Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Implementation of Memory Efficient Data Hiding Technique

**Anushka Nagpal**
CSE& Kurukshetra University
Haryana, India

***Abstract— Steganography is an important area of research in recent years involving a number of application. In this paper, a new Steganography technique is presented, implemented and analyzed. The proposed method hides the secret message into cover medium. It can hide three images into one. Evaluation is done on PSNR based. Comparison with existing techniques is also compared. Then the performance specification of image steganography is disscussed . Different embedding techniques that are LSB, Spatial domain ,DCT, Huffman encoding, are generalized .***

***Keywords- Steganography, Stego-image, Peak signal to noise ratio, least significant bit , discrete cosine transform.***

## I. INTRODUCTION

In the current scenario of web, user information gets highest priority within the field of information communication. This information must be sent firmly so as to keep the web usage reliable. For this security of information, numerous ways have been discovered. Some admired ways are cryptography and steganography.

### 1.1 STEGANOGRAPHY

Image steganography is the art of information hidden into cover image,. Is the process of hiding secret message within another message.The word steganography in greek means “Covered Writing”. The information hiding process in a steganography with different techniques includes identifying a cover mediums redundants bits. The embedding process creates a stego medium by replacing the redundant bits with data from the hidden message.

During the process of hiding the information three factor must be considered that are ***capacity*** it includes amount of information that can be hidden in the cover medium. ***Security*** implayes to detect hidden information and ***Robustness*** to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [1].

Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [2]. Using steganography a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. In cryptography techniques scrambles a message so it cannot be understood. Where as in steganography hides the message so it cannot be seen [3].

### 1.2 Some terminologies in Steganography:

- **Payload:** The information which is to be concealed.
- **Carrier File:** The media where payload has to be hidden.
- **Stego-Medium:** It is the medium in which the information is hidden.
- **Redundant Bits:** Pieces of information inside a file which can be overwritten or altered without damaging the file.
- **Steganalysis:** The process of detecting hidden information inside of a file.
- **Stego medium** = Payload file + Carrier file.

### 1.3 The four basic techniques used for Steganography are:

- **LSB method**: The LSB of carrier medium is directly inserted with the message bit. So LSB of the carrier medium contains the payload.
- **Injection:** Hiding data in sections of a file that are ignored by the processing application. Therefore avoid modifying those file bits that are relevant to an end perfectly usable.
- **Substitution**: Replacement of the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion.
- **Generation**: Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the sole purpose of hiding the message.

## II. RELATED STUDY

**Prof.S.V.Kamble et.al[1]** This author presented stegnography based on digital image. Various Concepts and priniciple of steganography were illustrated in paper. Different embedding techniques such as LSB,DCT, Huffman encoding [6] are generalized. Then the performance and specification of image steganography is discussed at last. In An image based steganography that combines LSB, DCT, and compression techniques on the image to enhance the security of the payload object.

**Pallavi Hemant Dixit et.al[2]** Today Network security and protection of data have been of great concern and a subject of research. There are many different forms of steganography mechanisms such as LSB, Masking and filtering and Transform techniques. All of them have their respective strong and weak points. The LSB embedding Technique suggests that data can be hidden in the least significant bits of the cover image and the human eye(HVS) would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format. This paper also explains the LSB embedding technique and Presents the evaluation for various file Formats. In a network, the success of the algorithm depends on hiding technique used to store information into the image. This paper is based on the study of steganography with its LSB algorithm. Human biometrics like iris, fingerprint, and face are the unique things for human.

**Mazhar Tayel et.al[3]**Data security has become an important problem in today’s communication systems. Steganography is used to hide existence of a secret-message. In this paper, a modified Steganography algorithm will be proposed depending on decomposition principle of both secret-message and cover-image. A fuzzification is performed in the secret message to optimize the decomposed coefficients before embedding in the coverimage to get a Stego Image. Also the well known metrics (Cor., MSE, PSNR, and Entropy) were used to evaluate the modified algorithm. Also, a trade-off factor was introduced to determine an optimum value for the embedding strength factor to get an acceptable degradation. Moreover to evaluate and assess the modified algorithm and any Steganography algorithms, a new histogram metrics are proposed which represents the relative frequency occurrence of various images.

**Saleh Saraireh[4]** This paper proposes a secure communication system. It employs cryptographic algorithm together with steganography. The combination of these techniques provides a robust and strong communication system that able to withstand against attackers. In this paper, the filter bank cipher is used to encrypt the secret text message, it provide high level of security, scalability and speed. After that, a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR) and histogram analysis.

