High Capacity Steganography Based on Least Significant Bit Technique

Jaydev Kumar Jha, Dr. Arvind Sahu

TIT Bhopal, India

Abstract - Communication has become a very essential aspect of today life. With the revolution of digital technologies, communication has become too rapid and also widespread. Often communication involves transmission of confidential information like bank transactions, military secrets, e-document etc., have to be guided over unauthorized access. This has led to the growth of a new arena of study called "Information Security". This deal's with transmitting confidential information from one person to another by maintain in confidentiality, integrity, authentication, and non-repudiation. In such a way that the information sent cannot be retrieved by anybody other than the sender and the intended recipient. For secured communication of information between sender and intendent receiver steganography technique is preferred, which embeds the confidential information in a cover image. Any digital media can be used as a original object. The original object may be a image, audio, video, text, etc., and it is necessary to hide and carry the confidential message. In this work digital images are to be considered for the purpose of hiding confidential information. Image steganography technique is derived from the signal- and digital image processing techniques.

I. INTRODUCTION

The fast evolution of the electronics era has led to all documentation, video and audio being digitized. This has increased the requirement for ensuring the safety and reliability of any document, video and audio to maintain privacy, and to prevent piracy and mass reproduction. This requirement varies from

individual to individual. The method used for ensuring this are cryptography and steganography of which the former is perceptible as noise while the latter is unrevealed to the human eye. Current Digital multimedia platform provide robust and easy way of editing data. This data need to be transmitted safely over computer network without interference. Steganography is a technique that hide data among the bit of a cover file like a graphics or an audio file. The word Steganography is Greek in origin which implies covered writing or hiding from plain eyesight.

1.1 Digital Right :- The evolution of Internet allowed multimedia content to become available in digital form and is a main factor in the increased use of copyright marking. Though digital information can be distributed very easily. It is too easy to misuse copyrighted material. Internet copies can very easily shared. On a point to point network, the information can be store on a server and make it harder for the authorized user to locate and accuse offenders. Steganography technique can be breakable steganography or robust steganography.

1.2 Steganographic Techniques :- Steganography technique provide a way of communication secretly as longer as an attacker doesn't find a way to detect the information. The most suitable type of files for stenographic transmission being, media files due to their bigger size. The host files masking other files are usually called carriers. The carrier files are functional files and does not raise a problem or arouse suspicion. This section lists a number of hiding method that are being used currently. Data can be embedded inside a file by taking advantage of human perception. Audio files use frequency masking on tones with analogous frequency and the casual listener does not hear the masked quieter tones.

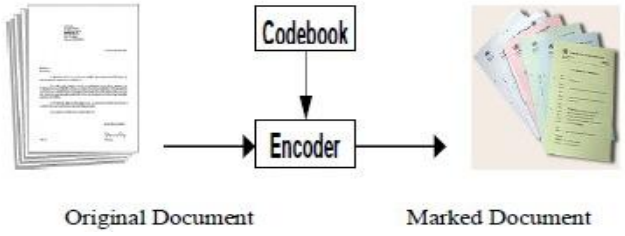

Figure 1.1 : Document embedding

1.3 Information Hiding Techniques :- Information security is the very significant asset because loss of information will lead to many problems in electronic world. The three techniques which is cryptography, steganography and watermarking form the base for secure communications.

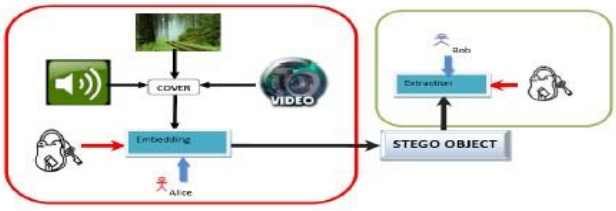

Figure 1.3 General schematic description of steganography with different types of covers

Cryptography is a method in which the secret information is encrypted and sent in an unintelligible format. It scrambles the confidential information in such a way that it appears to be garbage to any unauthorized user. The secret information which is to be communicated is a combination of permutations and substitutions and hence illegitimate users could not access the information.

