iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

A New Paradigm of LSB Based Image Steganography with Cryptography Using DIFFIE Helman Algorithm

S. Guneswari[1], R. Balu[2]
[1,2] *Research Scholar, PG & Research Department of Computer Science Sudharsan College of Arts & Science , Pudukkottai – 622 10, Tamilnadu, India*

Abstract: ***The steganalysis is the technology that detects the presence of the message and blocks the covert communication. Several techniques have been presented in the literature. The main purpose of steganography is to secure the communication. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. Because this method is susceptible to steganalysis to make it safe, this system embeds the original data in the image before it is encrypted. While the encryption process adds time to complexity, but at the same time offers higher security as well. This paper uses Diffie Hellman algorithm to encrypt the data. The result shows that the use of encryption in Steganalysis does not affect the time complexity if Diffie Hellman algorithm is used instead of RSA algorithm.***
Keywords: ***Cryptography, Image hiding, Least - significant bit (LSB) method, Steganography***

I. INTRODUCTION

Steganography is art of concealing a file, message, image, or video within another file, message, image, or video. Steganography is derived from Greek and literally means “covered writing”. In Steganography, we hide the secret image in such a way that it will be undetectable. To achieve a good result that is good image quality, covered media should be chosen in such a way that it is having good capacity. Cryptography also used for security but sometimes we need to secure the message, hence steganography came in picture. Steganography is classified in different types like image steganography, audio, video [1]. These are classified according to embedding the secret data. If secret data is embedded inside the image then it is image steganography, if secret data is embedded in audio then it is audio steganography and so on. Steganography depends on concealing undercover message in unsuspected mixed media information and is by and large utilized as a part of mystery correspondence between recognized gatherings. Steganography is a system for encryption that shrouds information among the bits of a cover object, for example, a realistic or a sound record. The method replaces unused or inconsequential bits with the secrete information. Steganography is not as hearty to assaults subsequent to the inserted information is powerless against obliteration.

Steganography is an art of invisible communication, achieved by hiding secret message inside a carrier file like image. Mainly steganography techniques are of four types, (i) steganography in image, (ii) steganography in audio, (iii) steganography in video, and (iv) steganography in text. Image steganography schemes are categorized into two major types, (i) spatial domain techniques, and (ii) transform domain techniques [2]. The spatial domain techniques perform direct manipulation over the pixels of the image. The transform domain techniques use some transformations to transform the image into transform domain and then hide the secret message [3].

The image with secret message hidden inside it is called as the stego-image. There are various categories of techniques in spatial domain, (i) LSB substitution, (ii) pixel value differencing (PVD), (iii) exploiting modification direction (EMD), etc. The transform domain techniques are based on various transforms like, (i) DCT, (ii) DWT, and (iii) FFT. In a steganography technique if the host image can be recovered along with the data from the stego image, then it is called reversible steganography [4]. Reversible steganography techniques are available both in spatial domain and transform domain. In image steganography the unnatural message is hidden inside a natural image in such a way that the distortion is minimum so that the intruder cannot notice it. The most familiar image steganography technique is the least significant bit (LSB) substitution. The LSB substitution can be extended upto 4 LSB planes to achieve higher embedding capacity. It is the simplest technique, but vulnerable to RS analysis. The LSB substitution can be enhanced in the following ways. The LSB bits of all the pixels can be formed as LSB array. The secret binary words can be hidden at minimum distortion locations of LSB array, so that the security could be improved. Similarly, the bits from four LSB planes can form four LSB arrays and the binary message can be partitioned into four parts and then one part of the message can be

hidden in one LSB array at minimum distortion locations, so that security can be improved. To increase the hiding capacity and security, the three LSB planes can be investigated, but only two bits can be embedded in two selected planes based on the secret data bits [5]. This is called data dependent embedding. Similarly, only two LSB bits can also be used to achieve data dependent embedding.

