when both images embedded with the five modulus method, which makes detection of secret image from cover image more difficult for any intended recipients. The visual quality of both the embedded image and extracted image is good that has been proven by getting higher PSNR and lesser MSE value.

Keywords- *Cryptography, Image Steganography, Five Modulus Method, LSB Substitution, Security, PSNR, MSE.*

*****

I. INTRODUCTION

In today's electronic era, to providing security on internet communication the steganography techniques are used. It is very important to keep message secure while it transmitted over the communication channel. Steganography is a word of Greek origin and means "concealed writing" from the Greek words where steganos stands for covered or protected and graphei is for writing, which has originated far back since 440(B.C.). Steganography is based on hidden communication and this technique strives to hide the existence of the information itself from the observer. It has an ability to hide information in cover media, so that only intendant recipients know that the message transmission is taking place.

The rapid growth of wireless communication has increased through the development of electronic devices. When any confidential information has shared between two parties the security and privacy has desired in wireless communication. Many hackers try to know the information which is transmitting over the channel. So the possibility of intrusion increased when the systems used wireless communication extensively. Therefore transmission of confidential data over the network becomes dangerous for user and developers. To overcome on this problem steganography has used through digital media which includes text, images, audio and video files. Steganography and Cryptography are counter parts in digital security [1]. The main advantage of steganography over cryptography is that the cryptography allowed the unintended recipients to detect the transmission of information on channel; it only keeps secret the contents of information, where steganography hides the existence of information.

To know the basic features of Steganography and Cryptography, a comparison table shown below –

TABLE I. COMPARISION OF STEGANOGRAPHY AND CRYPTOGRAPHY

Area of comparison	**Steganography**	**Cryptography**
Objectives	Keep the existence of message secret	Keep the contents of message secret
Applications	Used to secure information from unauthorized persons or intruders	Used to secure information from unauthorized persons or intruders
Specific Technical Problem	• Confidentiality • Identification and authentication	• Confidentiality • Data integrity • Identification and authentication • Non-repudiation
Services offered for security	• Key distribution • Steganalysis	• Key distribution • Government law and rules • Cryptanalysis

Steganography is an emerging field in computer science, cryptography and communication media. Steganography has intended by its recipients who involved into communication as the solution to provide security by hiding the secret message into any other kind of digital media. Steganography is also used for secret communication like cryptography, but objectives of these two technologies are differing. The difference between these two can define as - Cryptography means "secret writing" where steganography refers to "covered writing".

Secret data can be hiding inside any cover media. According to R. Doshi, P. Jain and L. Gupta [2], the procedure for steganography technique can be described as:
cover_medium + hidden_data + stego_key = stego_medium.

Steganography is mainly use to prevent detection of secret information from the unauthorized parties. To concealing message steganographic techniques have been in use for hundreds of years, but enhancement of electronic format new techniques arrives for information hiding. Steganography can be portioned into two parts –

i. Fragile

In fragile steganography, when information embedded into a file that can be easily destroy [4]. Thus this method is not suitable to record any copyright holder of the file because it can be easily modify or remove.

ii. Robust

The main aim of robust steganography is to embed in that way which cannot be easily destroyed. However no mark is truly unbreakable, a system can be considered robust if the lots of modification have been applied to extract the mark and not succeed to get the information.

Working mechanism of steganography –

In general there is no need of using any key for secret communication is "pure" steganography. But now these days there are other variations on these techniques where some of the techniques implement a key. The digital and modern steganography could be implemented on any kind of digital media like text files, image, audio or video.

In the process of image steganography the secret information could be embedded into cover image by using some algorithm. The combined data which holds the secret information called stego image, transfer to the communication channel whereas this stego image transmitted to the receiver and receiver extract the secret information from the stego image.

