Rahul Joshi, Lokesh Gagnani / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1291-1294

Improve Security & Quality of Stego Image Using Proposed LSB Method

Rahul Joshi[1], Lokesh Gagnani[2]
[1] *PG Student,KIRC,Kalol*
[2] *Asst Prof,KIRC (I.T Department),Kalol*

Abstract

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information.In this paper proposed method focus on improving quality of stego image by increasing value of PSNR and SNR with less number of LSB changed compare to simple LSB method result in better security. This paper also compares results of proposed method with simple LSB.

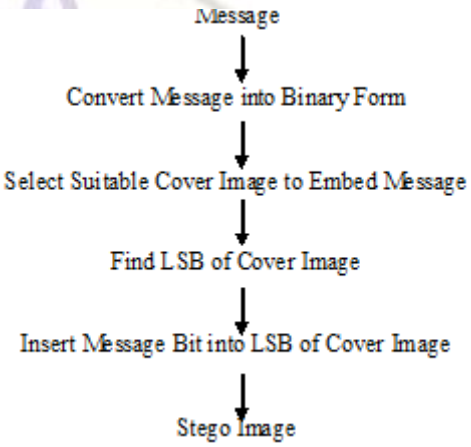
I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" [1] defining it as "covered writing". In image steganography the information is hidden exclusively in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [2]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [2]. The strength of steganography can thus be amplified by combining it with cryptography. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [3], forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [4].

Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

II. SIMPLE LSB METHOD

Algorithm



The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may be like this:

00100101 11101011 11001010 00100011
11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become:

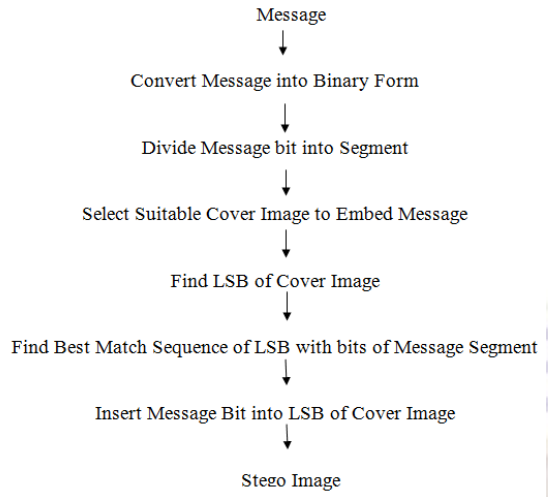
00100100 11101011 11001011 00100010
11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

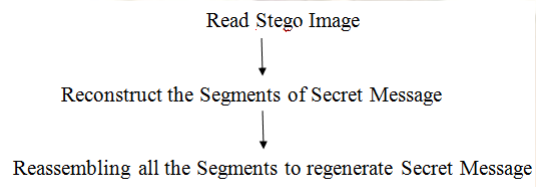
III PROPOSED LSB METHOD

Algorithm-Hiding Operation

.



Algorithm-Extracting Operation



In this method message bits divide into segment using proper segment length (like 2,4,8 etc). Create the segments in such a way that consist equal number of bits in each segment. Select suitable cover image enough to embed entire message. For testing purpose I use bmp type image of 8 bit depth. Store segments into one list called segment list. Find all lsb of cover image and store into one dimensional array called imagebits. Now find the best match sequence of lsb in one segment with sequence of imagebits. If match is found then replace that sequence of lsb with message bits of segment. If match is not found then insert message bits into lsbs without overlapping the sequence of lsb .Repeat this process for all segments.
Resultant image is called stego image. To extract message follow algorithm for extracting operation.

IV.EXPERIMENTAL PARAMETER

a) .Number of LSB changed
This parameter count the number of lsb changed. For better result value of this parameter keep as minimum as possible
b). **Time**
This parameter use to measure time required to hide message in image and also time required to retrieve message from image.
c). **Signal to Noise Ratio**
SNR is calculate using following equation

$$\mathrm{SNR} = 10 \cdot \log_{10} \left[\frac{\sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y)]^2}{\sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y) - t(x,y)]^2} \right]$$

Signal-to-noise ratio expressed in dB
d).Peak Signal to Noise Ratio
Peak signal-to-noise ratio expressed in dB

$$\mathrm{PSNR} = 10 \cdot \log_{10} \left[\frac{\max(r(x,y))^2}{\frac{1}{n_x \cdot n_y} \cdot \sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y) - t(x,y)]^2} \right]$$

PSNR is the standard measurement used in steganography technique in order to test the quality of the stego images. Higher the value of PSNR more the quality of the stego image.

V. EXPERIMENTAL RESULT

After implementation of Simple and Proposed LSB method for **lena.bmp and rocket.bmp** in Matlab (R2009a) following results are obtained. Here both images have 8 bit depth.