II. LITERATURE REVIEW

R. Vijayarajeswari et al., represents a compression scheme based image security algorithm for wireless sensor network is proposed to hide a secret color image within the source color image. The main contribution of this paper is to propose a compression scheme which is based on level matrix and integer matrix, and increases the compression level significantly. The performance of the proposed system is evaluated in terms of peak signal to noise ratio (PSNR), mean square error (MSE), number of pixels change rate (NPCR) and unified average changing intensity (UACI). The proposed method achieves 42.65% PSNR, 27.16% MSE, 99.9% NPCR and 30.99% UACI. The proposed system has high information entropy which indicates the strength of the security system and achieves average PSNR about 41.9 dB and average MSE about 28.45. The methodology in this paper achieves 99.9% of number of pixels change rate (NPCR) and 30.99% of the unified average changing intensity (UACI) [1].

Falesh M et al., intends to give an overview of image Steganography, its uses and techniques. It also attempts to identify the requirements of a good Steganography algorithm and briefly reflects on which Steganography techniques are more suitable for which applications. Different image file formats have different methods of hiding messages, that having different strong and weak points respectively. Whereas one technique lacks in payload capacity, while other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but it can hides only a very small amount of information. The Least significant bit (LSB) technique in both BMP and GIF makes up for this, but these both approaches result in suspicious files that increase the probability of detection when in the presence of a warden for an agent to decide on which steganographic algorithm to use, firstly he has to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others [2].

Odai M et al., a new algorithm for image steganography has been proposed to hide a large amount of secret data presented by secret color image. This algorithm is based on different size image segmentations (DSIS) and modified least significant bits (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly instead of sequentially; this approach has been applied before embedding process. The number of bit to be replaced at each byte is non uniform, it bases on byte characteristics by constructing an effective hypothesis. The simulation results justify that the proposed approach is employed efficiently and satisfied high imperceptible with high payload capacity reached to four bits per byte. The algorithm is employed effectively over an insecure channel and working against attacks by producing high imperceptible steg images for both low and high payload [3].

Jithesh Korothan et al., proposed method called SNBR, uses a location map to guarantee the correct extraction of the secret data. The goal of this study is to avoid degradation of the cover and improve the confidentiality of the information being communicated. Experimental results show that the new method achieves good security and a higher peak signal to noise ratio for the same number of bits per pixel of embedded image. The generated stego images possessed less perceptual distortion compared with highly noised cover image. They also prove to be secured against RS steganalysis. The experimental results evaluated on natural images using different kinds of steganographic algorithms show both visual quality and security of our stego-images are significantly better compared to typical LSB-based approaches and their edge adaptive versions [4].

Pooja Rawat et al., gives deeply description of both image Steganography breaking strategies of them. It also discusses that which image format is most appropriate or best for our algorithm and how can we perform compression on that. we have presented the two main domains of Steganography i.e. image domain and transform domain. Both domains include various Steganographic algorithms. We have also presented them and how can we break them [5].

III.OVERVIEW OF STEGANOGRAPHY

The Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means “covered writing”. A Steganography system consists of three elements: cover-image (which hides the secret message),the secret message and the stegano-image(which is the cover object with mes-sage embedded inside it).

A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image [6]. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Conse-quently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision [7]. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

IV. DESIGN AND IMPLEMENTATION

For security, only encryption may not be enough, hence pro-posed project includes Steganography wherein encrypted data is hid into the image and then image is transmitted in the network.