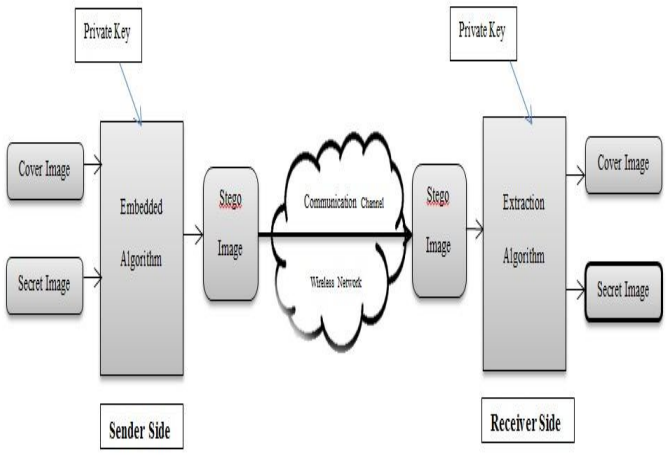

Figure 1: Working principle of Steganography

On the basis of media files steganography can be implemented on following four ways –

- Using Text files,
- Using Image files,
- Using Audio files,
- Using Video files.

II. Related Work

To hide any data information into any digital content could be done by steganography techniques without causing perceptual. This process embedded the secret information into any digital files. In image steganography technique many different types of steganographic schemes have introduced with various types of images. To get hide data into any digital media could be done with some popular techniques like watermarking, steganography and cryptography. In the field of steganography technique many research have done in ancient Greek.On the past decades of ancient Greek a secret data tattooing on the shaved head of a messenger and before sending him to the destination letting his hair to grow back. A popular method used in around 400 B.C., where the document marked with invisible ink like lemon juice.

There are various techniques proposed for implementing image steganography. On the basis of image format a popular Spatial Domain technique called Least Significant bit is the simplest and widest known steganography method which replaces the least significant bit of pixels selected to hide the content that holds information. The detail discussion on LSB could be found in [5]. In [6] and [7] some more steganography framework has proposed by using LSB substitution algorithm. Further an improved LSB substitution method used by V. K. Sharma and V. Shrivastava in [8], where secret image's MSB get embedded in to the cover image's LSB. A. Sharma, A. Agrawal and V. Kumar introduced a technique [9], where large amount of data could be hidden in enciphered with the help of secret key, which is then embedded at the end of image and then again deciphered with the help of same key. There are many steganography techniques to hide data inside in image discussed by many researchers in [10-13]. El-Sayed M. El-Alfy and Azzat A. Al-Sadi [10] used a method depends on pixel-value differencing, where the gray scale/color changes by adopting the number of embedded bits, which leads to increase capacity of embedding without losing quality of image.

Joyshree Nath and Asoke Nath [11] used a randomization method where the encryption and decryption takes place for generating the randomized key matrix. The two methods have used by them (i) the secret message encrypted, and (ii) the encrypted secret message inserted into the cover file. Ajit Danti and Preethi Acharya [12] presented, a Transform Domain based novel image steganography method that uses randomized bit embedding. The method follows two processes; first the Discrete Cosine Transform (DCT) of the cover image obtained then the stego image constructed by hiding the secret image in Least Significant Bit of he cover image in random locations. Matus Jokay and Tomas Moravcık [13] deal with the steganographic algorithm LSB (Least Significant Bits) in images (JPEG). The target is to minimizing of the number of modified DCT coefficients using Hamming codes. Also, good theoretical knowledge about steganographic technique and steganalysis could be studied in [14-16].

III. Basics of Data Embedding

The information or data which can any kind of digital files like plain text, cipher text, image, audio or video has embedded into cover object by using some steganography technique. The

 ISSN: 2321-8169
3663 - 3667

three features; security, capacity & robustness have involved for information hiding. Capacity refers to the amount of information that could be hidden in the cover object, security can say an unauthorized recipient's inability to detect secret data, and robustness is on to the amount of modification on stego medium can withstand before an adversary can destroy hidden information [13]. For embedding the information this paper uses image steganography. In image steganography technique an image that holds the secret information called cover image. The message which has to hidden is secret information of any kind of digital file. The steganography approaches for data hiding into an image divided into two types – (i) Spatial/Time Domain – This technique embedded message in the intensity of the pixels directly. (ii) Transforms Domain – In this domain data embedding is done in transform domain with a set of transform coefficients. Watermarking and steganography both are relates with information hiding system, where watermarking concentrate on to the high level of robustness and steganography focuses on security and capacity of the embedded data. When the steganography communication is taking place between intended recipients it is necessary that they know the secret key for embedding the secret data into cover media.

