www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-8, Issue-4, August 2018

International Journal of Engineering and Management Research

Page Number: 59-62

DOI: doi.org/10.31033/ijemr.8.4.7

Implementation of Steganographic Model using Inverted LSB Insertion

Shubhangi D. Kamat[1], Prof. S.S. Patil[2] and Prof. A.S. Mali[3]

[1]M.E. Student, Department of Electronics Engineering, Tatyasaheb Kore Institute of Engineering & Technology, Warananagar, Affiliated to Shivaji University, Kolhapur, Maharashtra, INDIA

[2]Professor, Department of Electronics Engineering, Tatyasaheb Kore Institute of Engineering & Technology, Warananagar, Affiliated to Shivaji University, Kolhapur, Maharashtra, INDIA

[3]Assistant Professor, Department of Electronics Engineering, Tatyasaheb Kore Institute of Engineering & Technology, Warananagar, Affiliated to Shivaji University, Kolhapur, Maharashtra, INDIA

[1]Corresponding Author: mmsovani@gmail.com

ABSTRACT

The most important thing in this insecure world is the secrecy of everything. In today's world, any important data costs more than money. Steganography is the technique in which one can hide data as a secrete in selected image. In case of spatial domain, LSB approach is most popular in steganography, where all the LSBs of pixels of image are replaced by the bits of secret data. But the problem is that the secrete can be easily guessed by the hacker and the data is obtained by extracting it from direct LSBs. To make the system more robust and to improve the signal to noise ratio, the conventional LSB insertion method is replaced by inverted LSB technic. The decision to invert or not the LSB depends on combination of the 2nd and 3rd LSB. As not each and every LSB is inverted, it makes the steganalysis very difficult.

Keywords— Steganography, Least significant bit, Peak signal to noise ratio, Cover image, Steganalysis

I. INTRODUCTION

As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret message transmissions over the Internet system suffer from serious security overhead. So, protecting of secret messages during transmission becomes an important issue [1].

To protect your secret information from the strangers, it is necessary to convert the information into unrecognizable form. So various methods for information hiding like cryptography or steganography are used. This paper deals about one of the efficient methods to avoid detection of secret data by attackers. The paper gives efficient method for security using inverted LSB method based on steganography [2].

Steganography is the term used to describe the hiding of data in images to avoid detection by attackers. It is an emerging area which is used for secured data transmission over any public media. Steganography is the art of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

Steganography is a data hiding technique which conceals the existence of data in the medium. Steganography provides secrecy of text or images to prevent them from attackers. Image steganography embed the message in a cover image and changes its properties. Steganography provides secret communication so that intended hacker or attacker unable to sense the presence of message [3].

When we deal with steganography then mainly three things should be taken seriously.

1) The capacity -to hide the secrete message. This should be maximum.

2) Imperceptibility- It is the visual quality after hiding the data

3) Robustness.

The conventional LSB insertion technic is good if it is related only to imperceptibility but when it comes to the capacity, it is very low as we can hide 1 bit per pixel.

Also it is not robust as once it is detected that the image contains some hidden message, by retrieving only LSBs one can get the secrete data easily.

ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

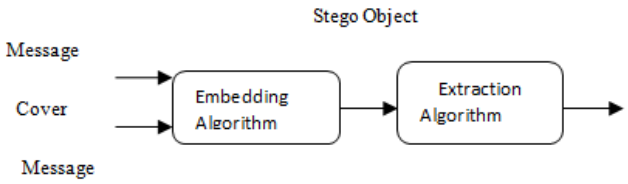


Fig. shows the model of steganography process.

1.1 Types of steganography:

1) Text Steganography: Digital files are not used very often because text files have a very small amount of redundant data.

2) Image Steganography: It is quite simple and secure way to transfer the information over the internet.

3) Audio/Video Steganography: It is very complex in use.

II. EXISTING METHODOLOGY

In the LSB replacement technic, it simply stores the Information in cover image directly by replcing a single bit of a pixel which does not cause perceptible difference in original image quality.

