A Steganography Using Spatial Domain Method for Enhance Data Security

Hardik Lakhani
PG Student
Computer Engineering Department

Abstract : **Steganography is an art for hiding the secret information inside other information which are digitally cover. The another definition of steganography can also be given as study of unseen communication that usually deals with existence of communicated message. The hidden message can be text, audio, image or video accordingly to that it can be cover from either image or video. In steganography, hiding information achieved to insert a message into cover image which generates a stego image. In this paper, we have analyze various steganography methods and also covered classification and applications.**

Keywords **Steganography, Video, Image, LSB**

I. INTRODUCTION

Nowadays, rapid growth in the use of internet leading to many information to be shared and transferred through it. As long as there have been secrets there has been need for people to hide them. For hiding information, steganography is used since ancient times.[1] Steganography is original from Greek words Steganos means covered and Graptos means writing. It is the science and art of writing hidden messages, by which third party cannot recognizes that message which is existed.[2]

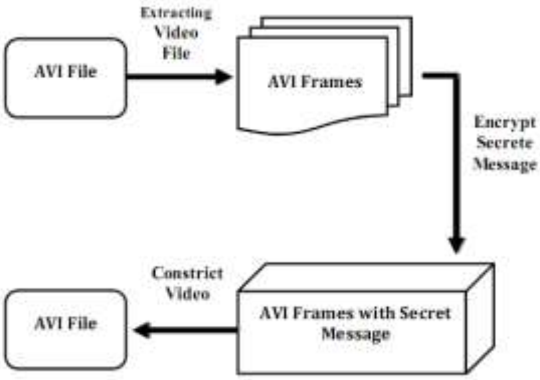


Fig 1:Video Steganography[3]

It is the science and art of writing hidden messages, by which third party cannot recognizes that message

Which is existed. Today's steganography system used multimedia objects like image audio video etc as cover media because people often convey digital

image over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information.

II STEGANOGAPHY IN DIGITAL MEDIUM

Depending on the type of the cover object there are many suitable stenographic techniques which are followed in order to obtain security.

Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and etc is used to achieve information hiding. [4]

Video Steganography: Video Steganography is a technique to conceal any kind of files or information into digital video format. Video (number of still images) is used as carrier for hidden information[4]. Generally discrete cosine transform (DCT) alter values which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats[10].

Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography. [4]

III STEGANOGRAPHY TECHNIQUES

Steganography techniques can be divided into following domains.

Frequency Domain Technique:

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it[9]. Frequency domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [5].

Frequency domain are broadly classified into[5]

- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).

Spatial Domain Methods:

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. All directly change some bits in the image pixel values in hiding data[11].

Spatial domain techniques are broadly classified into:

- Least significant bit(LSB)
- Pixel value differencing(PVD)
- Edge based data embedding method
- Random pixel embedding method

IV LEAST SIGNIFICANT BIT CONCEPT

Basically, the computer was created due to binary numbers, known as two numbers, namely 0 and 1. Both of these numbers are often referred to as bits. Then, these bits will continue to form a composite sequential and binary structure into a set of information. Set of information is composed of 8-bit or often referred to as 1 byte[12].

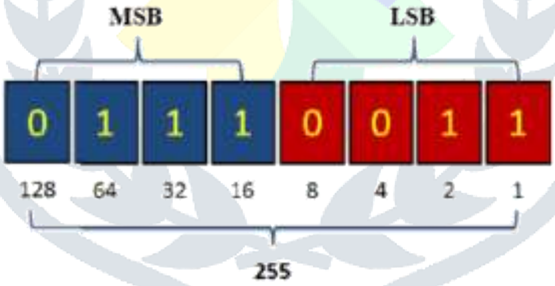


Figure 2: Binary representation [6]

Example

red green blue

Pixel value: (10110100, 11000101, 01010011)

Encoded Value: (10110101, 11000100, 01010011)

Message bit: 101

V LITERATURE REVIEW

In this paper [7] the proposed scheme video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken in to individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frame using sequential encoding of cover video[13]. To enhance more security of each bit of secret frames will be stored in cover frames will be stored in cover frames following a pattern BGRRGBGRB.

