International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 5,May 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Enhanced LSB algorithm for Color Image

Salony Pandey[1],Vinay Harsora[2]

[1] PG Student,RKU,Rajkot
[2] Asst Prof,RKU, Rajkot

Abstract: Steganography is the art of hiding the scenario that communication taking place. Steganography is been used since ancient times. But the method used for steganography is changing day by day. There are many algorithm used for steganography, the paper discusses the new method for steganography, which can be used to have secure communication.

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. BASIC LEAST SIGNIFICANT BITS METHOD

Current trends favour using digital image files as the cover file to hide another digital file that contains the secret message or information. One of the most common methods of implementation is Least Significant Bit Insertion, in which the least significant bit of every byte is altered to form the bitstring representing the embedded file. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. While this technique works well for 24-bit color image files, steganography has not been as successful when using an 8-bit color image file, due to limitations in color variations and the use of a colormap [11].The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

A: 01000001

@IJAERD-2014, All rights Reserved

Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used

III ISSUES IN LSB METHOD

- If Intruder Changes LSB of Every Pixel in Stego Image then message will be lost.
- If data hiding capacity is increased by using two, three, four bit Stego method then quality of image degrades.
- If Number of LSB change are high then value of PSNR decreases thus quality of image also decreases.
- If attacker performs different image operation such as image crop, image compression, image rotation on stego image then it affects retrieval of message from image

.

- Time required hiding and time required to retrieve message is also important issue in some algorithm.
- Selection of cover image is also important issue and selection depends upon length of message and requirement of application.

IV ENHANCED LSB METHOD

Following Proposed Method overcome some above mention issues. This method implemented on 24bit color image. This method measures value of PSNR, Number of LSB Changed, and Time. Results also compare with Simple LSB method. Steps of proposed method are as follow:

- Select proper cover image.
- Enter message which is to be embedded into cover image.
- Enter the key to encrypt message.
- Find the message length of encrypted message.
- Convert the encrypted message into binary form.
- Divide the message into equal bits.
- Find the LSB considering RGB components from cover image.
- Find the match sequence of LSB bits and Segmented message.
- If match is found replace that LSB bits with message bits else embed message bits into sequence

Hiding Operation

Step1: Find following data required for hiding:

@IJAERD-2014, All rights Reserved

- Length of secret message (number of character)
- Segment Length (depends on length of message)
- Number of Segment K
- Find height and width of image

Step2: for i = 1: height
for j = 1 : width
Convert pixel into binary
j=j+1;
end
i=i+1;
end
Step3: while (n<= length of binary form of pixel)
Fetch LSB(8th bit of every pixel) from RGB Component
n=n+8;
end
Step4: while (v<=number of segment)
Find match of message segment with LSB bits
Location = strfind(LSBs , message segment);
if(match not found)
Store message segment into other location
else

Store message segment into location where match is found
end
end

Step5: for i = 1: number of segment
Store location in one file where segmented message is stored
end

Step6: Generate Stego image

Extracting Operation

Step1: Read Stego Image

Step2: for i = 1: height
for j = 1 : width
Convert pixel into binary
j=j+1;
end
i=i+1;
end

Step3: while (n <= length of binary form of pixel)
Fetch LSB (8^{th} bit of every pixel) from RGB Component

@IJAERD-2014, All rights Reserved

n=n+8;
end

Step4: Reconstruct Message using Stored Location
Load file
Step5: Read Message

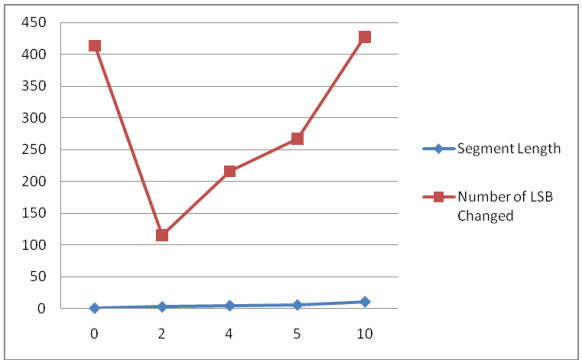
V DISCUSSION OF RESULT

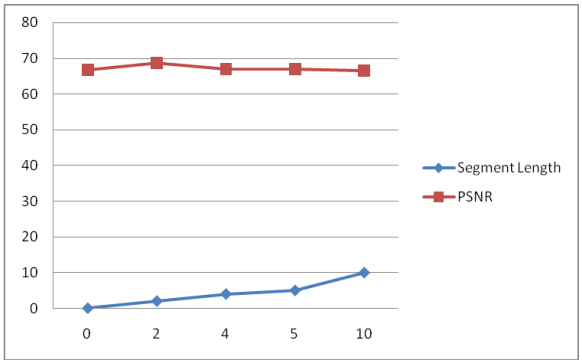
The image used for this algorithm is 100*100, 24 bit jpeg image. The algorithm can be used for any color image. But the size of image is directly proportional to time complexity.

	Simple LSB	Proposed LSB			
Message Size	100 Character				
Segment Length		2	4	5	10
PSNR	66.732	68.6207	66.9914	67.0137	66.5876
Time to hide	1.910615	26.94995	27.8798	25.60449	26.73813
No of LSB changed	414	115	216	267	428

The result shows that PSNR factor increases as compared to simple LSB algorithm. PSNR is used to measure quality of stego image. Also the proposed algorithm gives the best result for message segment length of 2, and as the segment length increases the number of LSB change also increases, because the probability of match found also decreases.

@IJAERD-2014, All rights Reserved





IV.CONCLUSION

Thus one can conclude that the proposed algorithm works for any image, but as the image size increases the time required also increases. But the quality of stego image and original image almost remains same. Thus human vision attack cannot detect changes made to the original image.

ACKNOWLEDGMENT

I am very thankful to my guide Prof. Vinay Harsora for giving me this opportunity to prepare this paper and Prof. Amit M. Lathigara for giving me such an opportunity.

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

[5]Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia"Application of LSB Based Steganographic Technique for 8-bit Color Images ," World Academy of Science, Engineering and Technology 50, 2009.

@IJAERD-2014, All rights Reserved