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

# Designing and Performance Evaluation of Advanced Steganography System

**Deepak Garg[1], Gourav Sharma[2]**
M. Tech Student[1], Associate Prof.[2],
M.M U. Mullana, Ambala, Haryana, India
deepakgarg2804@gmail.com, gorutyagi11@gmail.com

***Abstract:*** *Image steganalysis is the process of detecting the hidden data in cover images by means of steganography. A main definition of steganography includes all pathways to communicate in such a way that the existence of the message cannot be detected. The medium used to hold the message is called the cover. Stego media should look like to be 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 new 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, Cryptography, algorithms, Image, text message.*

## 1. INTRODUCTION

The term steganography is retrieved from the Greek words *stegos* means *cover* and *grafia* meaning *writing* defining it as *covered writing [1.] [7.]*. Similarity between steganography and cryptography is that, both are used to conceal information. But the difference is that the steganography does not reveal any suspicious about the hidden information to the user. Therefore the attackers will not try to decrypt information. There are other two techniques that seem to be same as Steganography. They are Watermarking and Fingerprinting. Both these techniques sounds to be same and provide same end goals but both are very different in the way they working. Watermarking allows a person to provide hidden copyright notices or other verification licenses. Whereas, Fingerprinting uses each copy of the content and make it as unique to the receiver. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level [1]. Using this method we hide information such that its presence is not detected [1.]. The secret message is encoding in a way such that the very survival 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 [2.] and to avoid drawing suspicion to the transmission of a covered data [3.]. 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 [4].

## 2. ERA OF STEGANOGRAPHY

1. During the cold war two the Microdot technology developed by Germans which prints the clear good quality photographs shrinking to the size of a dot [7.].

2. In Greece they select a person to send message by shaving their heads off. They write a secret message on their head and allow growing up their hair. Then the intended receiver will again shave off the hair and see the secret message.

3. During the world war two the secret message was written in invisible Ink so that the paper appears to be blank to the human eyes. The secret message is extracted back by heating the liquids such as milk, vinegar and fruit juices.

## 3. EMBEDDING PROCESS OF STEGANOGRAPHY

The main aim of steganography is to hide information in to the carrier file [7.]. The file that contains the embedded information inside of it, called as stego file. The information hiding may be text file, video, audio, image etc.

## 4. TYPES OF STEGANOGRAPHY

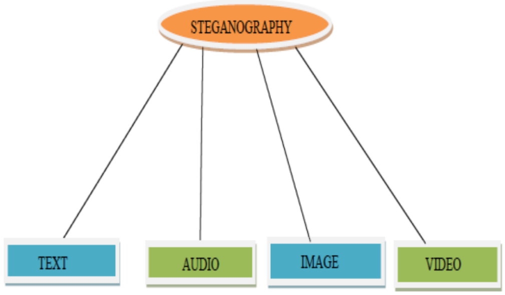


**Fig 1**: Types of Steganography

1. ***Text-based Steganography*** - In which the message to be sent is embedded in a text file by formatting it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the

embedded content hence the technique is not robust [8.].

2. ***Audio Steganography*** - Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding [5.] [6.].
3. ***Image Steganography*** - Hides message in the images. This technique is the most popular because of the fact that almost no perceivable changes occur. In images after hiding a large amount of data with wide variety of available images. Depending on the data hidden in the pixels directly or in the coefficients obtained after a suitable transform domain like FFT, DFT or DWT leads to spatial domain Steganography and frequency domain Steganography. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges [5.].
4. ***Video Steganography*** - Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video format [6.].

## 5. FACTORS AFFECTING A STEGANOGRAPHIC METHOD

The effectiveness of any steganographic method can be determined by comparing stego-image with the cover Image [5.]. There are some factors that determine the efficiency of a technique. These factors are:

*1) Robustness:* It is the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

*2) Imperceptibility:* This means invisibility of a steganographic algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

*3) Payload Capacity*: It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.

*4) PSNR (Peak Signal to Noise Ratio):* This is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image [5.].

*5) MSE (Mean Square Error):* It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient will be the image steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

*6) SNR (Signal to Noise Ratio):* It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise.