II. LITERAURE REVIEW

Divya et al. [1], proposed an algorithm in the area of steganography for JPEG image altering the block DCT coefficient. In this technique the DCT coefficient are divided into four frequency band by matrix encoding. A new technique for selecting the coefficient is used to make the concealed message less perceivable. The aim of steganography technique is to perceive the hidden information. This technique exploits the several image processing techniques such as cropping, filtering etc. Passive steganography method simply corrupt the image if any suspicion arises. Active steganography attempt to find the algorithm to hide the information and tried to retrieve that information.

Ammad U Islam et al. [2], proposed a new technique for image security combining three cryptography stenography and watermarking techniques. It not only hides the information but also provide better results for MSE, PSNR and embedding power even after the noise attacks. It also provided security for watermarked video. The algorithms are compared with the existing algorithm based on Error mapping syndrome embedding and with other algorithm based on Matrix Embedding and Pre- flipping Matrix Embedding.

Saikat Mondal et al. [3], presented a steganography method for secret sharing of data using gray scale images. The relation between the binary and gray code representation of a pixel is mainly taken into consideration here. And an EX-OR gate operation is used upon N cover image accessible to sender and receiver. Then, for the purpose of improving the image Steganography robustness against attacks of an image transmission, we encrypted the compressed message with RS-code which resulting into secret data stream.

Z. Khan et al. [4], proposed two technique for color image steganography. They proceeded with a hashing approach for secure information. Here secured images are transmitted at higher rate using gray scale images with this approach. Also various file formats such as bmp, JPEG, gif are supported in this technique of secured transmission.

Tulasidasu et al. [5], put forward an technique for concealing message in encrypted images by using a predetermined watermark embedding before the process of encryption. Here the encryption/decryption both has a unique key and watermark processing has a different key thus decryption of message transmitted is independent of extracting the image.

Sasirekha et al. [6], proposed an approach for data hiding by reversible image transformation. Here RTI based framework is used to hide the content of main image into another target image having same size. Traditional RDH scheme and unified embedding and scrambling method are used to insert watermark in the encrypted images.

L. Ramya et al. [7], proposed a method for data concealing using pixel value differencing and LSB substitution. Here image file is split into blocks of two successive pixels. The difference between two pixels is calculated, and as per the difference, it approximate the number of embedding bits into LSBs of two pixels.

Anupam K. et al. [8], presented AES cryptography method in color image by genetic algorithms and path re-linking. It presents a hybrid approach that replaces the LSB substitution technique thus increasing the usage of color images to hide a text message.

N. Sasirekha et al. [9], presented a secured approach to spatial image steganography by altered the neighborhood pixels of the cover image. Objective of this algorithm works in the presence or absence of image background and also is expected be robust to estimate various levels of noise even in the presence of image artifacts like “ghost effect”. By this method, the embedded area looks more regular and uniform.

Sukalyan som et al. [10], proposed a modern steganography method grounded on matrix pattern and LSB algorithms proposed for RGB images. This technique utilize the spatial domain of image for hiding the information. The Matrix pattern divides the RGB image into numerous B*B block into non overlapping layer.

III. METHODOLOGY

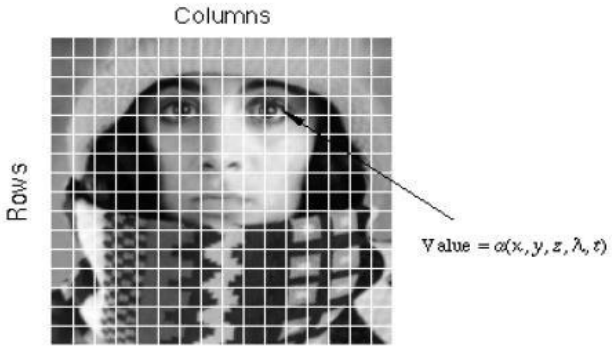

Figure 3.1: Digitization of an image

3.1 Image Processing :- The steganography thesis derives largely from the signal and image-processing research. An image may be defined as a two- dimensional as a function, f(x,y), where x and y are spatial coordinates, and the

amplitude of at any pair of coordinates (x,y) is known as the intensity or grey level of image at that point. When x, y, and the amplitude values of function (f) are all discrete and finite quantities then the image is said to be a digital image.

3.2 Image Compressions :- The bits are used to represent each pixel of an image file. The least bit depth is 8, which are for Monochrome and grey scale image (Owens 2002). They can display 256 shades or colors. The images are stored in 24-bit RGB color model file which called true color. Variations of image colors are derived from the primary colors of red, green and blue and each primary color is represented by 8 bits.