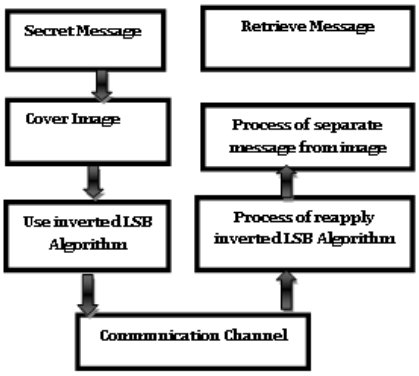
The disadvantages of LSB approach is the size of cover image required for a particular message image that is for a certain capacity of message, cover image required is 8 times .Thus it increases the bandwidth.

Another disadvantage is that if an attacker suspects that some information is hidden behind the cover image, He can easily extract information by just collecting LSBs of stego image. For these criteria, this method is not successful.

III. PROPOSED METHOD

To make the conventional LSB method more robust and to increase its hiding capacity, we are here with some changes in methodology. We will use color images as cover to increase the hiding capacity and we will change some LSBs depending upon some situations.

The proposed work is shown in block diagram 1. Proposed work is based on image processing with following steps.



Secret message –

The generation of secret message is always the first step in the workflow sequence. This is the data of user which is to be protected from the intruder. This message can be any data of prime importance that should be secured.

The cover image –

for hiding the secret message is obtained .This image can be of any form which should be converted to eight bit pixel format and the LSB of which is replaced with single bit of secrete message.

Inversion of LSB –

The secret bit embedded in cover image is not always kept as it is because if the hacker suspects about LSB insertion, he can retrieve the secret message easily. So one important change in this proposed method is that the LSB will be inverted depending on the combination of second and third LSBs.

With 2^{nd} and 3^{rd} LSB, there are total four combinations- 00, 01, 10, 11. Selecting one of these four, we will either invert the LSB or not. As all LSBs are not inverted, hence it may create confusion for the attacker about correctness of the retrieved message if he succeeds in hacking the message.

Retrieving message –

At the receiver side the intended recipient has the knowledge about the inverted bits. Hence upon receiving the data he can make separation of cover image and secrete message and with knowledge of inverted bits, he gains the original secret message without loss.

IV. RESULTS AND ANALYSIS

We use 3 cover images. Each image size is 800 * 600.

1) Taj

2) Sunset

3) Roses

and 3 secrete messages.

1. It is better to see something once, than to hear about it a thousand times. (Taj)
2. There is nothing more musical than a sunset.(sunset)
3. Be a rose which gives fragrance even to those who crush it. (Rose)

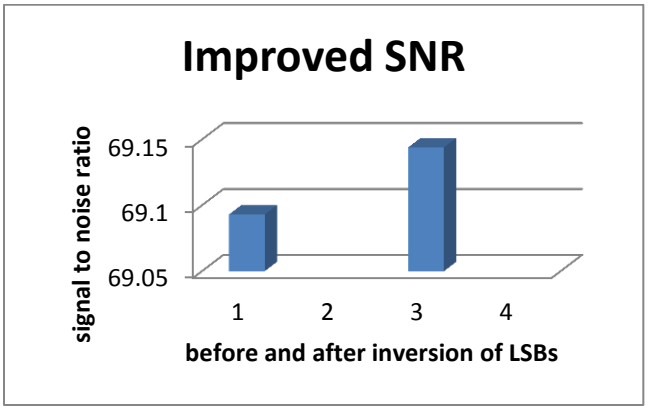
If we use different cover images and different message as a secrete data then let's check results.