In this paper author [3] given two techniques one has random byte hiding. In this technique the information hiding in each line of video frame at the different place. If the line begins with the pixel value of ZZ the information is stored over the zz+ x location where x is a only known to a authorized receiver. While in another technique is least significant bit. In this technique, some predefined sequences are well known to sender and the receiver. Over this predefined location the secrete message is made hidden and this can be easily detected at the receiving side. This technique is something like private key techniques.

In paper "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images" author suggest a pixel indicator technique in this method they have first collect 3 MSB bit then check pixel indicator table. PIT is nothing but give a pattern to hide a secret message. This PIT table is given below.[8]

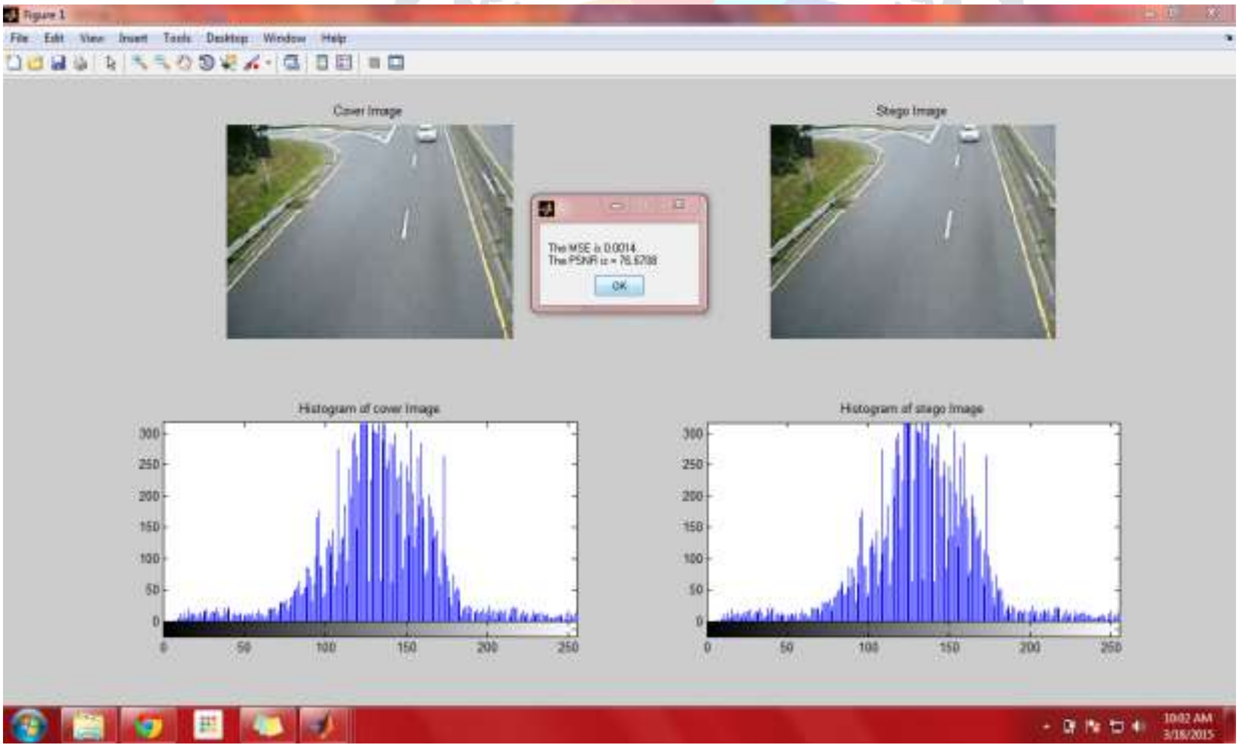
Table 1: Indicator Values [8]

MSB bits of Red, Green and Blue channel sequentially	**Sequence of channel's LSB bits where the message bits needs to be Hidden**
000	Red, Green and Blue (RGB)
001	Red, Green and Blue (RGB)
010	Red, Blue and Green (RBG)
011	Blue, Red and Green (BRG)
100	Blue, Green and Red (BGR)
101	Green, Red and Blue (GRB)
110	Green, Blue and Red (GBR)
111	Green, Blue and Red (GBR)

MSB bits of Red, Green and Blue channel sequentially Sequence of channel's LSB bits where the message bits needs to be hidden So in this table if MSB value is 000 it means add secret message in RGB channel in 1-LSB. If MSB bit is 100 it means adding value in BGR[8].

