# Improved and Optimally Shielded Multi Level Image Steganography

Sawan Soni[1], Prof. Arpit Solanki[2]

[1]*M. Tech. Scholar,* [2]*Research Guide*

*Department of Information Technology, RKDF School of Engineering, Indore*

***Abstract* - The image security is the going prominent among human being because of it is getting shared on various internet social media platforms and the authenticity of images are the primary tasks where creator has put several efforts to create or to capture of if there some kind of copyright laws associated with. So the distributed and shared images need to be authenticated with some information added with it, which will never compromise with the quality of image, and not even easy to guess or get hacked. Various algorithms were carried out to make security levels better in image steganography and had achieved multi level security also. In the same context this work also making efforts to make some unique way to integrate the information with the image which has multiple security levels. The proposed methodology has been tested on three different images and every image has been processed with different text lengths. The stego images has been evaluated with mean square error (MSE) and peak signal to noise ratio (PSNR) to compare with previous algorithms and show its performance.**

***Keywords* - Steganography, encryption, multi-level security, image forensics.**

## I. INTRODUCTION

Nowadays individuals exchange information straightforwardly using the existing communication technologies such as a local area network, a wide area network or simply the Internet. This information can be very sensitive and need to be protected against any intruder who can intercept them during the communication phase. Therefore, transferring sensible information cannot be solely relied on the existing communication technologies channels. We need then a robust technique to protect the information and ensure that they cannot be detected by other parties.

Steganography is the art of concealing sensible information into digital media (i.e., images, audio, text). It is a mechanism that completely differs from cryptography. In fact, in cryptography the information is modified but still can be seen in this unreadable format once sent over the networks, whereas in steganography the information is simply embedded into a digital support and cannot be noticed as long as the quality of the carrier is not deteriorated [5].

The steganography technique has been used many years ago to convey secret messages. For instance, a king in ancient Greece used to shave the slave's head and tattooed some secret information on it. When the hair was grown, the slave was sent to distribute the message. The receiver then shaved the hair and get the secret message [6]. In modern life, steganography is employed for many purposes such as embedding copyright [6], embedding individual's detail in smart IDs and inserting patient detail in medical imaging system. There has been a rapid growth of interest on steganography particularly with intelligent service institutions. For instance the US Pentagon has recently allocated significant funds to conduct research in this area, as they believe that terrorists may use this methodology to exchange information.

Steganography hides information into a digital media called cover object which can be a video clip, a digital image, an audio file or simply a text. This digital media is called respectively a cover image, a cover audio, a cover video, and a cover text. Once the information is embedded in that cover it is called a stego-object. If the cover is an image or an audio file, then the result of embedding the information in the cover is referred to as stego-image or stego-audio respectively.

It is shown that images are excellent carriers to hide and exchange sensible information over networks [7]. Many algorithms have been proposed recently to hide information into images and preserve their quality. In this Master thesis we focus on image steganography algorithms. An image consists of light luminance or pixels represented as an array of values at different points. A pixel consists of one byte or more. For example in 8-bit images each pixel consists of 1 byte (i.e., 8 bits). While each pixel in a 24-bit image is represented as three bytes representing the Red, Green and Blue (RGB) colors [6]. Any variation of the bits can lead to a different color.

In a good steganography algorithm, there are five vital features that should be considered [8]. The first one is the capacity payload which refers to the amount of secret information that a stego-cover can carry before the distortions become noticeable. The second feature is the un-detectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed. Other features that should be considered are: invisibility, security and robustness.

One of the most common reasons that intruders can be able to gain unauthorized access of information and they can use this information for their own purpose, to harm someone, modify and attack . As the technologies are continuously growing due to possibilities of information to be hacked or unauthorized are also growing and in modern era communication need special kind of protection from intruders. It's not only limited up to information or communication, it also applies on computer network because internet is only the medium to exchange the message. So, providing more security to computer network is more important because most of the information is transferred over the internet

## II. SYSTEM MODEL

Steganography is a word of Greek origin. The word Steganos means covered and Graptos means writing. It's conducted in a way that the existence of secret communication between two parties or more are hidden to snoops. The secret messages can be hidden in less suspicious digital objects that is not detectable by human perceptibility. Then the person who possesses the stego-key can only extract the message from the stego-object at the target destination.

