# Secure Communication Method Based on Encryption and Steganography using Least Significant Bit (LSB) Technique

**Kinan Sharon Minz[1] Pradeep Singh Yadav[2]**
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Electronics and Telecommunication
[1,2]Shri Shankaracharya Technical Campus, SSGI, Bhilai, India

*Abstract*— In this paper Steganography is done by LSB method. This paper, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.

***Keywords:*** Steganography; Encryption; Decryption, LSB

## I. INTRODUCTION

Steganography presents the process of hiding information. This inserts data at the carrying intermediate for masking secret messages. The usual Steganographic application is the communications among the two parties. The host medium taken generally for Steganography are digital medias like digital image, text, Audial, video, 3D model etc. The cost of embedment of secret data at the cover image creates image disruption. This has to two shortcomings. Firstly, cover image is fixed, secret messages embedment causes more image distortion. Therefore, finding the middle ground amongst the embedding capacity and the image quality resulting in the confined volume present in any specified covered image. This is the method for detecting secret messages hidden in the Stego image. A Stego image holds disruptions. Thus having second limitation as it is possible that an image's Steganalytic algorithm can setback the image Steganography and revealing the covered data present.

Steganography has a secure transformation of communication amongst the two events is not known to the invader and the success is influenced by detecting the existence of the communication [1]. Steganographic techniques are field of exploration of many authors and researchers. Steganographic uses have increased with internet and multimedia. Furthermore, they implement network QoS service and for getting improving data safety. Steganography improves accuracy of simulations. Discrete Cosine Transform, Wavelet Transform, temporal or frequency masking are also used in this method. Characteristics of digital file formats like least significant bit, unused fields/bits from headers, compression ratio (in case of compressed multimedia files and others are used. Though this technique does not depend on the difficult concepts that do not need much data.

This paper provides a unique data-hiding process built with LSB method for digital pictures. LSB method with no loss data hiding is proposed. Visible property of the image is not affected by LSB data hiding technique. Steganography comprises of many applications like merging information at cover image like text, video, and image with no disruptions at the cover image. The today's image steganography is a hard for transferring the implanted data at target deprived of being distinguished. The LSB set of rules are realized and data is embedded into the least significant bits of cover image to derive the stego-image.

Methodology:

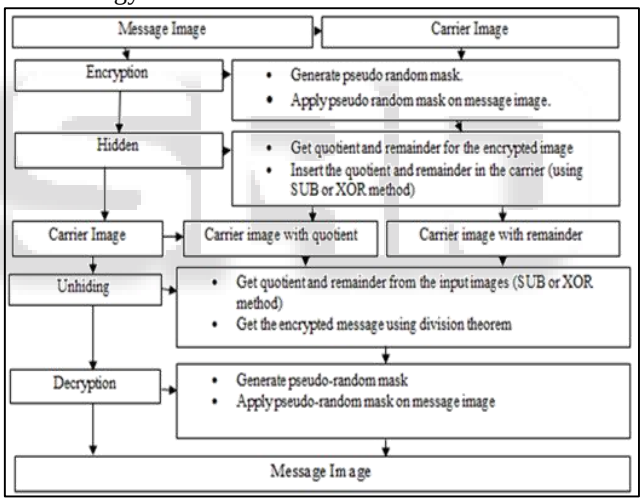



Fig. 2.1: Flowchart

The elementary model of steganography comprises of Carrier, Message and Password. Carrier is called as cover-object in which the message is implanted and helps to hide the presence of the message.

Message is the data that the sender wants to keep private. It could be plain text, cipher text, other image, or anything that could be embedded in a bit stream like the copyright mark, a covert communication, or a serial number. Password is called as the stego-key ensuring that it will be decoded with only recipient who knows the corresponding decoding key. The cover object having the secretly embedded message is called the stego-object.

The cover-object is needed for recovering message from a stego-object with the corresponding decoding key when the stego-key was used while the encoding process.