**Mridul Kumar Mathur [5]** “A picture is worth more than thousand words “is a common saying. What a image can communicate cannot be expressed through words. Images play an indispensable role in representing vital information and needs to be saved for further use or can be transmitted over a medium. In order to have efficient utilization of disk space and transmission rate, images need to be compressed. Image compression is the technique of reducing the file size of a image without compromising with the image quality at a acceptable level. This reduction in file size saves disk/.memory space and allows faster transmission of images over a medium. In this paper we have converted an image into an array using Delphi image control tool. Image control can be used to display a graphical image - Icon (ICO), Bitmap (BMP), Metafile (WMF), GIF, JPEG, etc, then an algorithm is created in Delphi to implement Huffman coding method that removes redundant codes from the image and compresses a BMP image file (especially grayscale image) and it is successfully reconstructed. This reconstructed image is an exact representation of the original because it is lossless compression technique. This Program can also be applied on other kind of RGB images (BMP, JPEF, Gif, and tiff) but it gives some color quality loss after reconstruction .Compression ratio for grayscale image is better as compared to other standard methods.

## III. PROPOSED WORK

**ASSUMPTIONS:**

1. Cover image, payload object (secret message) are raw images of any arbitrary size.
2. The LSB’s of cover image is used to embed the payload.
3. Cover image (A)
   Hidden Image (B)
   Stego image (C)

Read first byte of A and B, Run LSB, Compute DCT, Perform Quantization. Copy the output as stego image.

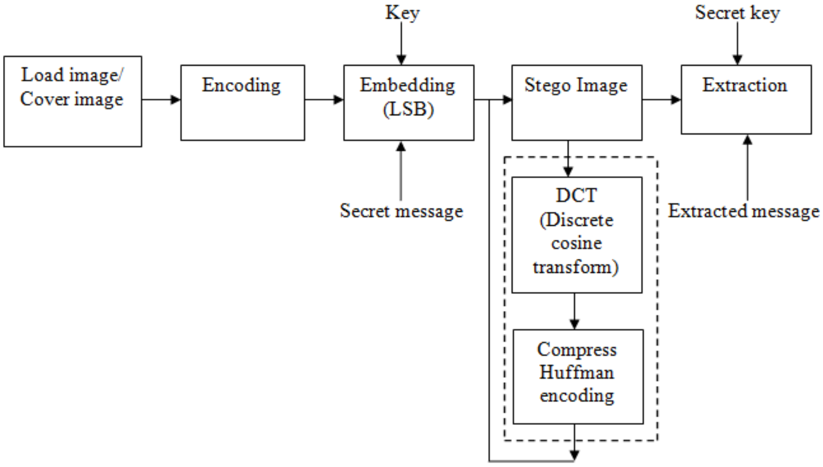


Figure 1: Proposed Architecture of steganography

**1. Load Image/Cover Image:** This cover file may be a graphics image (such as JPEG, PNG), or even a binary executable.

**2. Encoding:** the encoding is applied on the cover image.

**3 .Embedding:** Three different aspects in information-hiding systems contend with each other: *capacity, security, and robustness.* Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. We will use LSB embedding technique.

**LSB (least significant bit) embedding**: this technique the data is hidden in the least significant bit of each byte in the image. This technique is implemented in spatial domain, i.e processing is applied directly on the pixel values of the image.

In least significant bit(LSB), each pixel of an image transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image.

Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object.

**4. Stego Image:** A stego image is the original cover object with the secret information embedded inside. DCT domain embedding techniques is the most popular one, mostly because of the fact that DCT based image format are widely available in public domain as well as the common output format of digital camera.

**4.1 DCT (Discrete cosine transform):** DCT technique are implemented in frequency domain, i.e pixel values are transformed and then processing is applied on the transformed coefficients.

The discrete cosine transforms (DCT) is mathematical function that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components.

**4.2 Compress Huffman Encoding:** Huffman coding method that removes redundant codes from the image and compresses image file (especially grayscale image) and it is successfully reconstructed [5].

Huffman encoding is used to serve the following three:

*Lossless Compression* =It increases the embedding capacity .

*Security by means of encoding* =Huffman encoded bit stream cannot reveals anything. To extract the exact meaning, the Huffman table is required to decode. It provides one type of authentication, as any single bit change in the Huffman coded bit stream, Huffman table is unable to decode [6].

