Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach

Manoj Kumar
CE Dept.
Yadawindera College of Engineering
Talwandi Sabo,151302, Punjab, India

Gursewak Singh
Research Scholar, CE Dept.
Yadawindera College of Engineering
Talwandi sabo, 151302, Punjab, India

ABSTRACT
Steganography plays a very imperative role in secret communication. Many possible techniques are used to embed confidential information in digital images, the least significant bit (LSB) technique has very widely used. In this paper the proposed technique ,a new steganography technique is being developed to hide data in image using pixel based algorithm. Also, to make the algorithm more undetectable data is divided into segments and image into blocks and a data segment is embedded into an image block where it effects. The least image quality. The experimental results prove that the quality of stego image using the proposed algorithm. For the verification of the results, peak signal-to noise (PSNR) and mean square error (MSE) are calculated.

Keywords
LSB; stego image; secret image; Arnold's transformation; identical bits

1. INTRODUCTION
Steganography is the process of concealing information in a carrier such as text, image, voice, video, or protocol. Digital images are one of the common and most popular ones due to their frequency on the Internet and high capacity of data transmission without degrading effect on images quality [1]. It is a high security technique for long data transmission. For many years it has been considered that security in cryptographic algorithms is directly related to the complexity of the mathematical operations that define the core of the encoding process. However, research using hardware-aided reverse engineering has continuously demonstrated that every cryptographic algorithm has a relatively short lifecycle, defined by the evolvement of computational power. A secure communication system is reliable as long as the cryptographic algorithm on top of which it was built is reliable [3].

In second section of this paper we have written related work to proposed technique and proposed work, experiment and results and conclusion are binded in sections 2, 3 and 4 respectively.

2. 2. LITERATURE REVIEW
Harpal et.al [1] proposed a new steganography techniques for the colored image. Their are many steganography techniques like LSB,DCT, pixel based etc, but these technique have many problems. To improved technique used 2-2-4 LSB insertion three plans images and get best results.

R.kumar et.al [3] proposed a new method based on parity of the pixel in odd and even case. First of all message is encrypted by vernam cipher algorithm and apply LSB-S method of pixel and XOR operation, after this store the results and verify on different parameters to good results.

M.devi et al [3] proposed a new method based on parity of the pixel in odd and even case. Firs**t** of all message is encrypted by vernam cipher algorithm and apply LSB-S method of pixel and XOR operation, after this store the results and verify on different parameters to good results.

3. PROPOSED WORK
In this section algorithm and techniques are explained which are used to apply for good results. In this paper we used a newly and best technique which is based on pixel value. Technique is explain below.

2 bit-Identical
This method is used to hide the secret message and pixel of the image bits are analyzed one by one if identical value finding between the pixel then hide the secret message on those bits.

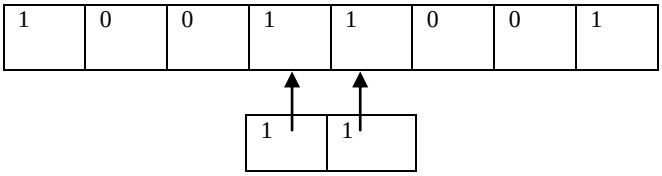


Fig 1. 2 bit Identical technique

Least significant bit technique
The most significant technique in steganography. It is used to hide the secret data in grey scale and colored images on its binary coding.fig 1.2 shows the LSB technique and shows the pixel of secret message bits. Algorithm shows the results by shifting right most two bits of LSBs of the pixel [1].

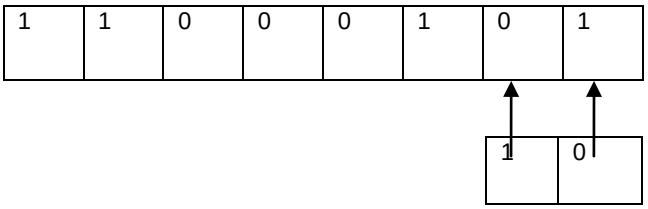


Fig 2. Least significant bit hiding technique

Entropy
There are many ways by which texture of digital image can be measured. Entropy is the most suitable way to measure the texture content of an image.Texture provides measure of properties of an image such as smoothness,coarseness and regularity.An image that is perfectly flat will have entropy of zero.The area of the image which have higher values of entropy are least visible to human because human eye is insensitive to these high entropy areas.Hence,if secrect image