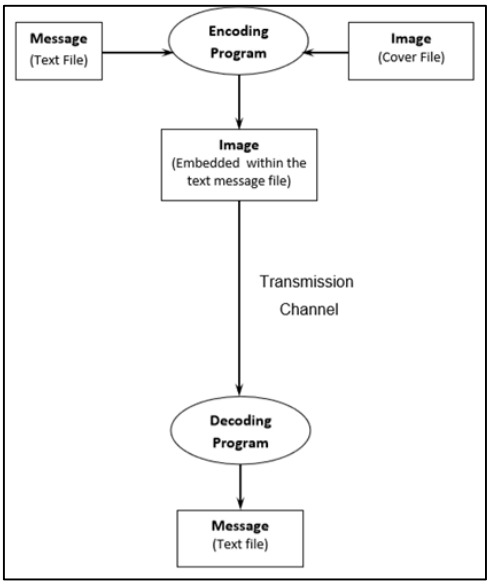



Fig. 2.2: Flowchart of LSB technique

Data masking in the least significant part of picture is done in LSB embedding techniques assuming that the resultant change is highly unnoticeable. Without losing the cover image visible quality and substantial data amount is embedded. The complete change to the image is so minor that cannot be found.

Hiding secret data in Cover image algorithm:

1) Cover image and secret text are read for embedding in to the cover image.
2) Private data compression.
3) Cipher text conversion of the compressed secret information with secret key sharing by receiver and sender.
4) Binary conversion of the compressed encrypted text message.
5) LSBs finding.
6) Insertion of the secret information bits into bits of LSB of the cover image.
7) Repeat the steps till the secret information is completely hidden into cover file.

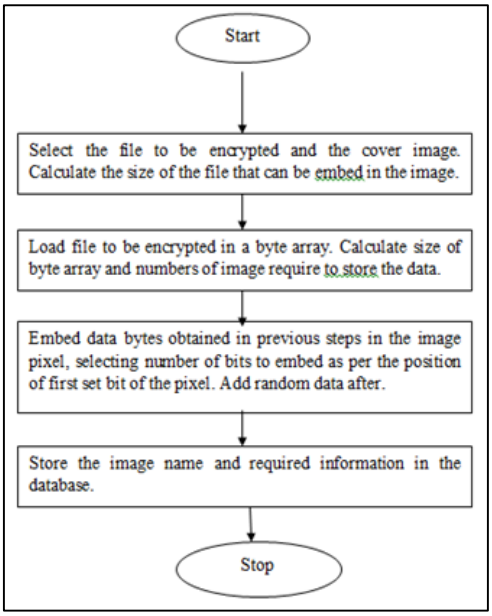



Fig. 2.3: Encryption Flowchart

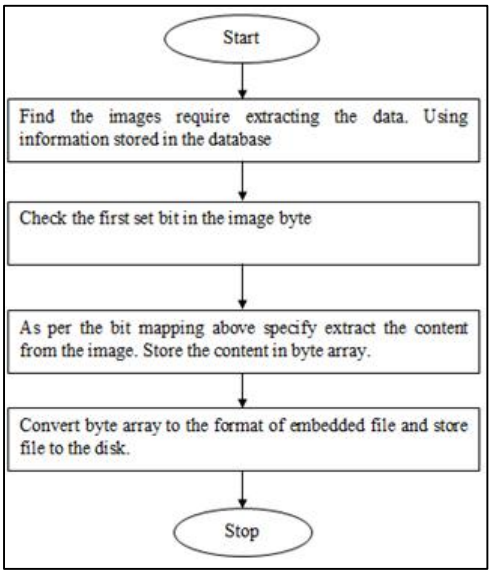



Fig. 2.4: Decryption Flowchart

## II. RESULT AND DISCUSSION

### *A. Encryption:*

The image is selected first through which the message data is to be encrypted. The figure 4 below shows the selection process.