VI EXPERIMENTAL RESULT

A 24 bit image namely rhinos.png as shown fig was used as the cover image. The outputs of the program run were remarkably similar to the original images. The histograms are shown in fig. it is seen that the proposed sterilization technique does not detectably distort the histogram of the cover image.



The MSE is 0.0014
The PSNR is = 76.6708

Figure 3: The input (left) and the corresponding output (right) of the program using the proposed technique for hiding data.

- **Evaluation of image quality**

For comparing Stego images with cover results it requires a measure of image quality. Commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and histogram.

1) *Mean Square Error (MSE):* The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error loss. The mean square error (MSE) between two images A(x,y) and B(x,y) is:

$$\text{MSE}= \sum_{i-1}^{x}\sum_{j=1}^{y}\frac{([A_{ij}-B_{ij}])2}{x*y}$$

Where, x and y are width and height of image

2) *Peak Signal-to-Noise Ratio (PSNR):* As a performance measurement for image distortion , the well-known peak-signal-noise ratio (PSNR) which is classified under the difference distortion metrices can be applied on the stego images. It is defined as:

$$\textbf{PSNR=10log}\boldsymbol{log_{10}}\ (\frac{\boldsymbol{C_{max}^{2}}}{\boldsymbol{MSE}})$$

Where, C_{max}^{2} holds the maximum value in the image, here

$$C_{max}^{2} \leq \{\begin{array}{l}\text{1 in double precision intensity images}\\ \text{255 in 8—bit unsigned integer intensity images}\end{array}$$

Cover Image	MSE	PSNR
Frame 1	0.054	74.39
Frame 2	0.163	75.53
Frame 3	0.002	60.65
Frame 4	0.150	72.11
Frame 5	0.100	73.55

CONCLUSION

This paper gave an overview of different stenographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. We have analyzed different proposed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods.

In future strategy we can collect MSB bit values in RGB channel for calculating lighter & darker pixel values in a given image. Then we can hide extra bit into those pixel value for information hiding

ACKNOWLEGEMENT

I take this great opportunity to express my gratitude and ineptness towards my esteemed guide Prof. Aspriha Das, , Department of Information & Technology, B. H. Gardi College of Engineering & Technology – Rajkot, for her constant encouragement, continuous support, valuable suggestion and timely advice, without whom my work would not have been a success. We are short of words to thank her for her unlimited patience and her affection bestowed upon me during my entire work.

REFERENCES

[1]h.wang,"cyber warfare:steganography vs steganalysis",communication of the ACM,vol 47,no. 10,2004.
[2]e.cole and r.d.krutz,hiding in plain sight:steganography and the art of convert communication,wiley publication,inc,isbn 0-471-44449-9,2003
[3] Ashish T. Bhole, Rachna Patel,Steganography over Video File using Random Byte Hiding and LSB Technique ,IEEE Publication,2012
[4] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).
[5] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, (2000), pp. 43-78.
[6]Jasril, Ismail Marzuki, and Faisal Rahmat, "Modification Four Bits of Uncompressed Steganography using Least Significant Bit (LSB) Method" ICACSIS 2012
[7]Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, "A secure video steganography with encryption based on LSB techniques"IEEE international conferance on computational intelligence and computing reserch,2013
[8]Ankit Chaudhar, J. Vasavada1, J.L. Raheja2, S. Kumar, M. Sharma "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images" The 22nd International Conference on Computer Graphics and Vision, Russia, Moscow, October 01- 05, 2012
[9] Pratap Chandra Mandal," Modern Steganographic technique: A survey", International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 3 No. 9 Sep 2012

[10] Jasleen Kour, Deepankar Verma, “Steganography Techniques –A Review Paper” International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) May 2014

[11] Alphy Ros Mathew, Sreekumar K, “A Study on Different JPEG Steganograhic Schemes” International Journal of Computer Science and Information Technologies, Vol. 5 (6), 7870-7874 , 2014

[12] Jasril, Ismail Marzuki, Faisal Rahmat “Capacity enhancement of messages concealment in image and audio steganography” International journal on smart sensing and intelligent system vol. 6, no. 5,December 2013

[13] Akansha Agrawal, Virendra Singh “Securing Video Data: A Critical Review” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014