INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Designing and Performance of Advanced Steganography System Using RGB Image

Shefali Narang[1], Ashish Shrivastava[2]

[1]M.Tech Scholar (CSE) PIET, Samalkha
narangshefali.5@gmail.com,
[2] Assistant Prof. CSE Deptt. PIET, Samalkha
ashish.cse@piet.co.in

Abstract- *Detection of hidden data in cover images by means of steganography is termed as Image steganalysis. A main definition of steganography includes all endeavors to communicate in such a way that the existence of the message cannot be detected. The medium used to carry the message is called the cover. Stego media should look natural, but carries secret messages innocuously. Thus, stego media should be indistinguishable from the plain cover media having no secret message. As a result, one of the most important aspects is undetectability which is strongly related to the security to construct secure steganographic systems. In order to improve security and processing speed, more and more new image steganographic algorithms become content-adaptive. In this research work, a novel method for hiding of text message behind a color image using RGB layer method is proposed. In this method each character or number from text is first converted into 8 bit binary format and than each bit of the text has been hided in color layer of cover image. Also, randomly header has been included in the beginning of the text using encryption key. This header not only increase the security of the text but also adds robustness to the proposed algorithm. MATLAB R2013a is used as an implementation platform. Image processing toolbox and general MATLAB toolbox has been used for implementation.*

Keywords: *Stegnography, Steganalysis, algorithms, Image, text message.*

1. INTRODUCTION

Steganography includes all endeavors to communicate in such a way that the existence of the message cannot be detected [2]. The medium used to bring the message is called the cover. Stego media should look natural, but carries secret messages inoffensively. So, the stego media should be interchangeable from the plain cover media having no secret message. As a result, one of the most important aspects is undetectability which is strongly related to the security to construct secure steganographic systems.

Companies, institutions and military often have a necessity to communicate a highly sensitive message and always carry the risk of capture text by unauthorized parties. Utilization of text message hiding in the picture using stegabography appears to be an alternative of predicting the limited text and capacity during embedding and extraction [9].Steganography is the procedure of hiding private information within any picture or media for incidence of communication. Steganography is frequently confused with cryptography since the two are related in the way that both are used to keep confidential material. The difference between Steganography and cryptography is in the appearance in the managed output; the output of steganography operation is not speciously visible but in cryptography the output is scrambled so that it can draw attention. Steganalysis is processed to detect of the presence of steganography [12].

2. STEGANOGRAPHY

The word steganography came from the Greek *Steganos*, which mean covered or secret and *–graphy* means writing. Therefore, steganography means covered writing. It is the method of hiding information such that its presence cannot be detected [4] and a communication is happening. The secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing methods, steganography can be used to carry out hidden exchanges. The main aim of steganography is to communicate securely in a completely undetectable manner [6] and to avoid drawing suspicion to the transmission of a covered data [7]. It is not to keep others from knowing the hidden information, but it is to maintain others from view that the information even exists. If a steganography method causes to suspect someone about the carrier medium, then the method has failed [8].

Basically, the model for the steganography is shown in Figure 1 [1]. Message is the data that the sender wishes to remain it top secret. It can be text, 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 the *stego-key*, which make sure that only recipient who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *stego-object.*

3. TYPES OF STEGANOGRAPHY

3.1 Text Steganography

It consists of trouncing information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

following: i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method [11-12].

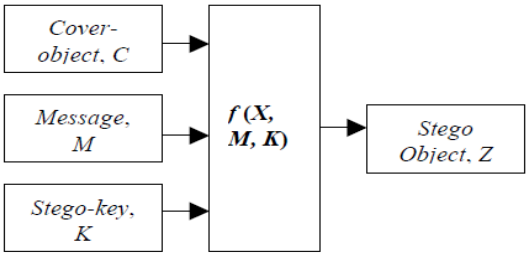

Figure1: Basic Steganography Model

3.2. Image Steganography

Hiding the data by taking the cover object as image is called as image steganography. In image steganography pixel intensities are used to cover the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

3.3. Audio Steganography

It includes hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are various different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

3.4. Video Steganography

It is a technique of hiding any types of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to cover the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

3.5. Network or Protocol Steganography

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used. The following fig 2 shows the types of steganography.