An illustration of the steganography process to embed and extract a message is presented in Figure 2.1. This example uses an image as the cover object to carry bits of the secret message. At the sender's side, the secret message is embedded into the cover image by using some embedding function and the stego-image can be parameterized by a stego-key. Then the stego-image is sent over a communication channel to the receiver. The communication channel can be any type of transmission technologies that exist such as the Internet or E-mail. Then at the receiver's side the secret message is extracted using the extracting function. In addition, the extracting function uses the shared stego-key if it was used in the embedding phase.

The five features of steganography recognized in are: undetectability, invisibility, security, capacity and robustness. The following paragraphs will explain each type of the properties that characterize steganography.

It is critical in any steganography system to provide undetectability feature. The existence of the secret message in the stego-object should not be revealed by steganography systems that detect the presence of secret information. The steganography systems that use statistical analysis to detect the existence of secret messages in a stego- object are called steganalysis.

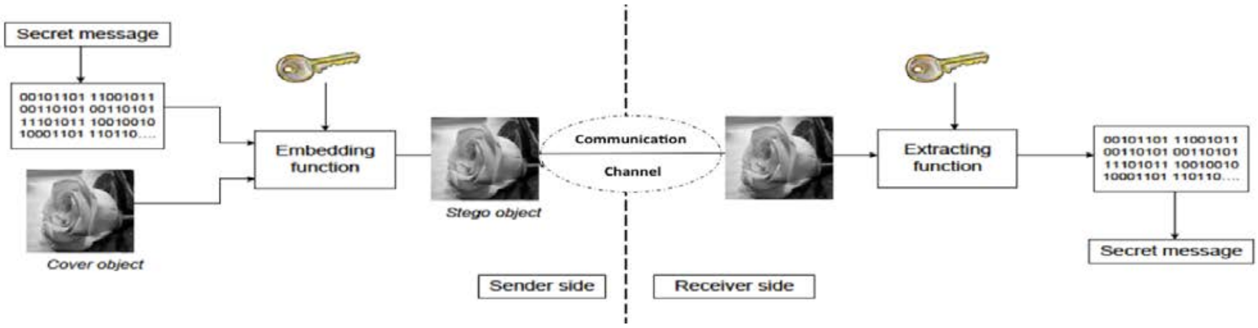


Figure 2.1 Process of Steganography

## III. PROPOSED METHODOLOGY

It is a well-known data-hiding technique used widely because of its straightforwardness. It conducts a modification to the least significant bit of the stego- image pixels, which change only the tone of the color. If the path is randomly generated then the pseudo random number generator PRNG is used. The PRNG should be seeded with some stego-key that is shared between the sender and receiver. In this way the message bits will be spread over the stego-image.

as depicted in figure 3.1 input cover image separated in RGB layers basically the system is divided in 4 blocks input block random string generator computation process and stego mage output.

The process can be better understood by the flow of process demonstrated in figure 3.2.

(1) Select Image for process of Steganography.

(2) Generate Random String of desired length.

(3) Divide the string in three parts.

(4) Convert ciphering text in to ASCII code.

(5) Based on ASCII codes make change in encryption code.

(6) Now convert the ASCII code in to Encrypted string.

(7) Convert the binary string to binary number.