3.3 IMAGE COMPRESSION AND STEGANOGRAPHY :- Image compression play a significant role in deciding the stenographic algorithm to be used. The embedded image may be partially lost in lossy compression techniques, since part of the message may be discarded when compressed (Dunbar 2002). The secret message may not be lost in a lossless compression technique but the image is not compressed to a small size as well.

3.4 **BASIC TERMS OF STEGANOGRAPHY**

Cover image – the carrier which used to preserve the embedded bits.

Stego image – Cover image after the embedding information.

Key – key is mandatory for embedding and extracting to obey "Kirchhoff's principle". **Capacity / Payload** –. The capacity of the system is defined as the maximum size of the secret information that can be hidden

Robustness –ability to withstand even an intentional attack.

Security – Security is the most important essential requirement of steganography technique, and it ought to be robust against steganalytic attacks, which may be passive or active.

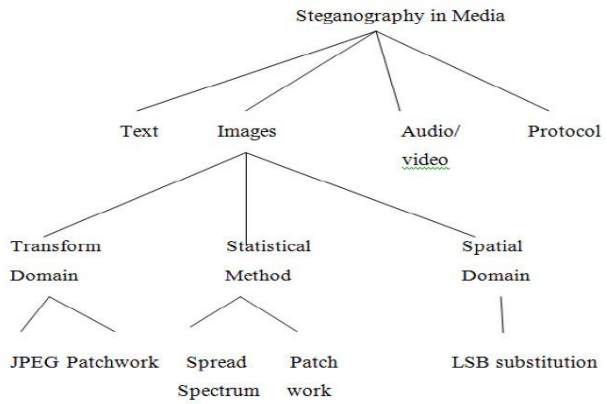

Figure 3.2: Categories of image steganography

3.3 IMAGE STEGANOGRAPHY :- Stenographic algorithms or techniques developed for image can be divided into three groups, namely Statistical techniques, Spatial Domain techniques and Transform Domain techniques. In the spatial domains, secret messages are embedded in the pixels directly.

3.4 TRANSFORM DOMAIN STEGANOGRAPHY :- In this technique, any one of the transformations is applied on the secret message and cover image the secret message is embedded in the transform coefficients. In JPEG steganography, the first step is to convert the RGB color representation to brightness and chrominance (YUV). Research studies indicated that human eye cannot comprehend changes in color compared to the changes in brightness (Currie & Irvine 1996). JPEG compression uses this concept initially to reduce the file size and down sample color data. The U and V values of Chrominance signal are divided by two, thus decreasing the file size by fifty percent. Once the file is halved the actual transformation of the image is done by using Discrete Cosine Transform (DCT), which transforms an image representation into a frequency representation.

IV. IMPLEMENTATION WORK

4.1 **SIMULATION PARAMETERS** The peak signal to noise ratio (PSNR) and mean square error (MSE) are used to measure the resulting error of watermarking image.

The mean square error (MSE) is defined as,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[y(i,j)-x(i,j)]^2 \qquad (4.1)$$

Where y(i,j) is the watermark image and x(i,j) is the original image.

4.2 PROPOSED METHODOLOGY :-

Cover-Image: An image in which the secret information is to be hiding. The term "cover" is used to describe the original message, audio, data, still, video etc. The cover image is sometimes called as the "host image".

Stego-Image: The medium in which the information is to be hidden. The "stego" data is the data which containing both the cover image and the "embedded" information. Logically, the processing of the hiding of secret information in the cover image is known as embedding.

Payload: The information that is to be concealed. The information which is to be hidden in the cover data is known as the "embedded" data

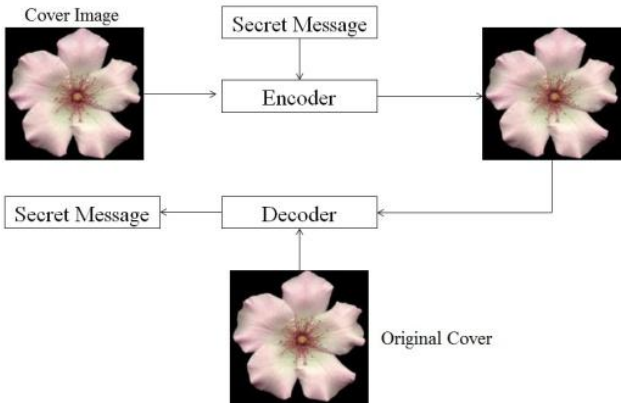

Figure 4.1: Block Diagram of Methodology

This method works best when the file is longer than the message file and if image is grayscale.