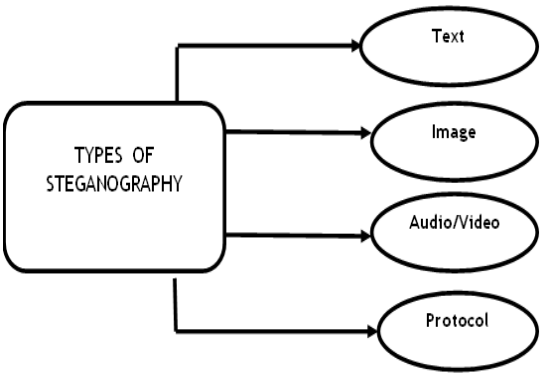

Figure 2: Stegnography types [13]

4. STEGANOGRAPHY TERMINOLOGY

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it. The stegnography block diagram is given below in the fig.3.

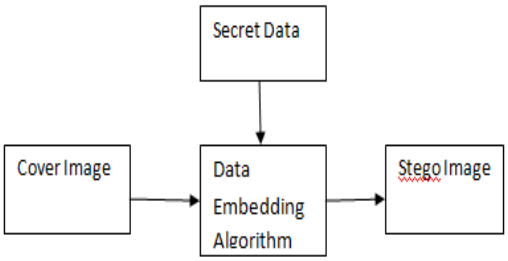

Figure 3: Stegnography block diagram.

5. VARIOUS STEGNOGRAPHIC TECHNIQUES

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed [3].

a) Least significant bit substitution technique (LSB):

In LSB steganography, the least significant bits of the cover media's digital data are used to cover up the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be covered. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value [3].

Algorithm to embed text message:-

Step 1: Read cover image and text message which is to be covered in the cover image.
Step 2: Convert text message in to binary.
Step 3: Calculate LSB of each pixels of the cover image.
Step 4: Replace LSB of the cover image with each bit of secret message one by one.
Step 5: Write the stego image.
Step 6: Calculate Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego mage.

Algorithm to retrieve text message:-

Step 1: Read stego image.
Step 2: Calculate LSB of each pixels of the stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

Advantages of LSB

1. Less mistrustful to human eyes.
2. Simple to implement and many techniques uses this method.
3. High perceptual intelligibility [10].

Disadvantages of LSB

1. Three weaknesses- Robustness, Tamper and Resistance.
2. Extremely sensitive to any types of filtering.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

3. Scaling, Rotation, Cropping, adding extra noise lead to destroy the secret message [10].

b) Discrete Cosine Transform Technique (DCT)

DCT technique is used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components [3].

Algorithm to embed text message:-

Step 1: Read the cover image.
Step 2: Read secret message and convert it into binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from the left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

c) Discrete Wavelet Transform Technique (DWT)

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one [3].

Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2DHaar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is Added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image. Extract the message bit by bit and recomposing the cover image.
Step 3: Convert the data into message vector. Compare it with original message.

6. APPLICATIONS OF STEGANOGRAPHY

There are various applications in steganography; it varies among the user requirements such as copyright control, covert communication, smart ID's, printers etc [10][12].

Copyright Control:

Inside an image, secret copyright information is embedded. This is achieved by Water-marking which is the complex structure, So that the intruder cannot identify the copyright information. There are various methods available to find the watermarking. It is achieved by statistical, correlation, similarity check. Watermarking is used to protect the copyright information.

Covert Communication:

In general concealed channel passes information by non-standard methods. Communication is obscured that is unnoticed. The aim of the covert communication is to hide the fact that the communication is being occurred. Covert communication ensures privacy. Steganography is one of the best techniques of covert communication [12]

Smart Id's:

In smart ID's the information about the person is implanted into their image for confidential information. For an organization, the authentication of the resources is accessed by the people. So identifying the theft related to prevention of crimes.

Printers:

Steganography make use of the modern printers like HP printer etc. In those printers, very small yellow dots are inserted into all pages. Information is hidden inside the yellow dots like serial number, date and time stamp. Property is available in laser printer for watermarking the confidential information [12].

Digital Watermark:

A digital watermark is a type of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.

Use by terrorists:

Steganography on a large scale used by the terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It come in concern that terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper.