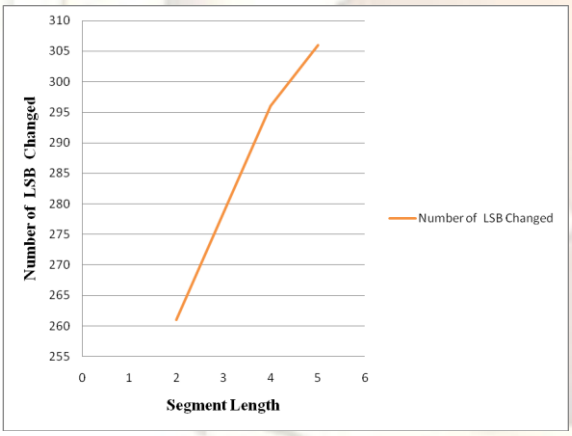
Following Table shows the result of both methods for **lena.bmp**

	Simple LSB Method	LSB With Message Segmentation		
Segment Length	------	2	4	5
Image	lena.bmp	lena.bmp	lena.bmp	lena.bmp
Image Size	256 x 256	256x256	256x256	256x256
Message(number of char)	100	100	100	100
Number of LSB Changed	418	261	296	306
SNR of Stego Image(db)	64.3985	66.4426	65.8961	65.7518
PSNR of Stego Image(db)	69.3744	71.3827	70.8362	70.6919
Time (Hide) seconds	0.000027	0.026270	0.013574	0.012909
Time (Extract) seconds	0.207298	0.209317	0.223182	0.219487

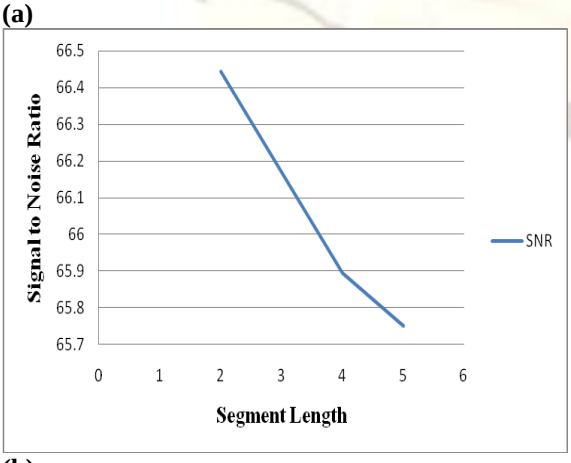
Following Table shows the result of both methods for **rocket.bmp**

	Simple LSB Method	LSB With Message Segmentation		
Segment Length	------	2	4	5
Image	rocket.bmp	rocket.bmp	rocket.bmp	rocket.bmp
Image Size	256 x 256	256 x 256	256 x256	256 x256
Message(number of char)	100	100	100	100
Number of LSB Changed	404	238	291	293
SNR of Stego Image(db)	54.0052	56.3018	55.4286	55.3989
PSNR of Stego Image(db)	70.2318	72.5298	71.6567	71.6269
Time (Hide) seconds	0.000028	0.024234	0.013286	0.010906
Time (Extract) seconds	0.213516	0.214853	0.218408	0.220135

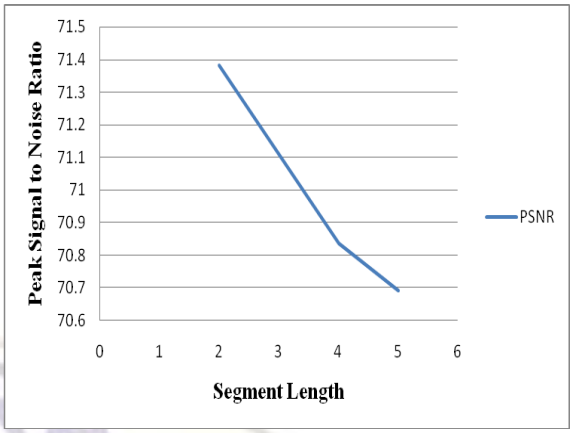
Following Figures (a to d) Shows the effect of segment length on various parameters for **lena.bmp**



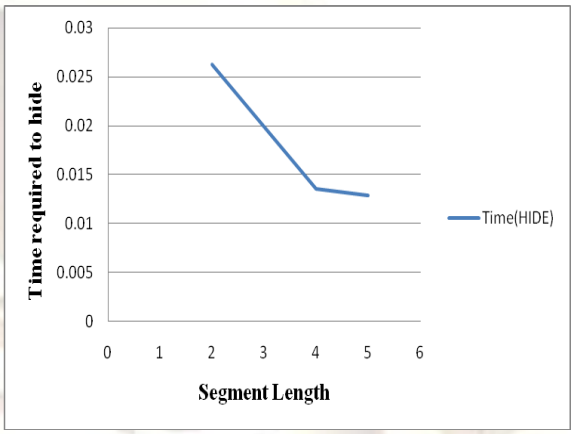
(a)