When applying the LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel. If the LSB of the pixel value of the cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

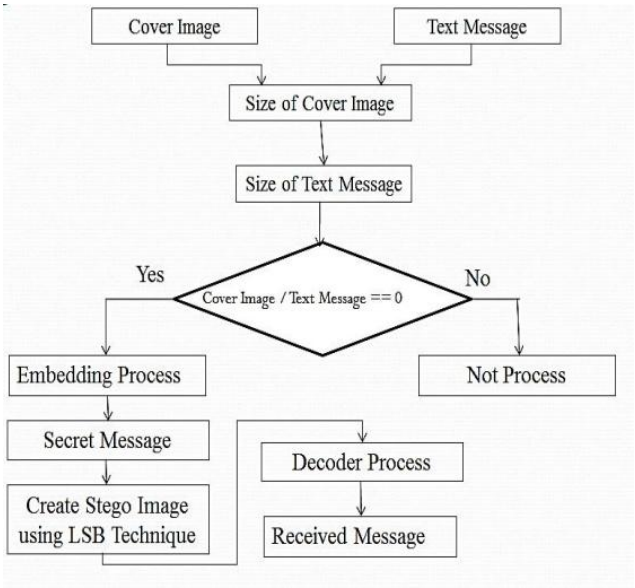

Figure 4.2: Flow Chart of Methodology

V. SIMULATION RESULT

5.1 SIMULATION RESULT :- Open the graphical user interface (GUI) window shown in the figure 5.1. In the figure 5.1 shows the window is divided into four part which is current folder, command window, workspace and command history. All the file path shown in the current folder and all the variable space used in MATLAB shown in workspace, all the command types in command window and history presented in all document.

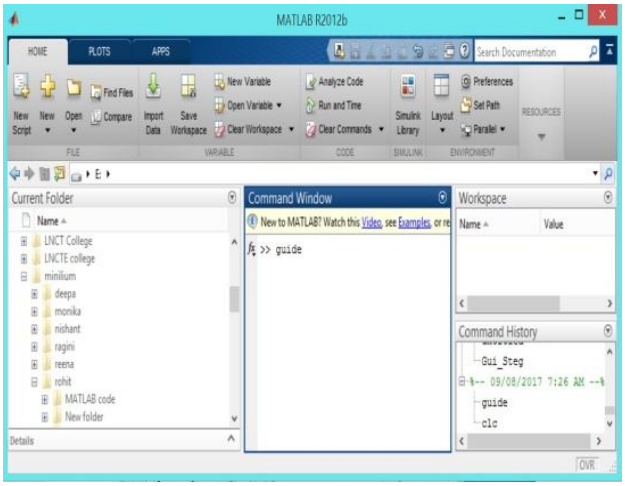

Figure 5.1: Open the Graphical User Interface (GUI) Window

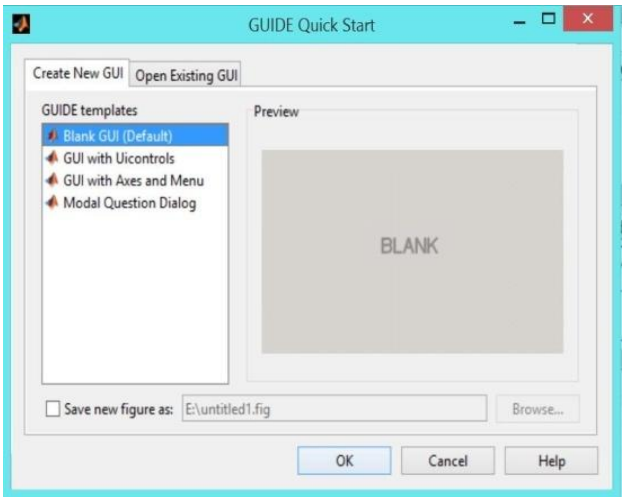

Figure 5.2: Graphical User Interface

Open the graphical user interface (GUI) window which is shown is figure 5.2. In the figure 5.2, shows the window is divided into four part which is current folder, command window, workspace and command history.