Feature Tagging:

The Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Secret Communications:
In many of the situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive I formation can be transmitted without alerting potential attackers or eavesdroppers.

7. EXPERIMENTAL RESULTS

In this research work, a novel method for hiding of text message behind a color image using RGB layer method is proposed. In this method each character or number from text is first converted into 8 bit binary format and than each bit of the text has been covered in color layer of cover image. Also, a random header has been included in the beginning of the text using encryption key. This header not only enhance the security of the text but also adds robustness to the proposed algorithm**.** MATLAB R2013a has been used as an implementation platform. Image processing toolbox and generalized MATLAB toolbox has been used for implementation. Text file '2.txt' having 502 characters is used as text file to be embedded for experimental purpose. Figure 4 is the snapshot of input text file to be embedded. It is easily seen from snapshot that all the special character along with upper and lower characters has been used for embedding purpose. Figure 5 is the snapshot of histogram for all 3 layers i.e. R, G and B of input image. Figure 6 is the snapshot of MATLAB command window showing time for embedding of text message. Figure 7 is the snapshot of bar chart comparing time for embedding the text. Six methods i.e. Canny, Sobel, Prewitt, Robert, Log [9] and proposed method has been compared for embedding time in this chart. Figure 8 is the snapshots of cover image and embed image (image having text). It is quite visible from analysis of both images that there is almost no difference in both the images i.e. cover image and embed image (image having text). This similarity is the proof of efficiency and security of proposed method. Figure 9 is the snapshot of histogram for all 3 layers i.e. R, G and B of embedded image. Figure 10 is the snapshot of MATLAB command window showing time for extraction of text message. Figure 11 is the snapshot of bar chart comparing time for extracting the text. Six methods i.e. Canny, Sobel, Prewitt, Robert, Log [9] and proposed method has been compared for extraction time in this chart. Figure 12 is the snapshot of extracted text file 'secfn.txt'. It is easily seen from snapshot that all the special character along with upper and lower characters has been properly extracted. Embedding and extraction time has been taken as output performance parameter for evaluation of performance of proposed method.

The time is calculated for a text file having 500 characters for all the methods [9]. Table 1 shows the comparison of embedding and extraction time for existing methods with proposed method. Time taken for embedding and extraction is much lesser as compared to existing methods for same amount of text. This is the proof of efficient working of proposed methodology.

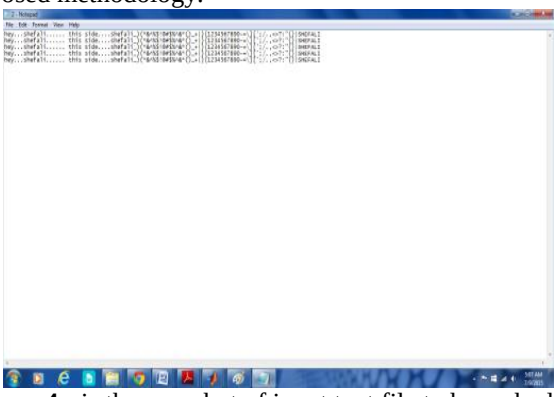

Figure 4: is the snapshot of input text file to be embedded

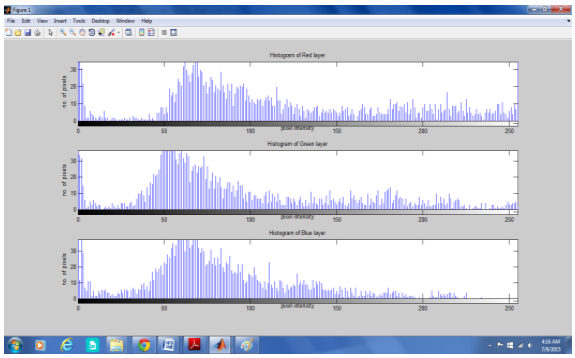

Figure 5: is the snapshot of histogram for all 3 layers i.e. R, G and B of input image