Many different types of techniques used to hide information in image. Some known methods which included the secret data into image are;

- Least significant bit insertion,
- Masking and filtering and,
- Transformation techniques and algorithm.

The above mentioned techniques could be implemented with varying degrees of success on different image files [16].

IV. METHODOLOGY

This paper used two methods, first Five Modulus Method proposed by Firas A. Jassim [3], and the second is the simplest and widest known steganography technique called Least Significant Bit. The proposed method intends to use of image steganography, where a secret image can transfer in a cover image by nesting the five modulus method with LSB substitution technique.

In proposed technique,

- The secret image gets partitioned into two parts. The first part of the image hides into cover image by using Five Modulus Method. Moreover, a private stego-key also combined with FMM algorithm to make it difficult for any unauthorized recipients to extract the secret image from the cover image.
- The stego image has sent over the communication medium and receives at destination, where the secret image needs to be transferred.
- On the destination point receiver get the stego image, and by applying the same private stego key and algorithm the secret image extracted from the cover image.

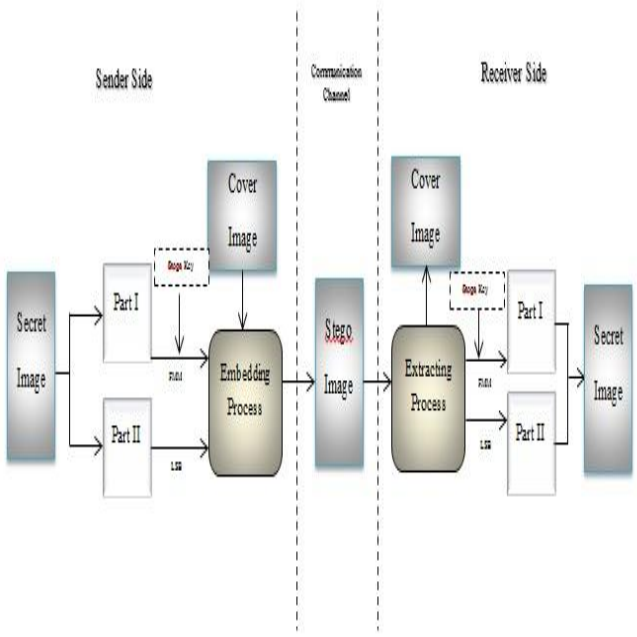

Figure 2: System Architecture

Five Modulus Method

The FMM algorithm use an idea is to transform the whole image into multiples of five. This technique used a digital image. Digital Image Background – A Digital image can represents as a rectangular array of pixels, arranged in M (row size in integer) X N (column size in integer) array. In digital color image, each pixel stored into three bytes; the pixel of array constructed by combining 3 different channel (RGB), where each channel represent a value from 0-255. To demonstrate the pixels value and place we can partition the image in no of k x k windows. The FMM method would be applied for both the cover and the stego images. Private Stego Key - Stego-key helps to recover the hidden information. It works as a password between the intended recipients. In proposed methodology the stego-key is used for forward shifting of stego pixel either horizontally or vertically on 4x4 windows which contains 16 positions.

Least Significant Bit method

In image steganography Least-Significant Bit strategy is one of the simplest and widest known algorithms. The idea behind this algorithm is that by maintain the good quality of image by changing the negligible variations to each pixels of the image so that the visibility is indictable. This algorithm uses only the least-significant bit of each pixel value to encode the secret message. This technique was originally designed to work on gray scale images. But later it extended to color image by treating each color plane as a single plane in which data has inserted in the LSB. Because of applying this algorithm resultant variation is so small and manipulation has very little effect on appearance of the cover object. But, this algorithm limits the amount of information data that can be contained, since the secret message must be scaled to fit into the least significant bits of each pixel value of cover object.

The basic ides for flow of execution has shown in below figure 3.