## 6. PROPOSED METHODOLOGY

The growing possibilities of modern communications need the special means of security especially on computer network. Steganography hides the secret message within the host data set and presence imperceptible. From the above literature survey, it can be concluded that there are many challenges regarding in designing a steganalytic system like processing time, complexity and security. Various kinds so security model can be designed in accordance with type of data to be encrypted. Also, one of the major issues to be considered is the computational speed of the steganographic model. Existing techniques are not as susceptible to cropping, compression, etc. But, they also increase the total cost of the system because computational time of the algorithms have a major impact on the determining the cost effectiveness and efficiency of the system. So, authors need a better technique which must provide high level security, cost effective, lesser computational time, higher computational speed and high efficiency. Also, the text which will be ciphered by this method must not be broken. By implementing the proposed method, this entire problem can be handled easily, by hiding characters information into various layers i.e. red, green and blue of colored image.

### 6.1 ENCRYPTION AND HIDING OF TEXT MESSAGE WITHIN A CANVAS IMAGE

Allow user to select of canvas image and text message file & to select a proper encryption key.

### 6.1.1 SEQUENTIAL ENCODING

Conversion of text message into ASCII integer values including space & applying Header to Beginning of Message to be encoded. Then determine Message Image's Size for Encoding in Header. After that Encrypting of message is done using XOR Key. Integer values are converted into binary & Hide the data points using a RGBBGRRG Order behind RGB colored image. Hiding this data along the columns is done by moving from left to right through the target image. Write Canvas Image to .BMP File. BMP, or bitmap format, is chosen because it does not use compression. JPEG compression destroys the message.

### 6.2 DECRYPTION AND EXTRACTION OF TEXT MESSAGE FROM MESSAGE EMABDDED IMAGE

Import "Canvas Image" With Hidden Message & Prompt User for Encryption Key to decrypt the message.

### 6.2.1 SEQUENTIAL DECODING

Find and remove the header by taking modulus of message embedded image with 2, so as to get digital bits. Next step is used to determine whether or not authors have reached the end of the image to extract the message. Authors then need to move to the next column and reset our pattern to the top row. Decrypt and determine message by converting binary data into integer values. Conversion of integer values into respective characters. Writing of text and save text into user defined .txt file MATLAB R2013a has been used as an implementation platform. Image processing toolbox and generalized MATLAB toolbox has been used for implementation. Text file 'deepak.txt' having 502 characters is used as text file to be embedded for experimental purpose. Some images with '.jpg' extension have been taken as cover images. Steps for proposed methodology are as follows:

### 6.3 ENCODING AND HDING OF TEXT MESSAGE

1. Inputting of the cover image.
2. Conversion of image into matrix.
3. Assignment of each layer matrix i.e. Red, green and blue to three different Variables.
4. Calculation and display of histogram of all three layers.
5. Inputting and reading of text file data.
6. Prompt User for Encryption Key and inputting of encryption key.
7. Note down the starting time for encryption.
8. Determining Message Type. If message is text this will be true; False otherwise.
9. Conversion of text into ASCII Integer Values.
10. Calculation of length of message or number of characters in text message.
11. Preparation of a header to be included in the text message.
12. Applying Header to Beginning of Message to be encoded.
13. Determine Message Image's Size for Encoding in Header.
14. Padding of zeros in the header if rows of text are less than 4.
15. Padding of zeros in the header if columns of text are less than 4.
16. Applying Header to Beginning of Message to be encoded.
17. Mixing of text included text and encryption key.
18. Preparation of cover image for hiding of encrypted text.
19. Hide the data points using a RGBBGRRG Order.
20. Hiding this data along the columns moving from left to right through the target cover image using logical AND and OR operations.
21. Initializing the Counters for above operation i.e. Rm, gm and bm.
22. Calculation of the size of encoded message and assigning into a Variable. This variable indicates the number of message characters that need to be encoded in the cover image.
23. This next step is used to determine whether or not we have reached the end of the image. We then need to move to the next column and reset our pattern to the top row. Since we have no idea when we will reach this point we have to check this EVERY time after we increase the rm/gm/bm counter.

### 6.4 EXTRACTION AND DECCODING OF TEXT

24. Inputting and reading of encrypted image.
25. Assignment of each layer matrix i.e. Red, green and blue to three different variables.
26. Calculation and display of histogram of all three layers.
27. Prompt user for encryption key and inputting of key for decryption.
28. Recovery of header set from encrypted image, first.
29. Initializing the counters for recovery operation i.e.Rm, gm and bm.
30. Note down the starting time for decryption.
31. This next step is used to determine whether or not we have reached the end of the image. We then need to move to the next columns and reset our pattern to the top row. Since we have no idea when we will reach this point we have to check this every time after we increase the rm/gm/bm counter.
32. Analysis of header and extraction of encrypted data.