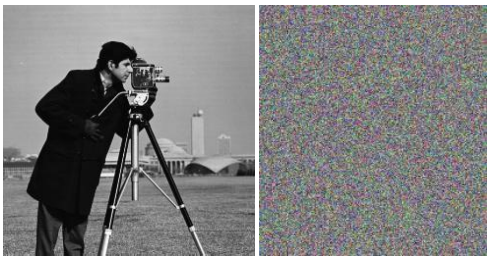
is embedded in high entropy areas of an image then higher imperceptibility can be obtained.Entropy can be defined as the statistical measure of randomness.

$$E = -\sum Plog_2(P) \qquad [1]$$

Where E is the entropy and P is the histogram count.

4. ARNOLD'S CAT MAP

Arnold's cat map (ACM) or Arnold transform (AT), proposed by Vladimir Arnold in 1960, is a chaotic map which when applied to a digital image randomizes the original organization of its pixels and the image becomes Imperceptible or noisy. However, it has a period p and if iterated p number of times, the original image reappears [11].



(a) **(b)**

(C)

Fig 3. (a) original secret image.(b)encrypted secret image.(c)decrypted image

In this figure shows that having original image encrypted with secret image apply ACM random iteration of 20 times which obtain an encrypted image. we can retrieve the original image by applying inverse Arnold'stransformation.

Table. 1 Steps of Hiding Process

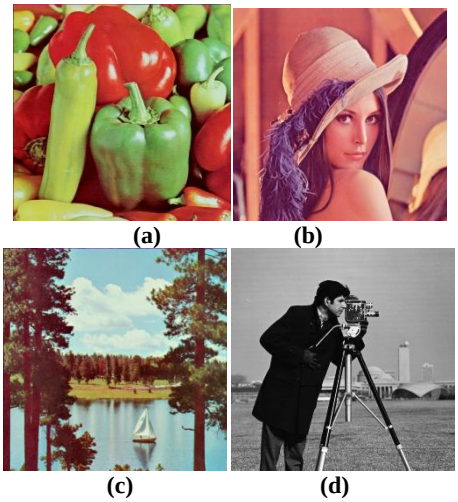
1	Read 256x256 color cover image.
2	Divide color image into 16 images into 64x64 bits.
3	Select four blocks of image to hide data.
4	Find RGB of each of four blocks.
5	Convert green component of each block into bits,64x64x8=32768.
6	Divide these bits into 4096 groups of 8 bits each.
7	Read 64x64 grey scale secret image and apply arnold's transformation to get an encrypted image
8	Convert encrypted image into bits 64x64x8=32768.
9	Divide these bits into 4 blocks having 8192 bits each then in these groups divide bits into 4096 groups of 2 bit each.
10	Select group of bits of block 1 we have choosen for hiding data and in first group of bits of secret image, apply proposed algorithm.(2-bit identical+LSB),save bit positions in an array(4 arrays for 4 blocks).
11	Repeat step 10 all of four blocks we have selected for hiding data.
12	Combine all of 16 blocks of image (12 blocks + 4 updated blocks).
13	Combine all of 16 blocks of image(12 blocks + 4 updated blocks).

Table. 2 Steps of Retreving process

1	First of all Read the stego image of 256x256 bits.
2	Divide the stego image into 16 blocks of each bits.
3	Then select 4 blocks from where we have already fixed.
4	Apply RGB on each of 4 blocks of bits.
5	Convert RGB's green componet of 64x64[1x8=32768
6	Divide each of the blocks with 8 bits which is =4096.
7	Repeat 5,6 step until for each 4 blocks.
8	Select first group and having an array that was defined in first embedding process.
9	Select position of bits from an array and extract at those positions from corresponding Blocks
10	Repeat the 8,9 steps each of 4 block.
11	After this combine those extracted bits to get encrypted secret image.
12	Apply ARNOLD'S inverse transformation, shows the extracted image.

5. EXPERIMENTAL RESULTS

The proposed technique has been implemented for cover image. With the help of this stego image has been evaluetad. For implementation we have several colored cover images of 256x256 pixel then divide into different blocks of each pixel of 64x64 total 16 blocks. Grey scale image of 64x64x8 bits. Then proposed scheme presented digital image that employ hybrid technique of 2-bit identical. PSNR Peak Signal Noise Ratio is used to measure the quality between cover image and stego image within size.



(a) (b)

(c) (d)

Fig 4. (a)Peeper (b) lena (c) lake (d) cameraman.

Peak Signal Noise Ratio

PSNR is used to measure the quality between cover image and stego image within size.

$$\text{PSNR} = 10.\log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right) \qquad [1]$$

In this formula I is the value of each pixel. Greater the value of PSNR better the quality of image.
MSE (Mean Square Error) also a parameter used to test the performance of proposed algorithm.

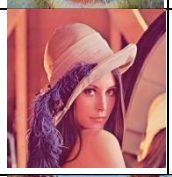
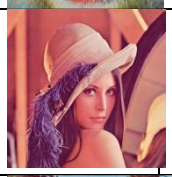
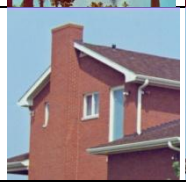
$$\text{MSE}= \frac{1}{\text{Min}}\sum_0^{m-1}\sum_0^{n-1}||f(i,j)-g(i,j)||^2 \quad [2]$$

where, M and N denotes the total number of pixels in the horizontal and vertical dimensions of an image. Xij represents the pixels in original image and Yij represent the pixels of stego image.

Imperceptibility

To measure the imperceptibility of proposed method. PSNR and MSE are calculated for different data bits.

Table 3 Results are shown in the table.

Images	Original image	Stego image	PSNR	MSE
Peeper			62.2661	0.0114
Babbon			61.6711	0.01163
lena			62.6708	0.0031
lake			61.6607	0.0211
home			61.9366	0.0147

The hiding capacity of proposed method is high up to 2bpp. Several images of 256 x 256 pixels are taken and data is hidden in these pixels. The total capacity of the proposed method is 131072 bits.

The capacity is calculated as given below:

capacity of 1 blocks = 64 x 64 x 2 =8192

capacity of 4 blocks =64 x 64 x 2 x 4 =32768

capacity of 16 blocks =64 x 64 x 2 x 16 =131,072

Total capacity =131,072.

6. CONCLUSION

In above proposed scheme using 2-bit identical approach with LSB, we have achieved PSNR value above 60 for different images shown in table which implies that our proposed scheme results in good perceptual quality of stego image. Arnold's transformation provides security by encrypting the secret image. For future work, it can be extended to be used with other techniques like DHT, DWT etc. Further it can be extended for video steganography**.**

7. FUTURESCOPE

At some point LSB seemed to be unbreakable but as natural images were better understood and newer models were created LSB gave way to new and more powerful algorithms which try to minimize changes to image statistics. But with further improvement in understanding of the statistical regularities and redundancies of natural images, most of these algorithms have also been successfully steganalysed. For future work, it can be extended to be used with other techniques like DHT, DWT etc. Further it can be extended for video Steganography.

8. ACKNOWLEDGMENTS

First of all, I am extremely grateful to my Research Guide, Er. Manoj Kumar, Assistant Professor, for his valuable guidance, scholarly inputs and consistent encouragement. A person with an amicable and positive disposition, Sir has always made his available to clarify my doubts despite his busy schedules and I consider it as a great opportunity to work on my thesis under his guidance.

9. REFERENCES

[1] A.singh, H.singh, "An Improved LSB based Image Steganography Technique for RGB Images," international confrence IEEE, vol.978-1-4799-6085-9/15/$31.00 ©2015 IEEE.

[2] M.devi, N.sharma, "Improved detection of LSB SteganographyAlgorithms in Color and Gray Scale Images," UIET Panjab University Chandigarh, vol. 978-1-4799-2291-8/14/$31.00 ©2014 IEEE.

[3] K.joshi, R.kumar, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", Third International Conference. Vol. 978-1-5090-0148-4/15/$31.00© 2015 IEEE .

[4] Shashikala Channalli, Ajay Jadhav , "Steganography An Art of Hiding Data", International Journal of Computer Science and Engineering.

[5] C.-K. Chan and L. Cheng, "Hiding data in images by simple {LSB}g substitution ," Pattern Recognition, vol. 37, no. 3, pp. 469 – 474, 2004.

[6] X. Qing., X. Jianquan and X. Yunhua., "A High Capacity Information Hiding Algorithm in Color Image.", Proceedings of 2nd International Conference on E-Business and Information System Security, IEEE Conference Publications, pp 1-4, 2010.