ISSN: 2321-8169
3663 - 3667

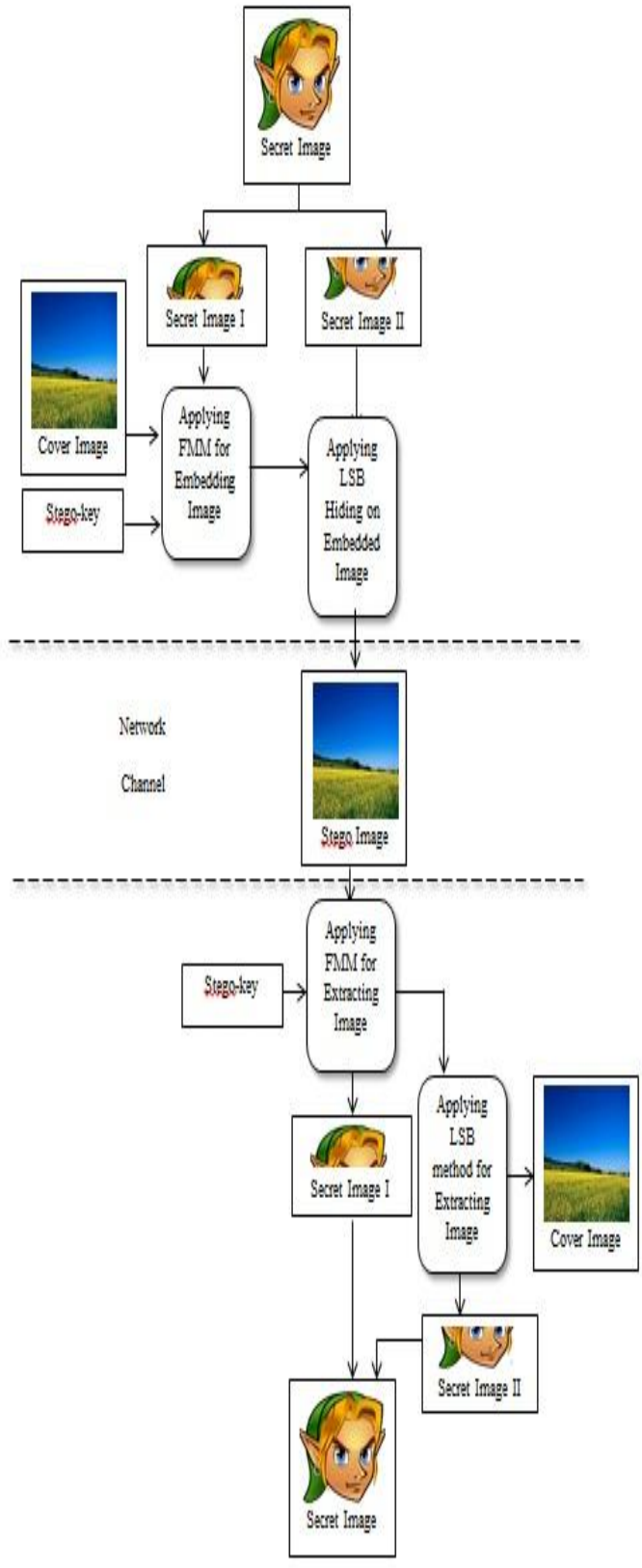

Figure 3: Flow of Execution

V. EXPERIMENT RESULT

To implement the proposed methodology the experiment has done by using MATLAB. The above mentioned algorithm with respect to image steganography are fulfill the criteria for hide any image.

For implementing the nested algorithm the experiments have tested and analyzed. As discussed previously the FMM algorithm uses the concept to store 1 pixel of secret image into a 4X4 window of cover image which is size of 16 pixels, means to save 1 pixel we need 16 pixels, so that the maximum payload is always 25% of cover image. But when combining the LSB with FMM in same secret image the maximum payload can increases.

To demonstrate this methodology, four jpeg images (Nature1.jpg, Nature2.jpg, and Nature3.jpg, and Nature4.jpg) are used as cover image. Alternatively four jpeg images (Secret1.jpg, Secret2.jpg, and Secret3.jpg, and Secret3.jpg) are used as secret image, which have combined with the previous cover image to make stego image, respectively in Figure: 1.