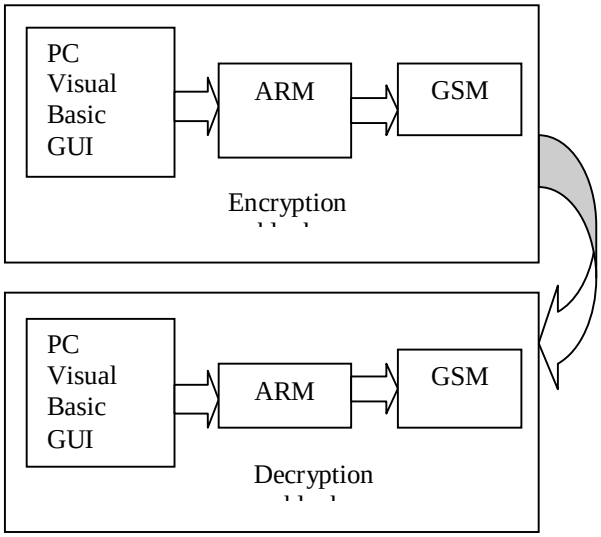


Fig. 1: Block diagram of Encryption

Encryption process: Read the secret and cover image and convert them into gray scale images, then check the size of the secret image with that of the cover image such that size of the secret image should be less than cover image [8]. Encode the secret image into binary using bit gate command and divide it into RGB parts then substitute MSB bits of secret image into LSB bits of cover image. Hide the password with Stego image. Decryption process: The reverse process takes place at the receiving end, Stego image can be decrypted using password.

A. Evaluation of LSB methods on GIF file format

GIF file format is used for storing multiple bitmap images in single file [9]. It was designed to allow easy interchange and viewing of image data stored on local or remote computer systems.GIF files are read as continuous stream of data and the screen is read pixel by pixel.GIF is a lossless compression format.

Three evaluation methods are,

1) Pattern analysis of Image Pixels. This method is based on looking for patterns in the bits that make up the pixel colors.

2) Pattern analysis of Image Palette This method is based on looking for patterns in the images palette

3) Low level Visual Inspection of Image Pixels

This method is based on carrying out a detailed inspection of selected sections of an image at a high degree of magnification.

B. Evaluation of LSB method in PNG file format

PNG (Portable Network Graphics) image file format is used for hiding messages. This is used as a container file.PNG supports indexed colors, gray-scale, and RGB. It works better in online viewing applications such as World Wide Web. A PNG file starts with an 8-byte signature. The hexadecimal byte values are 89 50 4E 47 0D 0A 1A 0A.After the PNG header chunks will arise continuously [10]. A chunk will contains four parts: length, chunk type/name, chunk data and CRC. PNG images can use either palette-indexed color or made up of one or more channels. Since multiple channels can after a single pixel, the number of bits per pixel is often higher than the number of bits per channel.

V. SIMULATION AND RESULTS

A. MATLAB Simulation

MATLAB is a high-performance language for technical computing. Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively. In this work, Matlab is implemented for processing LSB steganography technique with different frame size 256*256, 128*128, 64*64 and simulation results are shown. There are mainly four steps involved in implementing LSB steganography.

B. Conversion of Image To Matrix

In the conversion process of image to matrix we convert the input cover image into matrix values which is stored in a text file [11]. Firstly an image is read from computer, the original image is in the form of RGB which is converted into grey image. The grey image is resized to a particular size of 256*256. Each image has intensity values for every pixel, here these intensity values are stored into a text file.

C. Embedding Process

After completion of image to matrix the next step is to embed a message into an image. The image obtained during this process is called as stegano-embed image [12]. The message is embedded into the intensity values of image obtained during image to matrix conversion.