**5. Extraction:** The recipient must decode the stego image in order for them to view the secret information. The decoding process is simply the reverse of the encoding process. It is the extraction of secret data from a stego image. This is the reconstructed image.

## IV. RESULTS AND DISCUSSION

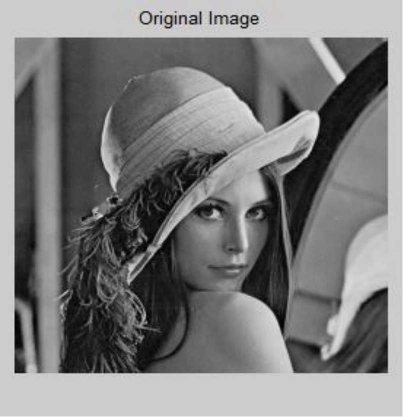


Fig 4.1: Original Image

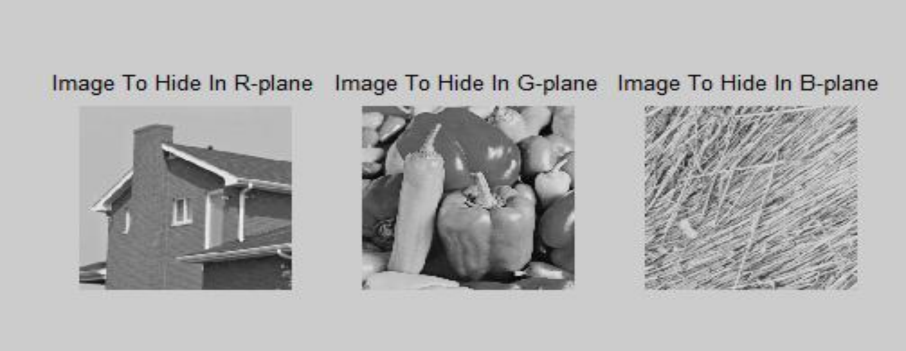


Fig4.2: Message to be hidden

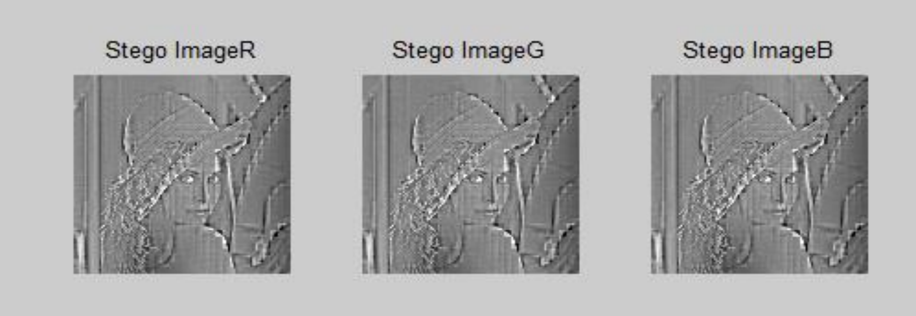


Fig4.3: Stego Image Obtained.

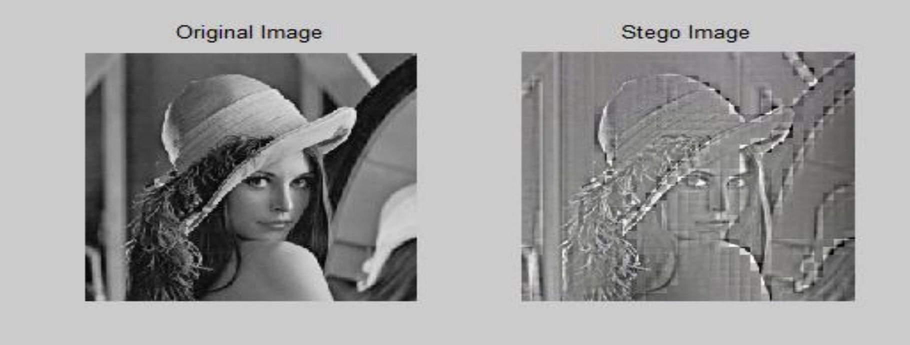
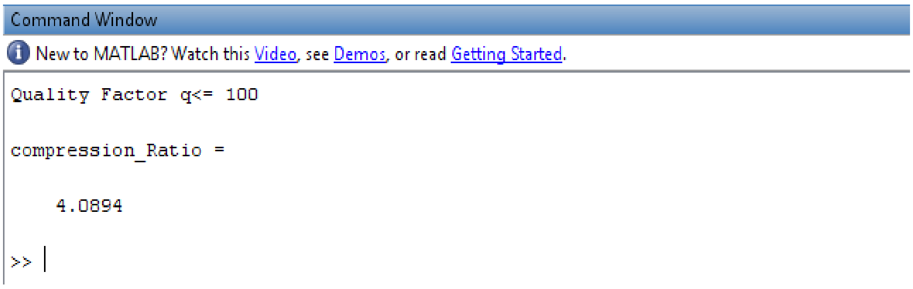


Fig 4.4: Comparison of Original image and stego image from proposed work.