- Case 1: if the header starts with character't', it is a text file.
- Case 2: if the header doesn't start with't', then the message is an image with the dimensions described in the header.

33. Extraction of potential message from encrypted message using RGBBGRRG order using
34. Modulo arithmetic.
35. This next step is used to determine whether or not we have reached the end of the image. We then need to move to the next column and reset our pattern to the top row. Since we have no idea when we will reach this point we have to check this every time after we increase the rm/gm/bm counter.
36. Note down end time for decoding and calculation of total decryption time.
37. Separation of message text from key using logical XOR operation.
38. Preparation of message to be shown as actually it was before hiding and encryption.
39. Writing decrypted message to .txt file

## 7. RESULT

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 'deepak.txt' having 502 characters is used as text file to be embedded for experimental purpose. Figure 4 is the snapshot of origional 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 extracted data from image.

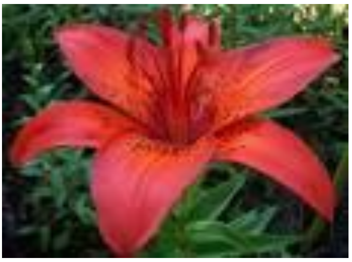


**Fig. 2**: Original image

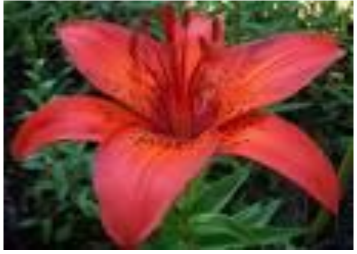
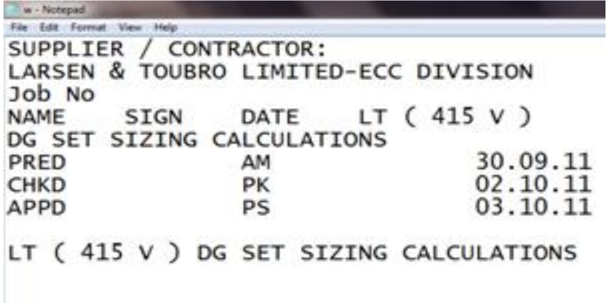


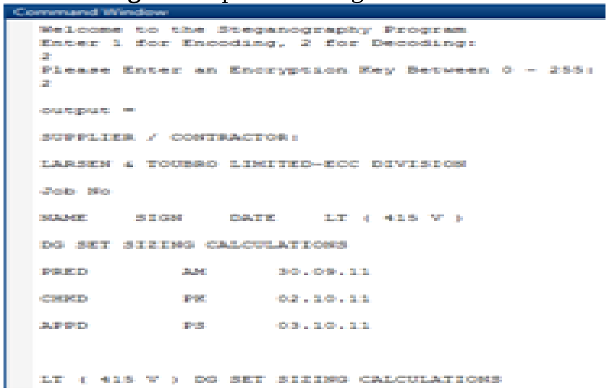
**Fig. 3:** Image with text data



```
SUPPLIER / CONTRACTOR:
LARSEN & TOUBRO LIMITED-ECC DIVISION
Job No
NAME      SIGN     DATE     LT ( 415 V )
DG SET SIZING CALCULATIONS
PRED              AM                  30.09.11
CHKD              PK                  02.10.11
APPD              PS                  03.10.11

LT ( 415 V ) DG SET SIZING CALCULATIONS
```

**Fig. 4**: Snapshot of Original text data



```
Welcome to the Steganography Program
Enter 1 for Encoding, 2 for Decoding:
2
Please Enter an Encryption Key Between 0 - 255:
2

output =

SUPPLIER / CONTRACTOR:

LARSEN & TOUBRO LIMITED-ECC DIVISION

Job No

NAME      SIGN      DATE      LT ( 415 V )

DG SET SIZING CALCULATIONS

PRED          AM        30.09.11

CHKD          PK        02.10.11

APPD          PS        03.10.11


LT ( 415 V ) DG SET SIZING CALCULATIONS
```

**Fig. 5**: Snapshot of extracted data from image

## 8. CONCLUSION

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.

## REFERENCES

**[1.] 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.**

**[2.] 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.**

**[3.] 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.**

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

**[5.] 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.**

**[6.] 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.**

**[7.] 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.**

**[8.] Vanitha, Anjalin D Souza, Rashmi , Sweeta DSouza "A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm" , International Journal of Innovative Research in Computer and Communication Engineering. Vol.2, Special Issue 5, October 2014. Pp. 89-95.**