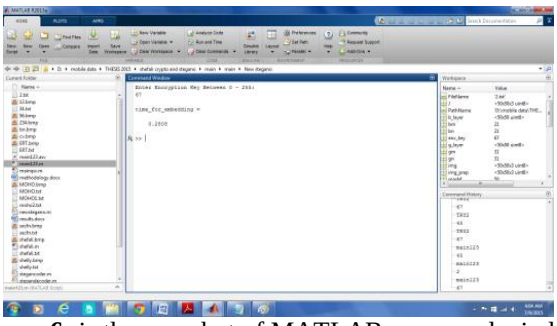

Figure 6: is the snapshot of MATLAB command window showing time for embedding of text message

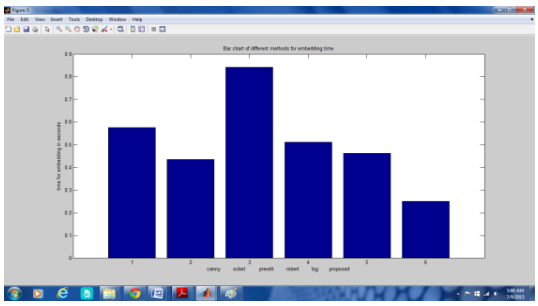

Figure 7: is the snapshot of bar chart comparing time for embedding the text

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Figure 8: is the snapshots of cover image and embed image

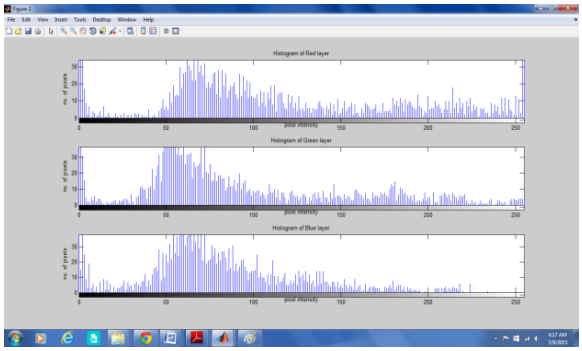

Figure 9: is the snapshot of histogram for all 3 layers i.e. R, G and B of embedded image

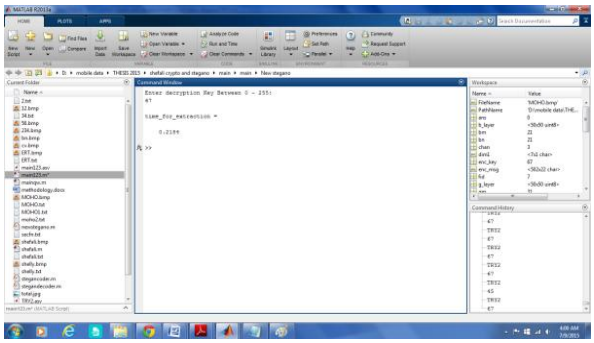

Figure 10: is the snapshot of MATLAB command window showing time for extraction of text message

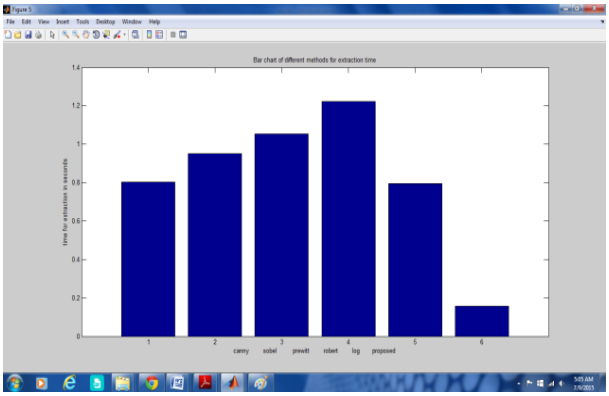

Figure 11: is the snapshot of bar chart comparing time for extracting the text

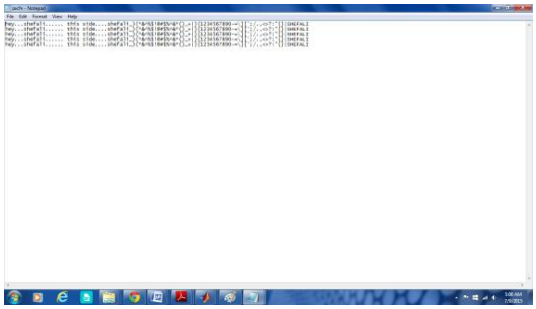

Figure 12: is the snapshot of extracted text file 'secfn.txt'