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
Quality Factor q<= 100

compression_Ratio =

    4.0894

>> 
```

Fig4.5: Quality factor.

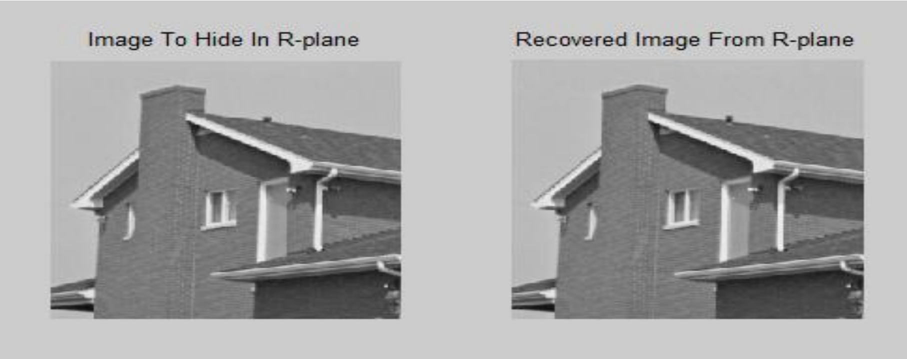


Fig4.6: Recovered image from R-plane.

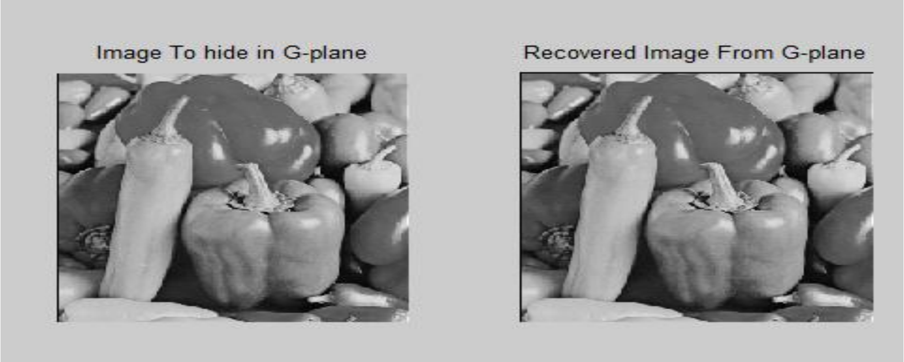


Fig4.7: Recovered image from G-plane.

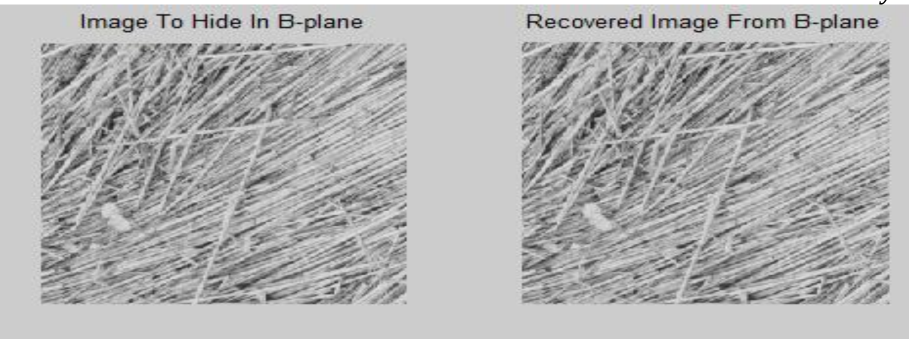


Fig 4.8: Recovered image from B-plane.

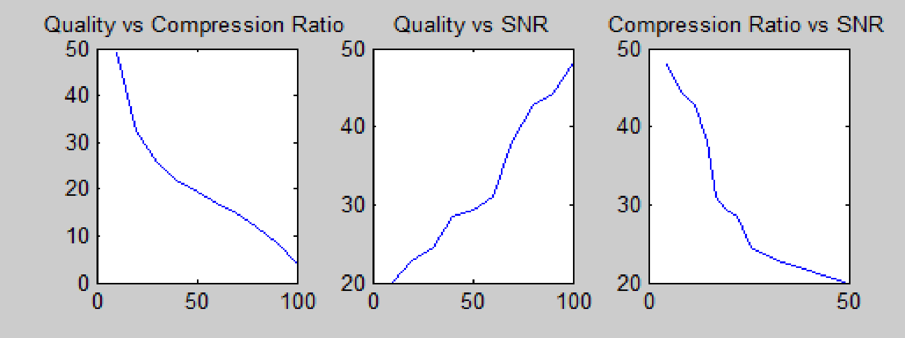
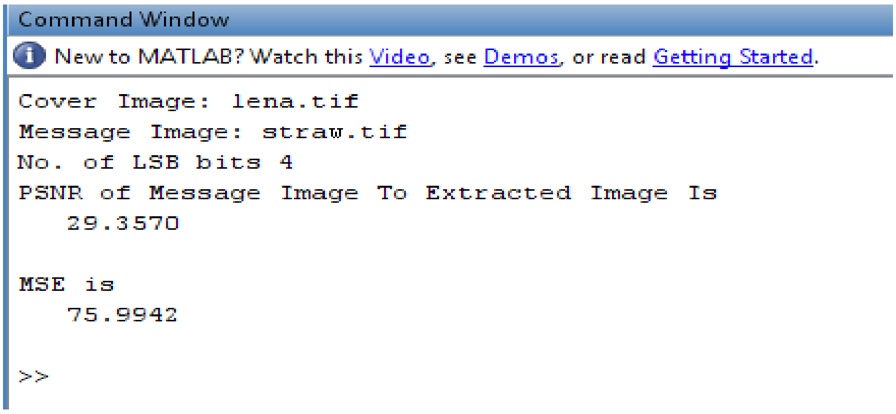


Fig 4.9: Comparison between Quality vs Compression ratio, Quality vs SNR, Compression ratio vs SNR.

Table 4.10

| Image | Quality | Compression ratio |
|---|---|---|
| **Proposed Technique** | 10 | 49.0661 |
| | 20 | 32.3103 |
| | 30 | 25.5401 |
| | 40 | 21.9306 |
| | 50 | 19.3626 |
| | 60 | 17.0371 |
| | 70 | 14.8900 |
| | 80 | 11.5822 |
| | 90 | 8.5821 |
| | 100 | 3.9782 |

## V. CONCLUSION


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
Cover Image: lena.tif
Message Image: straw.tif
No. of LSB bits 4
PSNR of Message Image To Extracted Image Is
   29.3570

MSE is
   75.9942


>>
```