(8) Make change in the cover image as per the binary sequence Layer wire (RGB) save the stego image (Encrypted image). And calculate the MSE and PSNR. the value of PSNR and MSE is displayed in table 1 and table 2

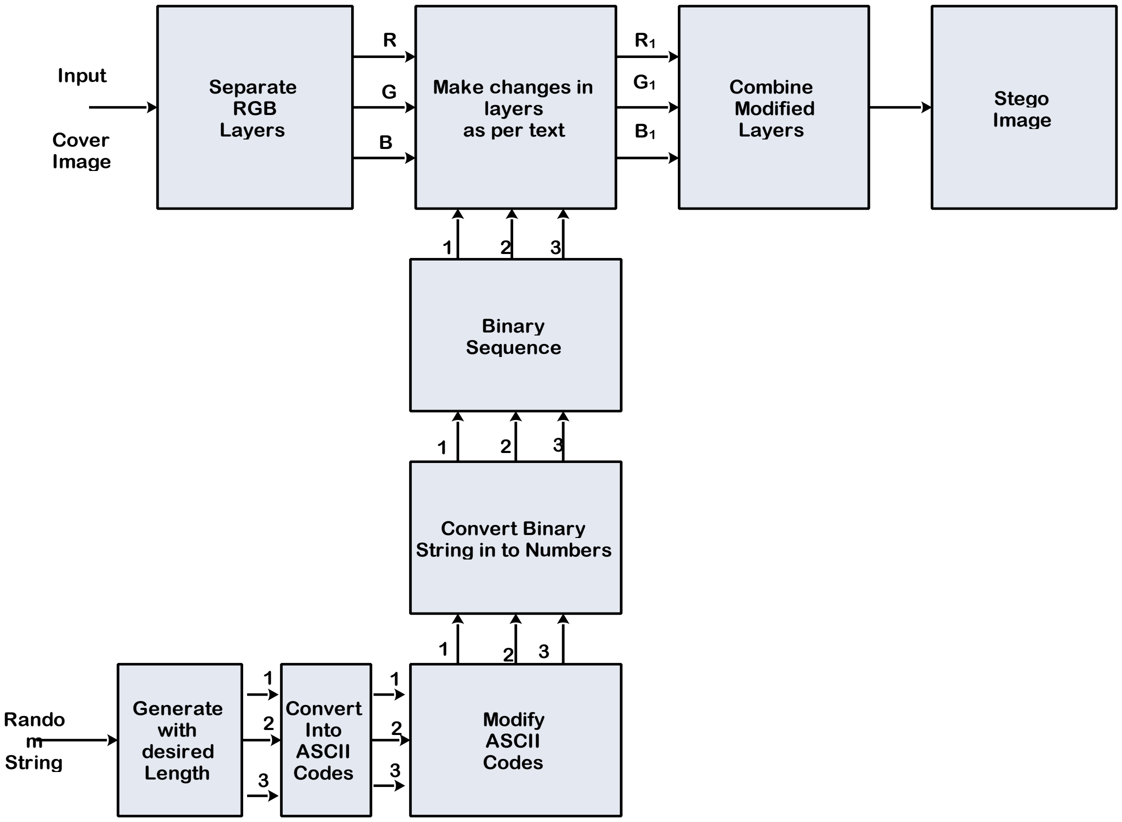


Figure 3.1 Proposed System Model.

