International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Data Hiding in Digital Image Using Steganography

Prajakta Sune[1], Asmita Rathod[2], Shantanu Tatte[3], Dushyant Mankar[4]

[1,2,3]Department of Electronics and Telecommunication Engineering
Prof Ram Meghe College of Engineering & Management, Badnera.
[4]Assistant Professor of Electronics and Telecommunication Engineering
Prof Ram Meghe College of Engineering & Management , Maharashtra, India

---

Abstract - *In this paper we have used a process to increase security of hidden data in Images and prevent data extraction. We will encrypt data by use data hiding key and hide data by using LSB technique. In the LSB technique , the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. It is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced , hence LSB-based technique is the most challenging one . By using the LSB technique , the chance of getting attacked by the attacker is reduced. Many different file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret data in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.*

keywords- Stego image , LSB, PSNR, SNR ,etc

1.Introduction

Steganography is the art of hiding information such that prevent the detection of hidden messages. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications etc. Steganography hides the message so that it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an —invisible message created with steganographic methods will not. In this article we discuss image files and how to hide information in them using LSB technique , and we discuss results obtained from evaluating available steganographic software. Steganography is the method of unobservable communication. This is practiced through hiding data in image. In Steganography, we use carriers to conceal the data. The carriers may be image, audio, text, video, etc. The confidential information is reserved in some carrier and then transported. Steganography can be applied in numerous regions.

1.1 Image Definition

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Grayscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour.

1.2. Embedding Data

Embedding data, which is to be hidden, into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the message—the information to be hidden. A message may be plain text, ciphertext, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a stego image. A stego-key (a type of password) may also be used to hide, then later decode, the message.

1.3 IMAGE STEGANOGRAPHY

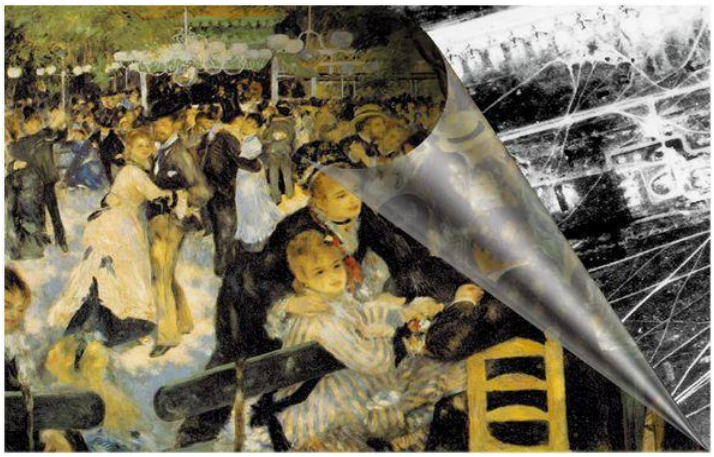

Fig -1.1: Data Hiding in Image

Image steganography Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthentic persons can only notice the transmission of an image but can't see the existence of the hidden message.

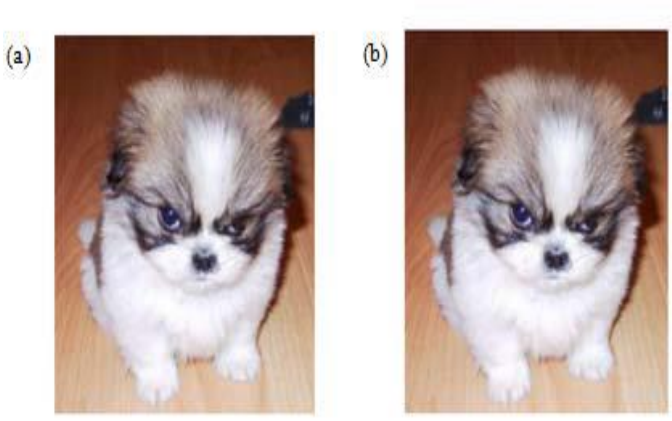

Fig.- 1.2 :(a) Original Image (b) Image containing data

2. STEGANOGRAPHIC FRAMEWORK

Any steganographic system can be studied as shown in Figure. For a steganographic algorithm having a stego-key, given any cover image the embedding process generates a stego image. The extraction process takes the stego image and using the shared key applies the inverse algorithm to extract the hidden message.