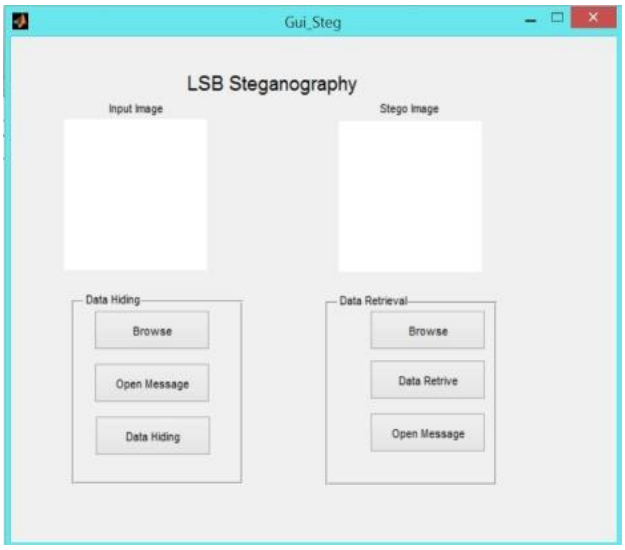

Figure 5.3: Window for LSB Steganography

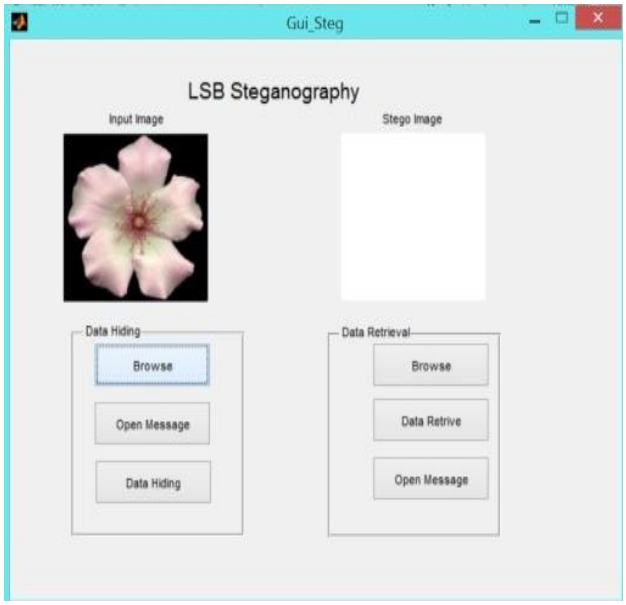

Figure 5.4: Window for Inter the Input Image

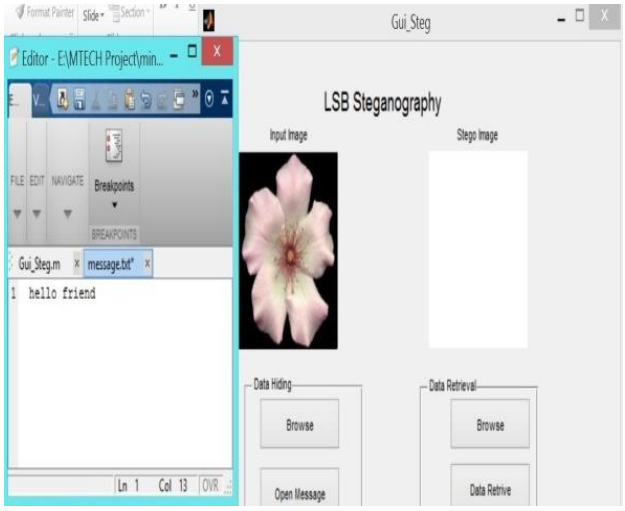

Figure 5.5: Window for Inter the Message

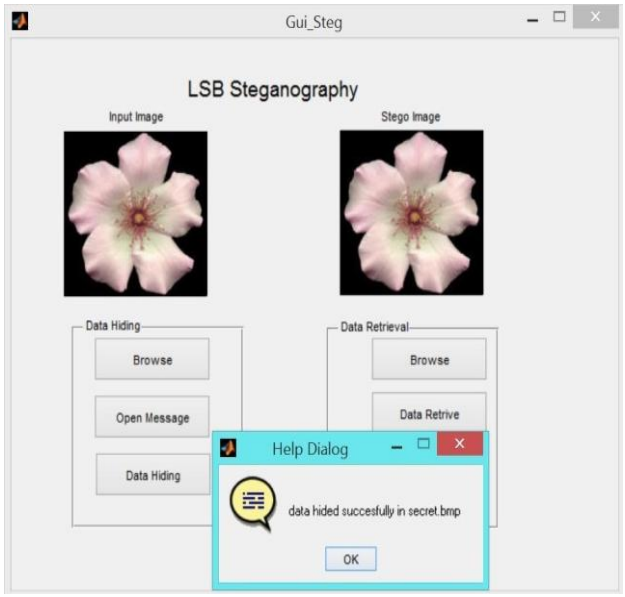

Figure 5.6: Window for Data Hided Successfully

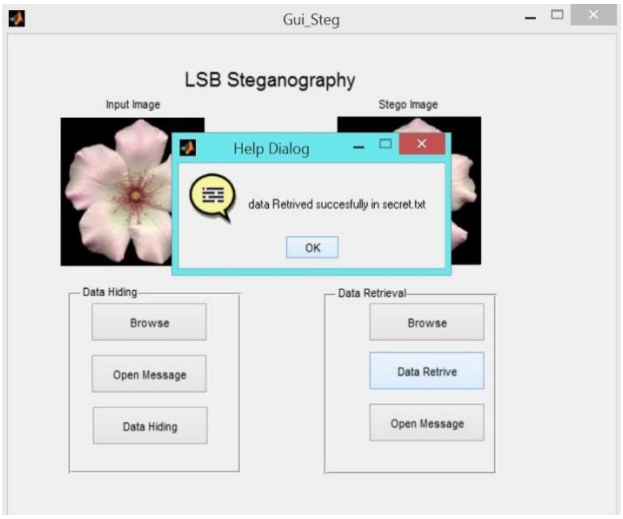

Figure 5.7: Window for Data Retrieved Successfully

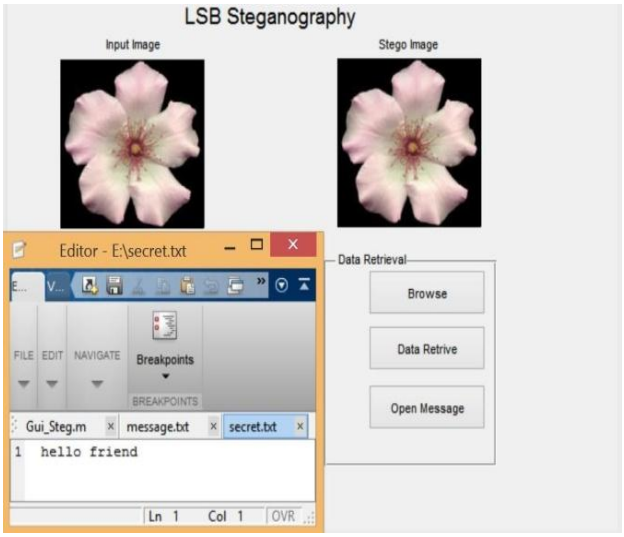

Figure 5.8: Window for Output Message

Table 5.1: Result for Different Image with 50 Characters

Image	Image Type	Characters	Parameter	
			MSE	PSNR
Flower Image	.jpg	50	0.0016	52.36 dB
Lena Image	.jpg	50	0.0013	53.46 dB
Building Image	.jpg	50	0.0011	53.87 dB
Tiger Image	.jpg	50	0.0012	52.78 dB

As shown in the table 5.1 the mean square error (MSE) and peak signal to noise ratio (PSNR) results are obtained for the proposed steganography method based on least significant bits (LSB) technique. From the analysis of the results

Figure 5.9: PSNR of the Different Image with 50 characters and .jpg format

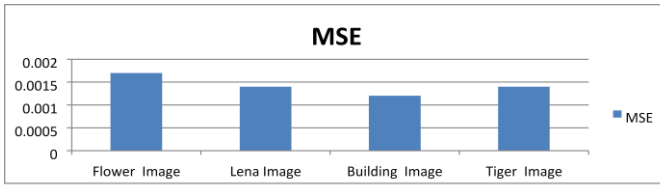

Figure 5.10: MSE of the Different Image with 50 characters and .jpg format

VI. CONCLUSIONS

6.1 CONCLUSIONS Steganography technique is one of the stimulating sub-disciplines of data hiding. Steganography is the one of the best art of secret communication using a medium like images. The important feature of steganography is to keep communication secure while transmitting images with hidden information. To fulfil this desire it is very important that the hiding data should not be introduced perceptual distortion in the cover image file and also be robust against steganalysis. The prominence of current research in image steganography has been focused more towards detection than developing novel hiding method.