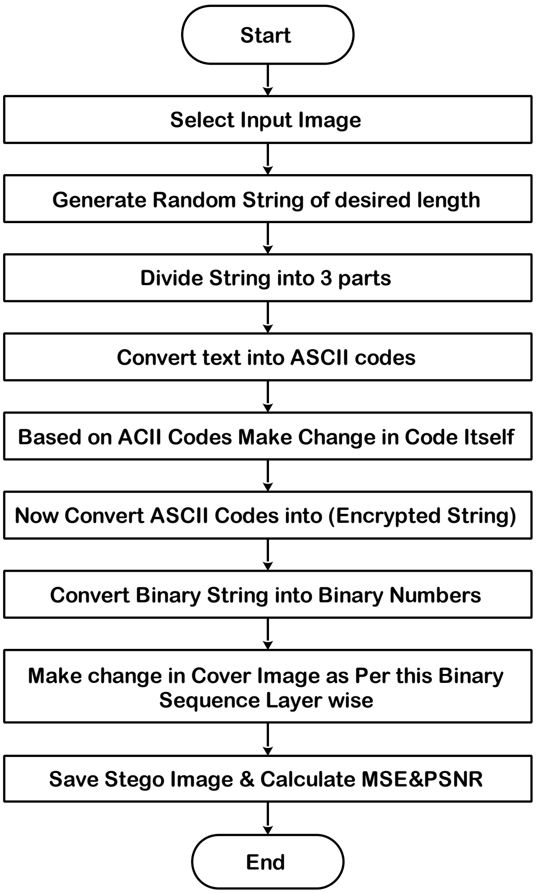

Start
Select Input Image
Generate Random String of desired length
Divide String into 3 parts
Convert text into ASCII codes
Based on ACII Codes Make Change in Code Itself
Now Convert ASCII Codes into (Encrypted String)
Convert Binary String into Binary Numbers
Make change in Cover Image as Per this Binary Sequence Layer wise
Save Stego Image & Calculate MSE&PSNR
End

Figure 3.2 Flow chart of the proposed system.

## IV. SIMULATION RESULTS

Table 1: PSNR of Different Images with Variable Texts Length

| Image | PSNR (in dB) for Different Text Length | | | | |
|---|---|---|---|---|---|
| | 100 | 200 | 300 | 400 | 500 |
| Lena | 75.6724 | 78.4237 | 80.1556 | 81.4906 | 82.2987 |
| Baboon | 75.5421 | 78.4184 | 80.2423 | 81.4609 | 82.3622 |
| Airplane | 75.4365 | 78.6207 | 80.3833 | 81.4314 | 82.4745 |

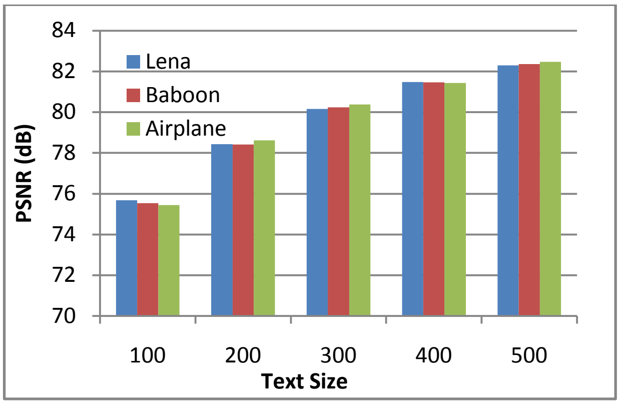


Fig. 4.1 Comparison Peak Signal to Noise Ratio (PSNR) for Different Text Sizes

Table 2: MSE of Different Images with Variable Texts Length

| Image | MSE for Different Text Length | | | | |
|---|---|---|---|---|---|
| | 100 | 200 | 300 | 400 | 500 |
| Lena | 0.0018 | 0.000942 | 0.00063 | 0.00046 | 0.00038 |
| Baboon | 0.0018 | 0.000943 | 0.00061 | 0.00046 | 0.00038 |
| Airplane | 0.0019 | 0.000900 | 0.00060 | 0.00047 | 0.00037 |