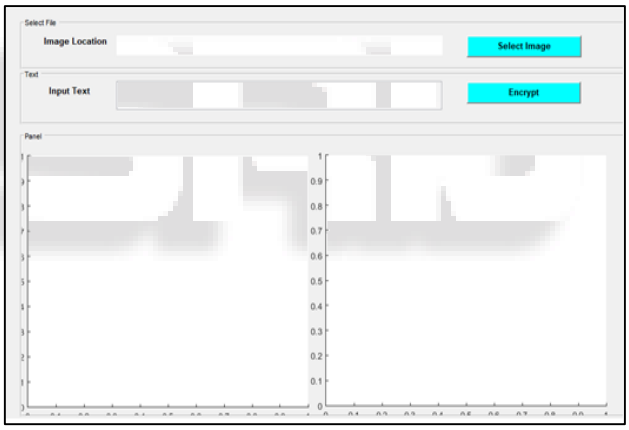



Fig. 3.1: Image selection and Message encryption


Fig. 3.2: Message encrypted

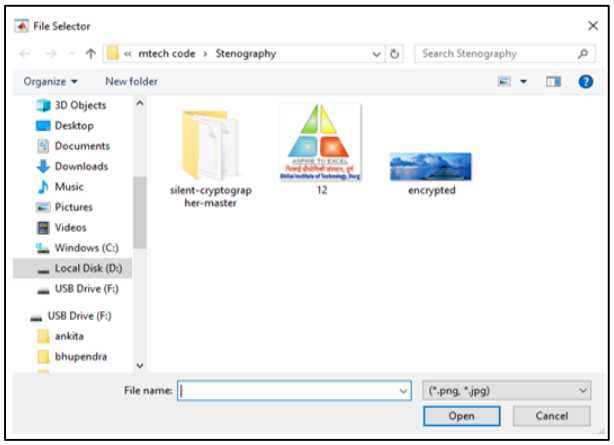



Fig. 3.3: Encrypted message with picture saved

### B. *Decryption:*

Similarly in decryption process the encrypted picture is selected from the location it is saved using the select image button as shown in figure 8.


Fig. 3.4: Encrypted image selection

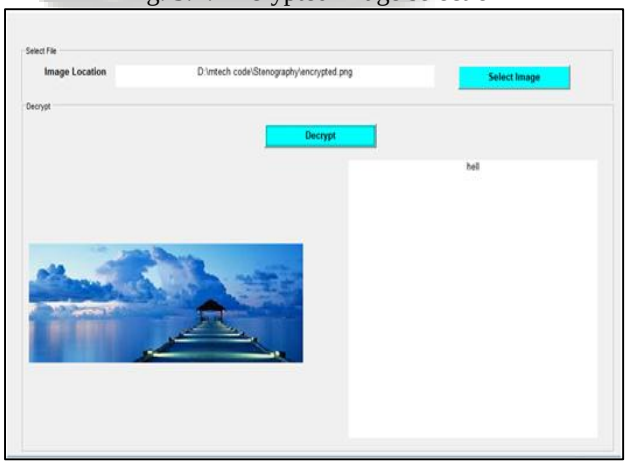



Fig. 3.5: Decrypted image and message

### C. *Histogram:*

A histogram represents the frequency distribution of continuous variables.