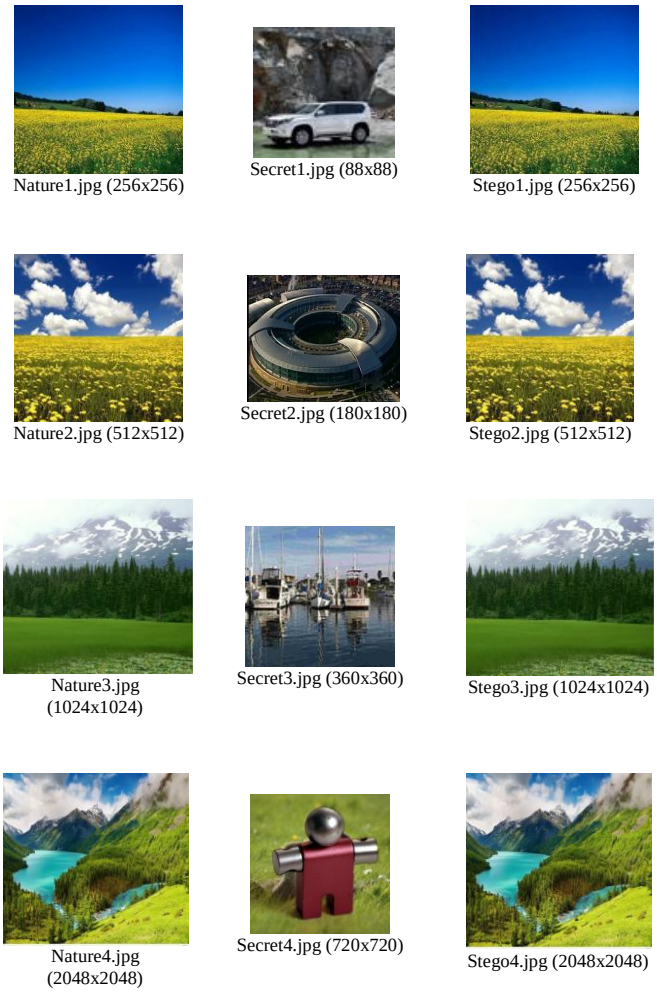

Figure 4: Implemented Cover Images (Left), Secret Images (Middle) and Stego Images (Right)

In the implemented steganographic framework the nested algorithm uses to enhance the capacity of cover image by taking care of the quality of embedded image. To measure quality of the stego images a standard metric have been established. By image coders mostly a metric used called Peak Signal Noise Ratio (PSNR).

To calculate PSNR value for an image, firstly need to calculate Mean Square Root (MSE) between the compound images. MSE could be calculated using following equation:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(P_i - Q_i)^2$$

And the Root of MSE can be measured as follows:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(P_i - Q_i)^2}$$

Where Pi denotes the pixels of original image and Qi defines the pixels of compound images.

Mathematically the equation can defined as the differences in the values of pixels between the original and reconstructed images [FMM for image comparison]. Hence, the PSNR could be calculated as:

$$PSNR = 20\,Log_{10}\frac{\max|P_i|}{RMSE}$$

To analyze the implemented method, table 1 shows the values of all images (cover image and respective secret image) that contain image size and resultant PSNR and MSE values after performing embedding operations.

TABLE II. RESULTANT VALUES OF PSNR AND MSE OF IMPLEMENTED APPLICATION

Original image (Size)	Secret image (Size)		Stego Image	PSNR	MSE
	Presently used size	*Previously used size*			
Nature1.jpg (256x256)	Secret1.jpg (88x88)	64x64	Stego1.jpg (256x256)	**66.45**	**0.0148**
Nature2.jpg (512x512)	Secret2.jpg (180x180)	128x128	Stego2.jpg (512x512)	**75.23**	**0.0019**
Nature3.jpg (1024x1024)	Secret3.jpg (360x360)	256x256	Stego3.jpg (1024x1024)	**75.49**	**0.0018**
Nature4.jpg (2048x2048)	Secret4.jpg (720x720)	512x512	Stego4.jpg (2048x2048)	**70.29**	**0.0061**

Table 1, shows the comparative results between the original images, implemented size of secret image and previous used size of secret image by evaluating PSNR. The PSNR proves the dissimilarities between original and stego image are very less because the resultant PSNR are having higher values and the quality of images are also good proven by the MSE value, which almost leads to zero. As shown by experimented result with the PSNR & MSE values the payload of secret image is also enhanced and having lesser dissimilarities proven by higher PSNR values. So using of LSB with FMM increases the hiding capacity of cover image as well as quality of stego image.