Fig 5.1: PSNR of exiting technique.

In conclusion, Proposed approach gives satisfactory PSNR value to establish the robustness of the work. Since only selected high frequency components are modified for the hiding method, therefore there must be a constraint on the secret image size. PSNR of extracted image is inversely proportional to the MSE. So, without compromising the quality factor we can compress our image.

## REFERENCES

[1] Hniels Provos & Peter Honeyman,"Hide & Seek : An Introduction to Steganography" IEEE Computer Society Pub-2003. 2] Shivangi Goyal International Journal of Science and Technology Volume 1 No. 3, March, 2012 IJST

[2] Amitava Nag, Sushanta Biswas,"A Novel Techniques for image steganography based on DWT and Huffman Encoding", IJCSS, Vol(4): Issue (6)

[3] Ge Huayong ,Huang ,"Steganography and Steganalysis Based on Digital Image", International conference & signal Processing-2011 IEEE.

[4] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 –8887), Volume 9, No.7, November 2010.

[5] K B Raja, R.K.Chhotary, K.B.Shiva Kumar," Coherent Steganography using Segmentation and DCT", IEEE 2010.

[6] Mamta Sharma,□ Compression Using Huffman Coding□, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010,pp 133-141.

[7] Johnson, N.F and Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Journal, February 2008.

[8] Blossom kaur1, Amandeep kaur and Jasdeep singh,"Steganographic approach for hiding image in dct domain "International Journal of Advances in Engineering & Technology, July 2011.

[9] J.R. Krenn, "Steganography and Steganalysis",January 2004.Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs ,"Implementation of LSB Steganography and its Evaluation for Various Bits", 2004.

[10] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012