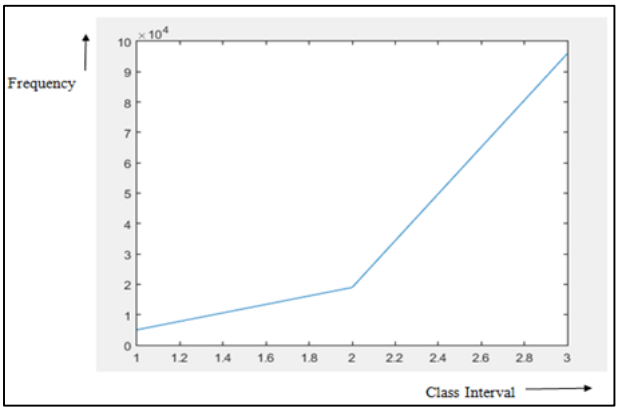



Fig. 3.6: Histogram of original image

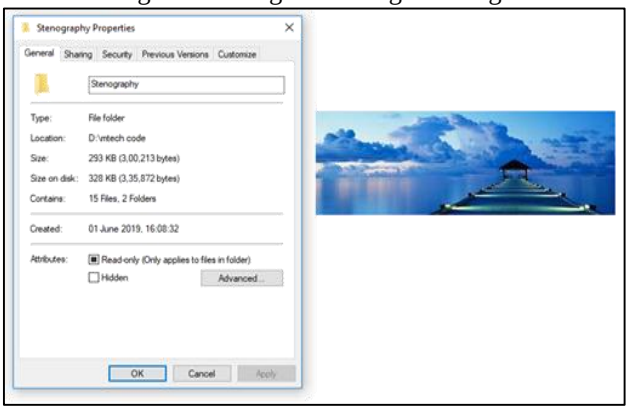



Fig. 3.7: Resolution of original image

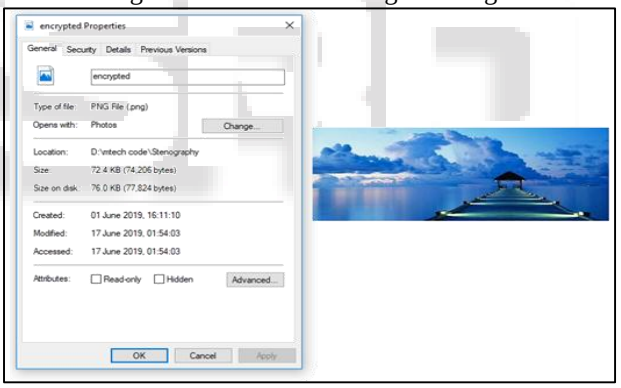


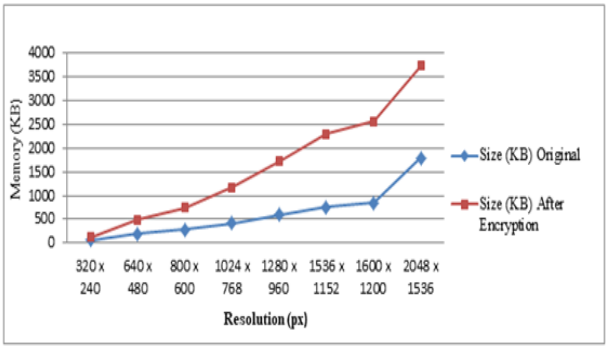

Fig. 3.8: Resolution of encrypted image

### D. *Memory vs Image Resolution:*

Memory specifies the total storage area or number of bits an image is occupying in the CPU. And resolution refers to the number of pixels in an image. Resolution is sometimes identified by the width and height of the image as well as the total number of pixels in the image.

| **Image** | **Size (KB)** | |
|---|---|---|
| **Resolution** | **Original** | **After Encryption** |
| 320 x 240 | 56 | 126 |
| 640 x 480 | 188 | 491 |
| 800 x 600 | 278 | 747 |
| 1024 x 768 | 418 | 1167 |
| 1280 x 960 | 594 | 1720 |
| 1536 x 1152 | 759 | 2293 |
| 1600 x 1200 | 850 | 2567 |
| 2048 x 1536 | 1792 | 3737 |

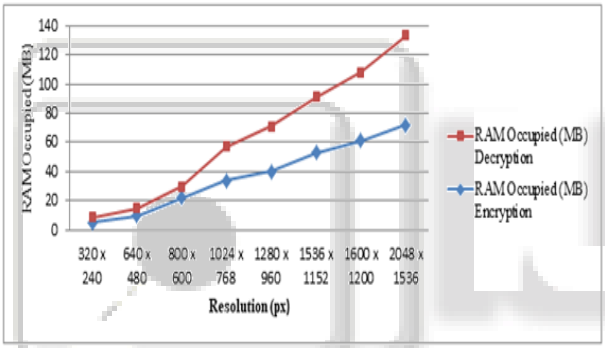
Table 3.1: Input Data for graph 3.1




Graph 3.1: Memory vs Resolution plot

| Image Resolution | RAM Occupied (MB) Encryption | Decryption |
|---|---|---|
| 320 x 240 | 5 | 4 |
| 640 x 480 | 10 | 5 |
| 800 x 600 | 22 | 8 |
| 1024 x 768 | 34 | 23 |
| 1280 x 960 | 40 | 31 |
| 1536 x 1152 | 53 | 38 |
| 1600 x 1200 | 61 | 47 |
| 2048 x 1536 | 72 | 61 |