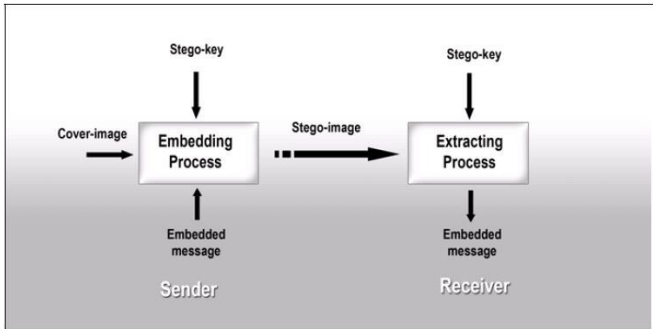

Fig 2.1: A generalized steganographic framework

2.1 LSB Algorithm For Encoding Data In Image

Step 1:Start

Step 2:Read cover image and message image & display them given as a input

Step 3:Analyse size of cover image and message image

Step 4:If size cover & message image is same then continue otherwise show error

Step 5:Make 0 to 3 LSB bit of cover image zero for each pixel of image

Step 6:Shift 4 to 7 MSB bit of message image towords its right for each pixel

Step 7:Add two Reconstructed image cover &message image

Step 8:Give name to the Addition image as Stego image

Step 9: End

2.2 LSB Algorithm For Decoding Data From Image

Step 1:start

Step 2:Read the stego image given as a input

Step 3:Make 0 to 3 LSB bit of stego image zero for each pixel of image

Step 4:From step 3we get cover image & display that image

Step 5:Shift 0 to 3 LSB bit of stego image towords left

Step 6:From step 5 we get message image & display that image

Step 7: End

2.3. OBJECTIVE

1. Increase security of hidden data in Image and Prevent data extraction. This can be done using LSB technique.

2. To hide the message or a secret data into an image which acts as a cover medium using LSB technique .

3. Implement proposed work in MATLAB.

3. CONCLUSION

In this paper we have used the LSB Technique on images to obtain secure stego-image. Our results indicate that the LSB insertion after encryption of Data for various size of images gives better results. The image resolution doesn't change much and is negligible when we embed the message into the image but image size will increase because of data hiding. So, it is not possible to damage the data by unauthorized personnel. Overall we can conclude that data security has been improved as attacker cannot extract encrypted Data.

3.1 ACKNOWLEDGEMENT

We offer our sincere and heartily thank, with deep sense of obligation to our mentors Mr. Dushyant V. Mankar for their priceless guidance, direction and inspiration to our system work without taking care of their comprehensive work. We are also thankful to the all faculty and technical staff of our college for taking personal interest in giving us constant support and timely suggestion.

3.2 REFERENCES

[1] N. F. Johnson, and S. Jajodia, ―Steganography: Seeing the Unseen‖, 1998, IEEE Computer.

[2]Piyush Goel, ―Data Hiding in Digital Images: A Steganographic Paradigm, 2008.

[3]Kshetrimayum Jenita Devi, ―A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique‖, 2013.

[4]A. Ker, —Steganalysis of Embedding in Two Least Significant Bits‖, 2007, IEEE Trans. on Information Forensics and Security.

[5] Xin Liao, —Embedding in Two Least Significant Bits with Wet Paper Coding‖

[6]Philip Bateman, —Image Steganography and Steganalysis‖, 2008.

[7]Hengfu YANG, —A High-Capacity Image Data Hiding Scheme Using LSB Substitution‖

[8]T. Morkel, —AN OVERVIEW OF IMAGE STEGANOGRAPHY‖

[9] J. K. Mandal, —Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images through Exclusion of Overflow/Underflow‖

[10] Rita Chhikara, —Concealing Encrypted Messages using DCT in JPEG Images‖