(b)

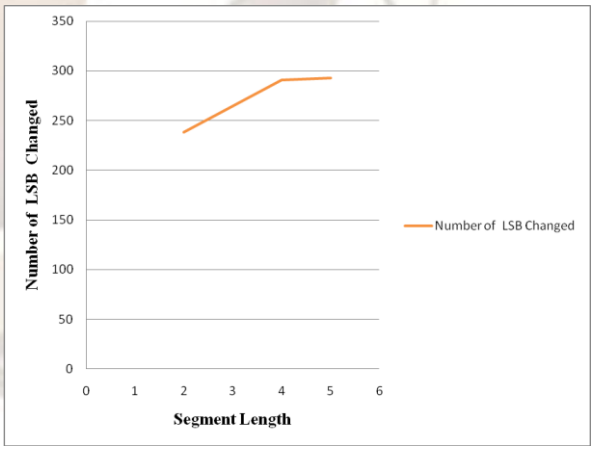


(c)

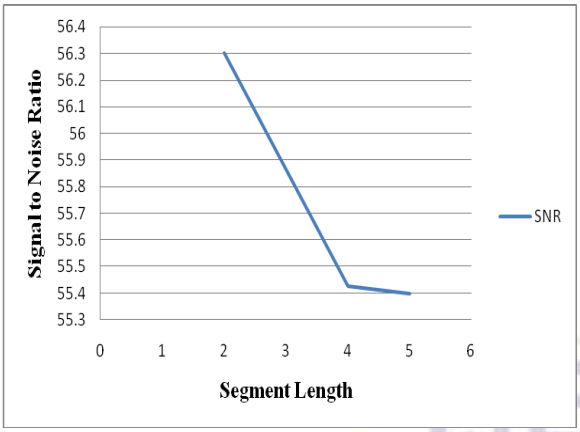


(d)

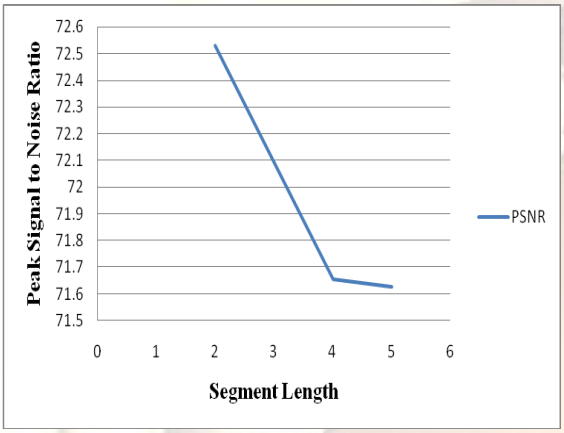
Following Figures (e to h) shows the effect of segment length on various parameters for **rocket.bmp**



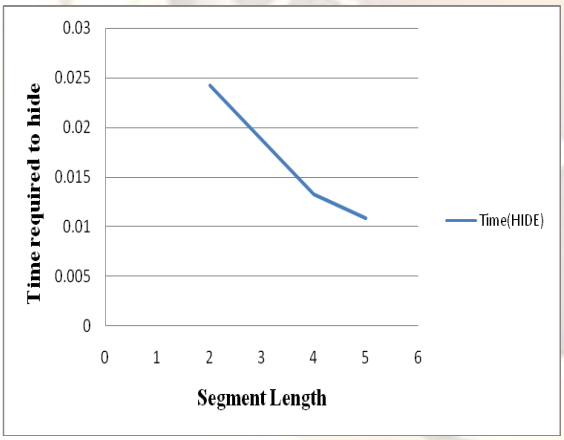
(e)



(f)



(g)



(h)

Figure (a,e) shows the effect of segment length (for 2,4,5) on number of LSB changed. As length of segment is increase number of LSB changed also increase because probability of finding match sequence is decrease as length of segment is increase.

Figure (b,f) shows the effect of segment length (for 2,4,5) on SNR. As length of segment is increase value of SNR is decrease due to number of LSB changed increase. This is also true for rocket.bmp

Figure (c,g) shows the effect of segment length (for 2,4,5) on PSNR. As length of segment is increase value of PSNR is decrease due to number of LSB changed increase.

Figure (d,h) shows the effect of segment length (for 2,4,5) on Time required to hide message in image. As length of segment is increase time required to hide message is decrease because number of segments is decrease .so time spend to search match sequence is also reduced.

VI CONCLUTION

The main purpose of this method is to decrease the number of LSB that are changed and as a result increase the immunity of the stego-image against the attack by human visual system (HVS). The problem of the proposed LSB Method is time required to hiding message that is spend during the search to find the best matching when using a large size stego-image. Implementation of this method for Audio and Video Steganography will considered as a future work.

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf

[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004

[3] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002

[4] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001