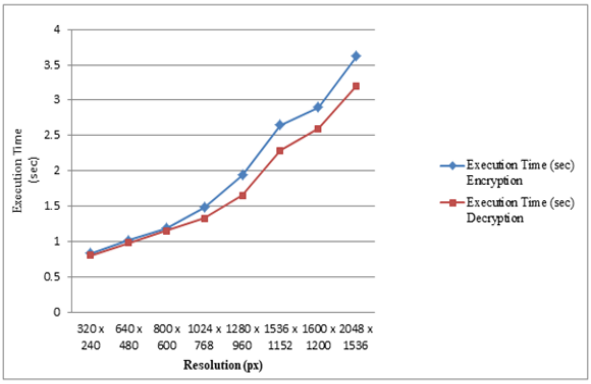
Table 3.2: Input Data for Graph 3.2




Graph 3.2: Memory vs Resolution plot

| Image Resolution | Execution Time (sec) Encryption | Decryption |
|---|---|---|
| 320 x 240 | 0.83 | 0.8 |
| 640 x 480 | 1.02 | 0.98 |
| 800 x 600 | 1.19 | 1.15 |
| 1024 x 768 | 1.48 | 1.33 |
| 1280 x 960 | 1.94 | 1.65 |
| 1536 x 1152 | 2.65 | 2.29 |

Table 3.3: Input Data for Graph 3.3




Graph 3.3: Memory vs Execution Time plot

## III. Conclusion

This paper presents a review of steganography and techniques that are used for steganography. Various papers have been reviewed on steganography. It is studied that there is various types of steganography like text, audio, video, image, network or protocol steganography [7]. This shows that text or data using steganography can be hidden in many ways.

This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties. Both steganography and cryptography can be woven into this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement. Also, the developed system has many practical, personal and militaristic applications for both point-to-point and point-to multi- point communications.

## IV. Future Scope

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

We hope to add support to hide all file formats. This allows for a much broader spectrum of uses: one would be able to encode .gif, .png, .pdf, .mp3, etc. The program would be more versatile because often hiding text just isn't enough. We also would like to implement batch image processing and statistical analysis so that we can run the program through a dataset of images and detect Steganography and perhaps crawl through Google Image Search to see how prevalent Steganography is. We eventually plan to port the program to use C/C++ so that we may take advantage of bit-fields in C and learn to code GUI's as well. I have a plug-in handler developed for C++ that I would like to use in this project so that third-party developers may contribute to the project.

## References

[1] ShashikalaChannalli, Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.
[2] MustafaCemKasapbas and WisamElmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sådhanå (2018) 43:68 Indian Academy of Sciences, vo(lV)FT3](0123456789().
[3] C.P.Sumathi,T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[4] R.Poornima and R.J.Iswarya, "ANOVER VIEW OF DIGITAL IMAGE STEGANOGRAPHY", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, February 2013.
[5] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.
[6] KetkiThakre, NehalChitaliya, "Dual Image Steganography for Communicating High Security Information", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-3 July 2014.
[7] RonakDoshi, Pratik Jain, Lalit Gupta, "Steganography and its Application in Security", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.
[8] Mr.Pravin R. Kamble, Mr.Prakash S. Waghamode, Mr.Vilas S Gaikwad, Mr.Ganesh B. Hogade, "Steganography Techniques: A Review", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 10, October – 2013, ISSN: 2278-0181.
[9] YunuraAzuraYunus, SalwaAbRahman, Jamaludin Ibrahim, "Steganography: A Review of Information Security Research and Development in Muslim World",American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-11, pp-122-128.
[10] Richa Khare1, Dr. Kuldeep Raghuwanshi2, "A REVIEW OF VIDEO STEGANOGRAPHY METHODS", Volume 2, Issue 1, January 2014 International Journal of Research in Advent Technology.
[11] MirzaAbdurRazzaq,Riaz Ahmed,ShaikhMirza, Adnan Baig.Ashfaque Ahmed Memon, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 5, 2017.
[12] Nikita AtulMalhotraȦ* and NikunjTahilramaniȦ, "Steganography Approach of Weighted Speech Analysis with and without Vector Quantization using Variation in Weight Factor", nternational Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161.
[13] HyderYahyaAtown, "Hide and Encryption Fingerprint Image by using LSB and Transposition Pixel by Spiral Method", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014, pg. 624-632.
[14] AshadeepKaur*, 2Rakesh Kumar, 3Kamaljeet Kainth, "Review Paper on Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016, ISSN: 2277 128X.
[15] Rashmi A. Sonawane*1, Mrs. Dipti Sonawane2, "Reversible Texture Synthesis Using Three Level Security in Steganography", © 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X Themed Section: Science and Technology.