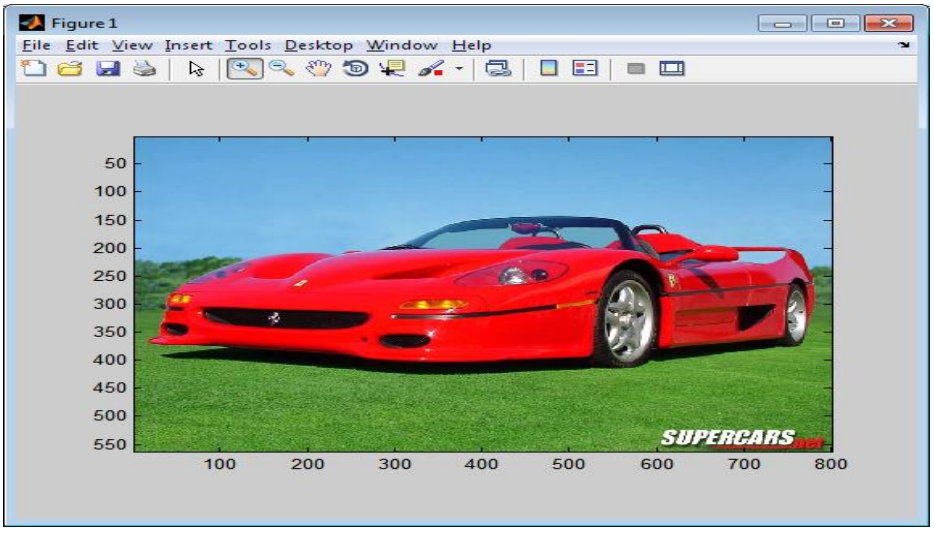


Fig. 2. Input Query Image

D. Conversion of matrix to image

In this stage intensity values are converted back to image. The image obtained has message embedded into it [13]. The cover image and the image obtained here have to be identical. Hence the objective of Steganography is satisfied [14].

E. Extraction process

In this process we extract the message which was embedded during embedding process [15]. At first declare a message byte, here the size of the message is 8 bits. Read a pixel from the array starting from address=0.Extract the LSB and replace the i th bit in the message byte where i =1 to 8 Ad-dress=address=1. When i =8, a byte is extracted. Repeat for extracting next byte.

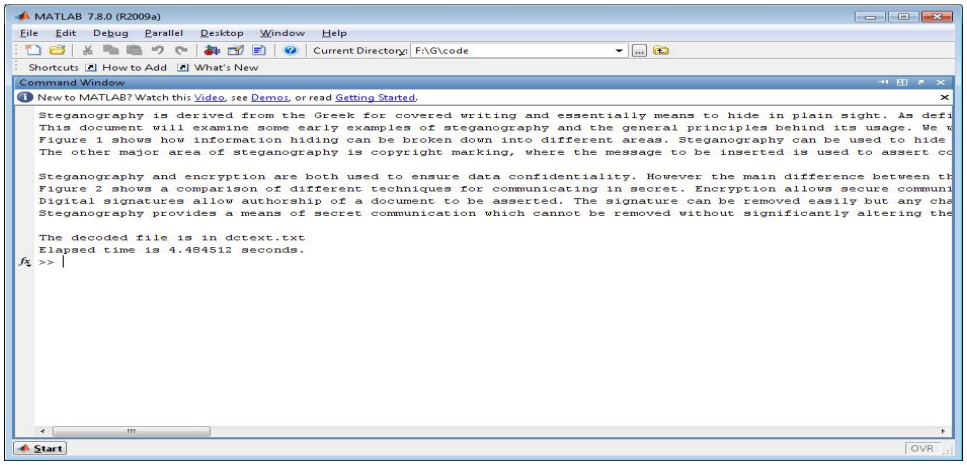


Fig.3. Output Data after Decryption

F. *Experimental Results*

Table 1. Time Complexity analysis for various input stegno images

Image Name	Image type	Resolution	Content size	Elapsed time for Encryption	Elapsed time for Decryption
Ferrari	.JPG	800*564	123 KB	3.690948	3.055553
Penguins	.JPG	1024*768	759 KB	12.308625	19.346595
Koala	. .PNG	1024*768	1709 KB	5.804328	4.591842
Jellyfish	.BMP	1024*768	2359.	5.400948	3.866312
Lena	GRAY	512*512	116 KB	3.449254	3.812467