The combination of 2nd and 3rd LSB can be 00,01,10,11. Out of these combination, we will choose the one for which the less number of bits are required to change. This will help us to fool the intruder with the help of Imperceptibility.

secrete message	cover image	Signal to noise ratio before inversion	Signal to noise ratio after inverstion	2nd /3rd bit combination
It is better to see something once, than to hear about it a thousand times.(Taj)	Taj Mahal	69.093	69.144	01
	roses	71.348	71.402	11
	sunset	62.492	62.498	01
Be a rose which gives fragrance even to those who crush it.(Rose)	Taj Mahal	69.117	69.154	10
	roses	71.39	71.431	11
	sunset	62.499	62.505	00
There is nothing more musical than a sunset. (sunset)	Taj Mahal	69.142	69.166	01
	roses	71.433	71.467	11
	sunset	62.503	62.507	00

For any of the combination of secrete message and the cover Image, we can find out the change in signal to noise ratio before and after inversion of LSB.

For example, if we consider the secrete message about Taj and the cover image is also Taj , then the signal to noise ratio changed can be shown with the help of a bar chart.



V. CONCLUSION

1. The proposed least significant bit inversion scheme enhances the stego-image quality. This is because not all the LSBs are changed, but depending upon the pair of 2nd and 3rd LSB, some of the LSBs are changed .This helps in making confusion for the hacker.
2. Even though the intruder could determine if the mes sage bits are embedded using some staganalysis methods, he would have difficulty to recover it because some of the LSBs have been inverted; it will misguide the staganalysis process and make the message recovery difficult. The bit inversion method makes the steganography better by improving its security and image quality.
3. It improves the signal to noise ratio. The signal to noise ratio SNR will be increased because the modification in cover image is less and so the stego image will not diverge much from original cover image as compared to classical LSB method.

REFERENCES

[1] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, & Partha Pratim Sarkar. (2012). An image steganography technique using x-box mapping. *IEEE- International Conference on Advances in Engineering, Science and Management (ICAESM)*, 709-713.

[2] Nadeem Akhtar, Shahbaaz Khan, & Pragati Johri. (2014). An improved inverted LSB image steganography. *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 749-755.

[3] Mandar D. Khatavkar & Prof. A.S. Mali. (2016). A Image security with image steganography using DCT coefficient and encryption. *International Journal of Innovations in Engineering Research and Technology, 3*(9), 1-8.

[4] Hemang A. Prajapati & Dr. Nehal G. Chitaliya. (2015). Secured and robust dual image steganography:A survey.

International Journal of Innovative Research in Computer and Communication Engineering, *3*(1), 30-37.

[5] Zhenhao Zhu, Tao Zhang, & Baoji Wan. (2013). A special detector for the edge adaptive image steganography based on LSB matching revisited. *10th IEEE International Conference on Control and Automation (ICCA) Hangzhou, China*, 1363-1366.

[6] Jatinder Kaur & Ira Gabba. (2013 August). Steganography using RSA algorithm. *International Journal of Innovative Technology and Exploring Engineering*, *3*(3), 75-79.

[7] Miss Sonali V.Nemade & Prof. A.S. Mali. (2016). A review of automatic detection of micro aneurysm and diabetic retinopathy grading in fundus retinal images. *International Journal of Research Publication in Engineering and Technology*, *2*(4), 1-3.

[8] Weiqi Luo, Fangjun Huang, & Jiwu Huang. (2010 June). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security*, *5*(2), 201-214.

[9] Swati Tiwari & R.P.Mahajan. (2012). A secure image based steganographic model using RSA algorithm and LSB insertion for increased robustness. *International Journal of Electronics Communication and Computer Engineering*, *3*(1), 7-85.

[10] Manjunath N & S.G. Hiremath. (2015). Image and text steganography based on RSA and chaos cryptography algorithm with hash LSB technique for more security. *International Journal of Electrical, Electronics and Computer Systems*, *3*(5), 5-9.

[11] Dr. M.Umamaheswari, Prof. S.Sivasubramanian, & S.Pandiarajan. (2010 August). Analysis of different steganographic algorithms for secured data hiding. *International Journal of Computer Science and Network Security*, *10*(8), 154-160.

[12] R.Chandramouli & Nasir Memon. (2001). Analysis of LSB based image steganography techniques. *IEEE International Conference on Image Processing (ICIP) - Thessaloniki, Greece*, 1019-1022.