VI. CONCLUSION

In this paper, nesting of two methodologies has been proposed. One of them is Five Modulus Method and another one is Least Significant Bit. The FMM approaches to reduce the original pixel range from 0…255 into 0...51 distinct values, by dividing the value of any pixel from 5. The LSB method uses the least significant bit of 4 pixel of cover image to hide 1 pixel of secret image. A stego-key is also use to provide more security. The constructed image or stego image has no noticeable dissimilarities, which has proved by calculating the high PSNR value. The MSE is also measured to proven quality of image is good by analyzing the resultant value which almost tends to zero. The maximum payload is increases from 25% to 33% size of cover image. In the embedding process the secret image size is always acceptable if the row and column size is having remainder value 0 when divided by 2 because the secret image needs to partition into two equal parts. The purpose of using both the FMM algorithm and LSB method is to enhance the capacity of original image and security of the secret image.

REFERENCES

[1] S. Sivasubramanian and J. Raju, "Advanced Embedding of Information by Secure Key exchange via trusted third party using Steganography," International Journal of Latest Research in Science and Technology, vol. 2, issue 1, pp. 536-540, Jan – Feb 2013.

[2] R. Doshi, P. Jain and L. Gupta, "Steganography and Its Applications in Security," International Journal of Modern Engineering Research (IJMER), Vol. 2, issue 6, pp. 4634-4638, ISSN: 2249-6645, Dec 2012.

[3] F. A. Jassim, "Hiding Image in Image by Five Modulus Method for Image Steganography," Journal of computing, Vol. 5, issue 2, 2151-9617, April 2013.

[4] Z. H.AL – Hadad and I. F. Abdullah, "Image Steganography," European Academic Research, Vol. 2, Issue 6, September 2014.

[5] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proceedings 2001 International Conference on Image, Vol. 3, pp. 1019-1022.

[6] M. Nosrati, R. Karimi and M. Hariri, "Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique," World Applied Programming, Vol 1, pp. 264-268, ISSN: 2222-2510, October 2011.

[7] H. Al-Bahadili, "A Secure Block Permutation Image Steganography Algorithm," International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, September 2013.

[8] V. K. Sharma and V. Shrivastava, "A steganography algorithm for hiding image in image by improved LSB substitution by minimizes detection," Journal of Theoretical and Applied Information Technology, Vol. 36, ISSN: 1992-8645, Feb. 2012.

[9] A. Sharma, A. Agarwal and V. Kumar, "A simple technique for steganography," arXiv: 1307.8385v1 [cs.MM] 31 Jul 2013.

[10] El-Sayed M. El-Alfy and Azzat A. Al-Sadi, "Pixel-Value Differencing Steganography: Attacks and Improvements," The Second International Conference on Communications and Information Technology (ICCIT), Feb 2012.

[11] J. Nath and A. Nath, "Advanced Steganography Algorithm using Encrypted secret message," International Journal of Advanced Computer Science and Applications, IJACSA, Vol. 2, No.3, March 2011.

[12] A. Danti and P. Acharya, "Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography," IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition RTIPPR, 2010.

[13] M. Jokay and T. Moravcik, "Image-Based Jpeg Steganography," Tatra Mt. Math. Publ. 45, 65–74. DOI: 10.2478/v10127-010-0006-9, 2010.

[14] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," Security & Privacy, IEEE, Vol. 1, Issue 3, pp. 32 – 44, ISSN: 1540-7993, June 2003.

[15] B. Dunbar, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment," SANS Institute 2002.

[16] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE Computer, Vol. 31, Issue 2, p. 26-34, ISSN: 0018-9162, Feb. 1998.