6.2 FUTURE SCOPE OF WORK :- Stego algorithms can be developed to provide both very high security and very high embedding capacity without compromising the quality of image.

In most of the existing algorithms the statistical characteristics of stego images are reformed. This may give a possiblity to hackers to retrieve the secret information. So there is further scope for research in expanding algorithms in image steganography technique that will be able to present additional security topographies for concealing data.

REFERENCES

[1] Divya and N. Sasirekha, “High Capacity Steganography Method Based on Wavelet Transform”, Online International Conference on Green Engineering and Technologies (IC-GET), IEEE 2016.

[2] Saikat Mondal, Rameswar Debnath, Borun Kumar Mondal, “An Enhanced Color Image Steganography Technique in Spatial Domain”, 9th International Conference on Electrical and Computer Engineering 20-22 December, IEEE 2016.

[3] Ammad U Islam, Faiza Khalid, Mohsin Shah and Zakir Khan, “An Enhanced Image Steganography Technique based on MSB using Bit Differencing”, the Sixth International Conference on Innovative Computing Technology (INTECH), IEEE 2016.

[4] M. Tulasidasu, B.lakshmi sirisha and K. Rasool Reddy, “Steganography Based Secret Image hiding Using Block Division Technique”, International Conference on Digital Signal Processing, IEEE 2015.

[5] Z. Khan, M. Shah, M. Naeem, T. Mahmood, S.N.A. Khan, N. Amin, D. Shahzad, “Threshold based Steganography: A Novel Technique for Enhanced Payload and SNR”, International Arab Journal of Information Technology, vol. 13, No. 4, pp.380-386, 2016.

[6] N. Sasirekha and K. R. Kashwan, “Improved Segmentation of MRI Brain Images by Denoising and Contrast Improvement”, Indian Journal of Science and Technology: Vol. 8, Issue 22, pp.1-7, September 2015.

[7] Anupam K. Bairagi, Saikat Mondal and Rameswar Debnath, "A robust RGB channel based image steganography method using a secret key," Proceedings of the 16th International Conference on Computer and Information Technology, pp. 81-87, Khulna, Bangladesh, March, 2014.

[8] Sukalyan som,Atanu Kotal & Sarbani Palit “A chaos based partial image encryption structure”, in Business and information Management, International conference of security and system , pp. 58-63, on January 2014

[9] B. D. Parameshachari and K. M. Sanjiv, “A fast and secure image hiding technique based on partial encryption technique,” in challenges in research & technology in the coming decades(CRT), National conference on, pp. 1-4, September 2013.

[10] Wangyan and Ling-Di Ping, “A new Steganography technique based on Spatial Domain,” in Symposium on Information Science and Engineering, International conference, pp. 408-411, on January 2013.

[11] Barnali Gupta Banik Prof. Samir K. Bandyopadhyay“A DWT Method for Image Steganography ”in International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Volume 3, Issue 6, June 2013.

[12] Barnali Gupta Banik Prof. Samir K. Bandyopadhyay“A DWT Method for Image Steganography ”in International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Volume 3, Issue 6, June 2013.

[13] L. Ramya and N. Sasirekha,”A Robust Segmentation algorithm using morphological operators for detection of tumor in MRI”, Innovations in information, embedded and communication systems (ICIIECS) International conference on March 2015.

[14] Emad T. Khalaf, Norrozila Sulaiman,”Segmenting and hiding information randomly based on index channel,”

International Journal of Computer Science Issues, Vol. 8, No. 1, Issue 5, May 2011.

[15] H S Manjunatha Reddy, K B Raja , "Wavelet based Secure Steganography method with Scrambled Payload "in International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-1, Issue-2, July 2012.