Table 1 comparison of embedding and extraction time for existing methods with proposed method

S. No.	Method for steganography	Time for embedding in seconds	Time for extraction in seconds
1	Canny	0.5751	0.8038
2	Sobel	0.4349	0.9511
3	Prewitt	0.8428	1.0546
4	Robert	0.5103	1.2230
5	Log	0.4615	0.7945
6	Proposed method	0.2808	0.2184

8. CONCLUSION AND FUTURE SCOPE

The increasing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more & more important as the number of data being exchanged on the Internet increases. Steganography and steganalysis are the important topics in information hiding In this research work, a novel method for hiding of text message behind the color image using RGB layer method is proposed. In this method each character or number from text is first converted into 8 bit binary format and than each bit of the text has been hided in color layer of cover image. Also, a random header has been included in the beginning of the text using encryption key. This header not only increase the security of the text but also adds robustness to the proposed algorithm. MATLAB R2013a has been used as an implementation platform. Image processing toolbox and generalized MATLAB toolbox has been used for implementation.This approach leads to very high capacity with low visual distortions. Experimental results demonstrate that our algorithm performs better than other similar algorithms. Figure 5 is the snapshots of cover image and embed image (image having text). It is quite visible from analysis of both images that there is almost no difference in both images i.e. cover image and embed image (image having text). This similarity is the proof of efficiency and security of proposed method. Table 1 shows the comparison of embedding and extraction time for existing methods with proposed method.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Time taken for embedding and extraction is much lesser as compared to existing methods for same amount of text. This is the proof of efficient working of proposed methodology. The steganalysis performance with different classifiers such as Fisher's linear classifier and logistic regression shall be part of future work.

References

[1] Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Ying Zeng "Pixel Group Trace Model-based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography" IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013. Pp. 216-228.

[2] Rongyue Zhang, Vasiliy Sachnev, Magnus Bakke Botnan, Hyoung Joong Kim and Jun Heo "An Efficient Embedder for BCH Coding for Steganography" IEEE Transactions on Information Theory, Vol. 58, No. 12, December 2012. Pp. 7272-7279.

[3] Stuti Goel, Arun Rana & Manpreet Kaur. "A Review of Comparison Techniques of Image Steganography". Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013.

[4] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie "A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm" IEEE Transactions on Multimedia, Vol. 12, No. 5, August 2010. Pp. 345-357.

[5] Graeme Bell and Yeuan-Kuen Lee "A Method for Automatic Identification of Signatures of Steganography Software" IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, June 2010. Pp. 354-359.

[6] Jun Zhang and Dan Zhang "Detection of LSB Matching Steganography in Decompressed Images" IEEE Signal Processing Letters, Vol. 17, No. 2, February 2010. Pp. 141-144.

[7] Weiming Zhang and Xin Wang "Generalization of the ZZW Embedding Construction for Steganography" IEEE Transactions on Information Forensics and Security, Vol. 4, No. 3, September 2009. Pp. 564-569.

[8] Zhiyuan Zhang, Ce Zhu, and Yao Zhao "Two-Description Image Coding With Steganography" IEEE Signal Processing Letters, Vol. 15, 2008. Pp. 887-890.

[9] Anwar H. Ibrahim, Waleed M. Ibrahim "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time" International Journal of Information Technology & Computer Science (IJITCS) (ISSN No : 2091-1610) Volume 7 : No : 3 : Issue on January / February, 2013.pp. 73-78.

[10] R. Poornima and R.J.Iswarya "An Overview of Digital Image Steganography" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.pp 23-31.

[11] Jasleen Kour and Deepankar Verma "Steganography Techniques –A Review Paper" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) May 2014. Pp.132-135.

[12] Rashi Singh and Gaurav Chawla "A Review on Image Steganography". International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 5, May 2014 ISSN: 2277 128X.pp 686-689.

[13] Gunjan CHUGH Image Stegnography Techniques: A Review Article ACTA TECHNICA CORVINIESIS-Bulletin of engineering Tome VI July-September 2013.ISSN 2067-3809.pp 97-104.