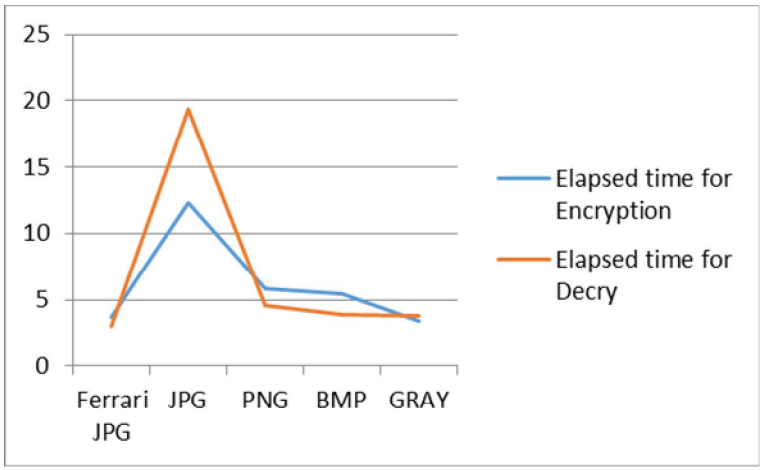


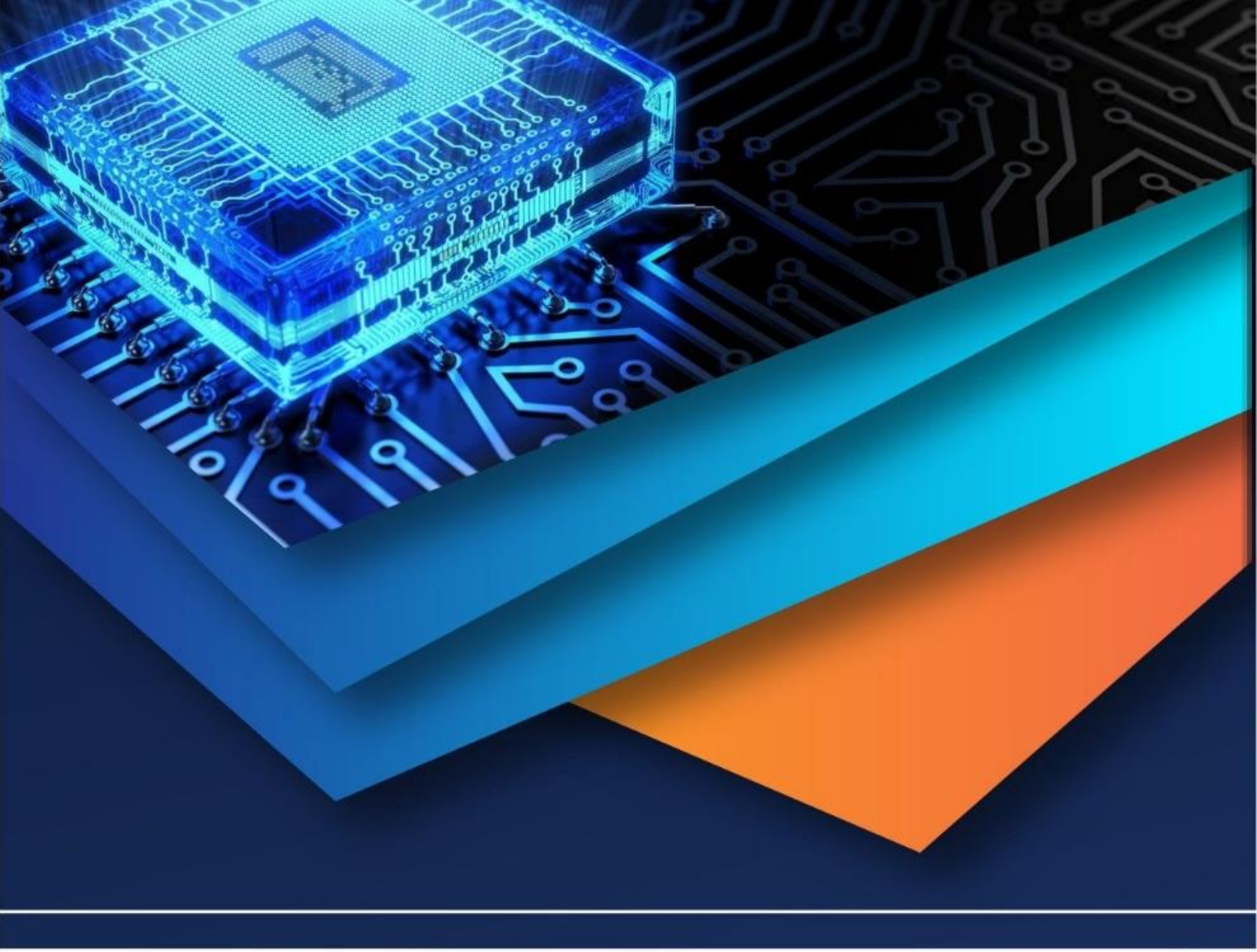
Figure 4. Time Measures for various steganalysis images