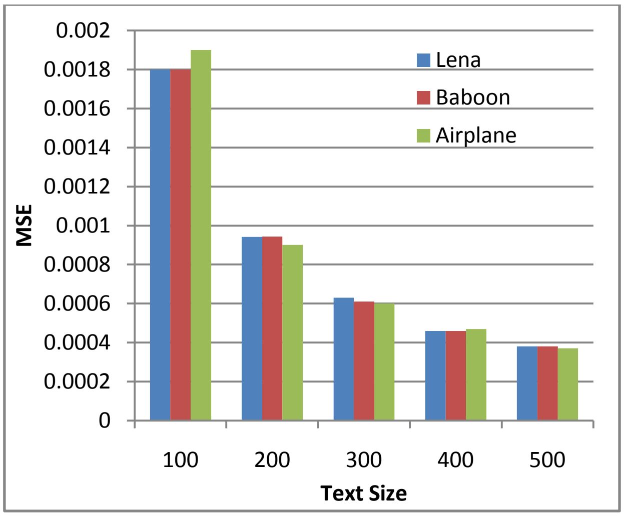


Fig. 4.2 Comparison Mean Square Error(MSE) for Different Text Sizes

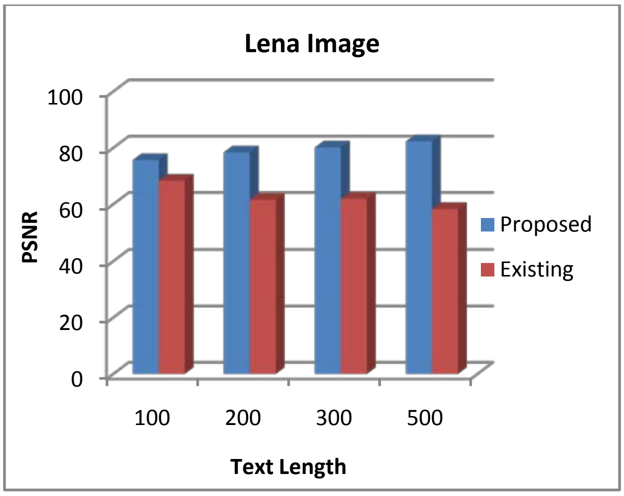


Fig. 4.3 Comparison PSNR of Lena Image with Different Texts Lengths

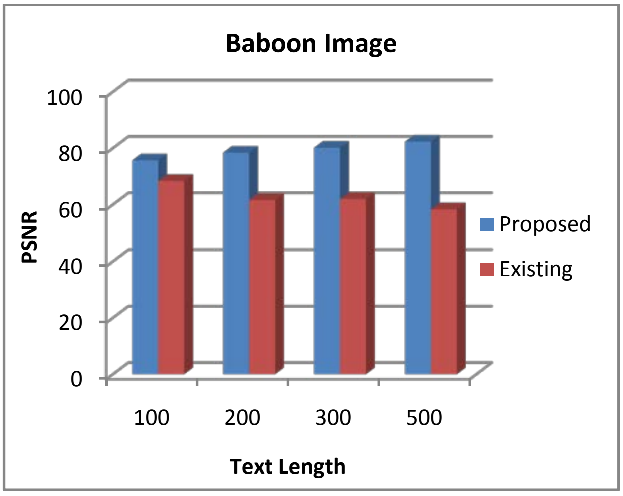


Fig. 4.4 Comparison PSNR of Baboon Image with Different Texts Lengths

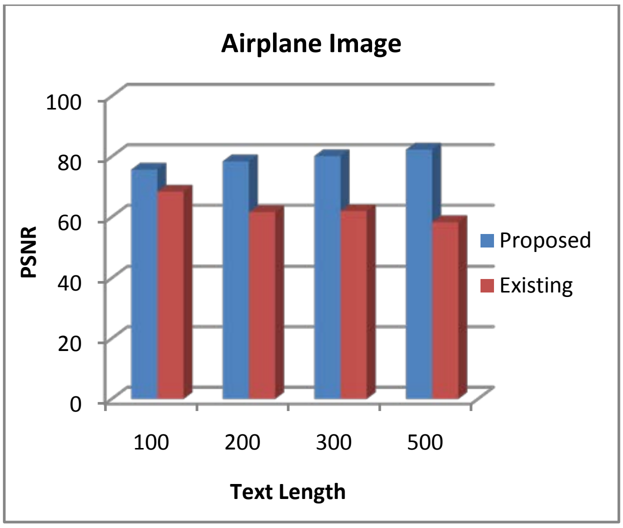


Fig. 4.5 Comparison PSNR of Airplane Image with Different Texts Lengths

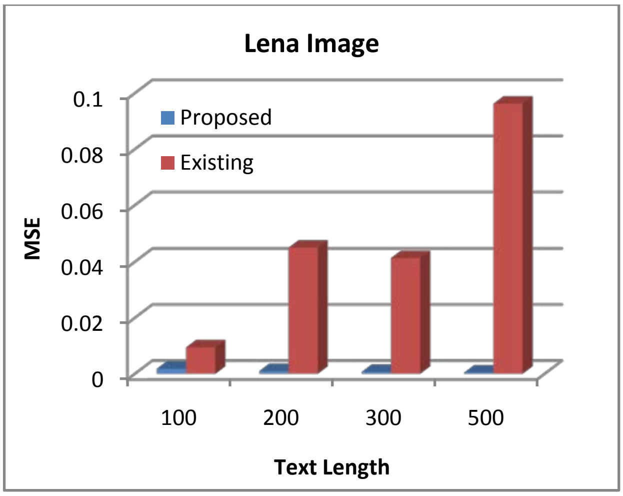


Fig. 4.6 Comparison MSE of Lena Image with Different Texts Lengths

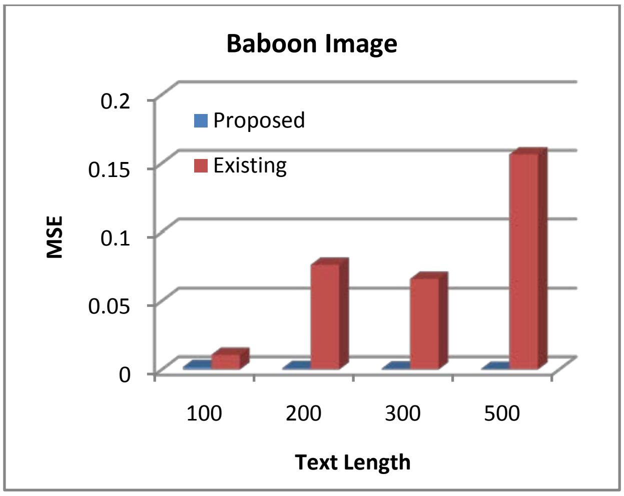


Fig. 4.7 Comparison MSE of Baboon Image with Different Texts Lengths

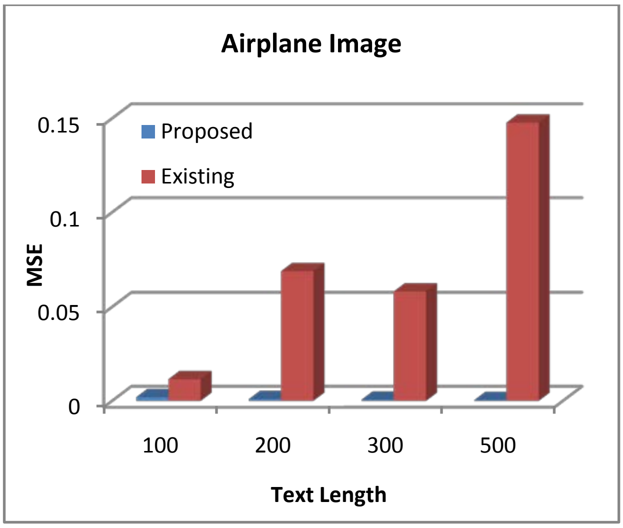
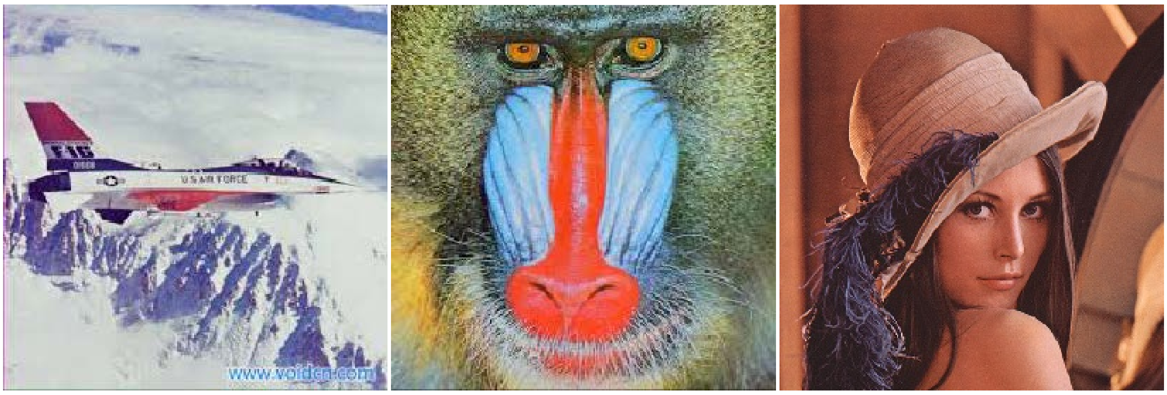


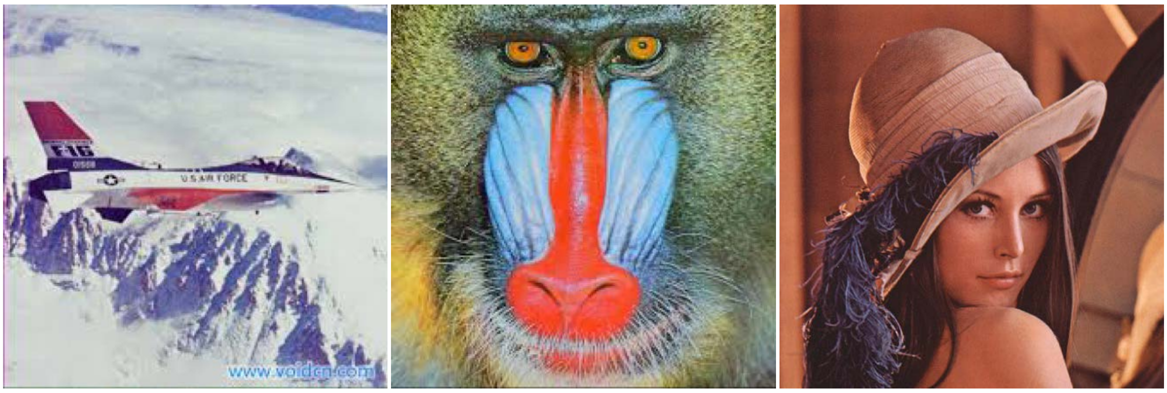
Fig. 4.8 Comparison MSE of Airplane Image with Different Texts Lengths



(a) Text Length 100

(b) Text Length 200

(c) Text Length 300



(d) Text Length 500

Fig. 4.9 Stego images with different text lengths of Airplane, Baboon and Lena Images

## V. CONCLUSION AND FUTURE SCOPE

A highly secured image unique way to integrate the information with the image which has multiple security levels steganography technique has been presented in this research work. Multiple levels of encryption have been added to the base steganography technique. The stego images has been evaluated with mean square error (MSE) and peak signal to noise ratio (PSNR) to compare with previous algorithms and show its performance. Proposed algorithm has added security and better performance when compared with base Lena Image with different text length image steganography technique. Future works includes extending this approach to various cover and secret formats.

## REFERENCES

[1] G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K, "A novel LSB based image steganography with multi-level encryption," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[2] Gomathymeenakshi,M., Sruthi, S .,Karthikeyan,B .,N ayana,M. ”An efficient arithmetic coding data compression with steganography”, in 2013 IEEE International.

[3] Guo,J,-M.,Le,T,-N, “Secret Communication Using JPEG Double Compression”, IEEE Signal Processing Letters, 17(10),5556462,pp.879-882.

[4] Hao,P.,Shi,Q. “Matrix factorizations for reversible integer mapping”, IEEE Transactions on Signal Processing. 49 (I0),pp. 2314-2324.

[5] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images," 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No.00TH8532), New York, NY, 2000, pp. 1279-1282 vol.3.

[6] Singla,D., Juneja,M. ”New information hiding technique using Features of image”, Journal of Emerging Technology in Web Intelligence, 6(2),pp.237-242.

[7] Mainberger,M.,Schmaltz,c.,Berg,M.,Weickert,J.,Backes,M. Diffusion-based image compression in steganography” 7432 LNCS (PART 2),pp.219-228..

[8] Conference on Emerging Trends in Computing and Nanotechnology,ICE-CCN 2013 6528520,pp. 342-345.

[9] Lin, Y.-K. “A data hiding scheme based upon DCT coefficient modification”, Computer Standards and Interfaces 36(5),pp.855- 862.

[10] Chen,Y.,Hao,P. “Integer Reversible Transformation to make JPEG lossless” 2004 7th International Conference on Signal Processings,ICSP. pp.837-840.

[11] Karthikeyan,B.,Vaithiyanathan,V.,Thamotharan,B.,Gomathy me enakshi,M.,Smthi,S.“LSB replacement steganography in an image using pseudorandomised key generation” Research Journal of Applied Sciences, and Engineer and Technology,4(5),pp.491-494.

[12] Hu,Y.,Wang,K.,Z.-M.” An improved VLC-based lossless data hiding scheme for JPEG images” Journals of Systems and Software 86 (8),pp.2166- 2173.

[13] Dr. K. L. Sudha, and Manjunath Prasad, (2011) “Chaos image encryption using pixel shuffling with Henon map,” in Proc. of Elixir Elec. Engg. 38, pp. 4492-4495.

[14] Kousik Dasguptaa, Jyotsna Kumar Mondal and Paramartha Dutta,” Optimized video Steganography using Genetic Algorithm (GA)” First International Conference on Computational Intelligence:Modelling Techniques and Applications,Vol lO ( 2013 ),pp. 131 - 137.

[15] Chang,C.-C.,Lin,C.-C.,Tseng,C.-S.,Tai,W.-L” Reversible hiding in DCT-based compressed images” information Sciences 177 (l3),pp. 2768-2786.

[16] Qian,Z.,Zhang,X.” Lossless data hiding in JPEG bitstream”, Journal of Systems and Software 85 (2),pp. 309-313.

[17] Bandyopadhyay,D.,Dasgupta,K.,Mandal,J,K.,Paramartha Dutta.”A Novel secure Image Steganography method based on Chaos theory in spatial domain”,International Journal Of Security,Privacy and Trust Management,Vol 3,No I.

[18] Karthikeyan,B. ,Ramakrishnan,S.,V aithiyanathan,V. ,Sruthi,S., Gomathymeenakshi,M. “An improved steganography technique using LSB replacement on a

scanned path image", International Journal of Network Security, 16(l),pp.14-18.

[19] Jovanovic,V,T.,Kazerounian,K, "Using Chaos to Obtain Global Solutions in Computational Kinematics", in Proc. of Journal of Mechanical Design, 120(2), pp. 299-304.

[20] Amigo,J.M.,Kocarev,L.,Szczepanski,J., "Theory and Practice of Chaotic Cryptography", Physics Letters, Section A:General Atomic and Solid State Physics,366(3),pp.211-216.

[21] Fridrich,J.,Du,R.,Long,M."Steganalysis and LSB Encoding in Color Images", IEEE International Conference on Media and Expo,(III/WEDNESDAY),pp.1279-1282.

[22] Saeed,M.J "A new technique based on chaotic steganography and encryption text in DCT domain for color images", in Proc. of Journal of Engineering Science and Technology,8(5),pp.508-520.

[23] Arun A.S. and George M. Joseph, (2013) "High Security Cryptographic Technique using Steganography and Chaotic Image Encryption", in Proc. of Journal of Computer Engineering (IOSRJCE), Vol 12, pp 49-54.