VI. CONCLUSION

The enhanced LSB technique described in this work helps to successfully hide the secret data into the cover object without any distortion. Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively. Since LSB doesn't contain any information there is no loss of information and secret image recovering back become undistorted. Cryptography with diffie hellman method is secures secret message in the stegno image with encoding scheme.

REFERENCES

[1] R. Vijayarajeswari, A. Rajivkannan, J. Santhosh, "A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN", Scientific Research Publishing Inc, 2016.
[2] Falesh M. Shelke , Miss. Ashwini A. Dongre , Mr. Pravin D. Soni by "Comparison of different techniques for Steganography in images", International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2014.
[3] Odai M. Al-Shatanawi and Nameer N. El. Emam by A New Image Steganography Algorithm Based on Mlsb Method With Random Pixels Selection, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015.
[4] Jithesh Korothan , Shirivas Kishor , and Pradeep Butey by "De-Noise Steganography by Enhancing the Cover Image: A Multi-Level Security Approach", The International Arab Journal of Information Technology, Vol. 13, No. 6A, 2016.
[5] Pooja Rawat, Amit Kumar Pandey, Shivpratap singh Kushwaha by "Advanced Image Steganographic Algorithms and Breaking strategies", International Journal of Computer Applications® (IJCA) (0975 – 8887) National Seminar on Recent Advances in Wireless Networks and Communications, -2014.
[6] Vijay kumar sharma, Vishal Shrivastava, "A Steganog-raphy algorithm for hiding image in image by improved LSB substitution by minimize technique", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.
[7] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon,, Image Steganography and: Concepts and Practice", Depart-ment of Electrical and Computer Engineering Department of Computer and Information Science Polytechnic Universi-ty,Brooklyn, NY 11201, USA.
[8] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu "A Comparative Analysis of Image Steganogra-phy",International Journal of computer Applications,Vol2- No3, May 2010.
[9] Saeed Mahmoudpour, SattarMirzakuchaki, "Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers", International Journal of Computer Applica-tions (0975 – 8887) Volume 37– No.7, January 2012.
[10] Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algo-rithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012.
[11] Bassam Jamil Mohd, Saed Abed and Thaier Al- Hayajneh, Computer Engineering Department Hashemite University, Zarqa, Jordan Sahel Alouneh,Computer Engi-neering Department, German-Jordan University, Amman, Jordan, "FPGA Hardware of the LSB Steganography Meth-od" IEEE 2012.
[12] Atallah M. Al-Shatnawi, "A New Method in Image ste-ganography with improved image quality", Applied mathe-matical science, Vol. 6, no79, 2012.
[13] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M, "Image Steganography Techniques: An Over-view", International Journal of computer science and securi-ty, vol (6), Issue (3), 2012.
[14] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, " A Sur-vey on Image Steganography and Steganalysis",Journal of Information Hiding and Multimedia Signal Processing c ISSN 2073-4212 Ubiquitous International Volume 2, Num-ber 2, April 2011.
[15] Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography, Global Journal of Computer Science and Technology", Vol.10, Issue 1, April 2010, pp.4-8.
[16] Rohit Garg, "Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images Vol.1, Issue 8,Oct 2012".,International Journal of Engineering Research and Technology(IJERT).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY