International Journal of Innovations in Scientific Engineering http://www.ijise.in

(IJISE) 2017, Vol. No. 5, Jan-Jun **e-ISSN: 2454-6402, p-ISSN: 2454-812X**

AN EFFECTIVE LSB TECHNIQUE OF COLORED IMAGESTEGANOGRAPHY

[1]Dr. Rajesh Kumar Pathak, [2]Neha Jain

1Professor &Director GNCT
Greater Noida, India.
2Assistant Professor
Dept. of CSE.GNIOT
Gr.Noida India.

ABSTRACT

In this paper we uses three layered approach which is helpful to hide large amount of message. Our approach provides a better way for embedding more secret data into cover image. This method makes the data embedding process to alter more LSBs of a pixel of RGB planes to increase the capacity of the steganography. It efficiently and effectively hides data with the help of a key in JPEG colored digital image. The proposed method makes the steganalysis harder by providing improved security and capacity to hide data. The security must be high so that any kind of attacks should not reveal secret information.

Keywords: Least Significant Bit (LSB), PSNR, MSE, Steganography.

INTRODUCTION

Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected.For comparing stego image withcover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity. [1]

1 Mean-Squared Error:

The mean-squared error (MSE) between two images I1 (m, n) and I2 (m, n) is[11]:

$$MSE= \sum M,N [I1 (m, n) \text{ and } I2 (m, n)]^{2}/M*N$$

M and *N* are the number of rows and columns in the input images, respectively.

2 Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the

image range [12]:

$PSNR = 10 \log_{10} (256^2/MSE)$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

3. Capacity:

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore, capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage [13].

4.Normalized Coefficient (NC):

Correlation is one of the best methods to evaluate the degree of closeness between the two functions. This measure can be used to determine the extent to which the original image and stego image remain close to each other, even after embedding the data.

5.Entropy:

It is a statistical measure of randomness that can be used to characterize the texture of the input image. It is given by:

$Entropy = -\ Pj\ Log\ Pj$

RESULT ANALYSIS

In this section, experimental results are discussed and presented for the evaluation of steganography robustness.[10]

Figure shows the five sample images which are used in the comparison. These are: “Lenna” (552120 bytes), “scene” (1440000 bytes), “green1” (337689 bytes), “bird” (605673) and “Lenna1” (921600).

The average PSNR and MSE values of test images versus LSB Steganography algorithm used in our experiments have been given in Table. The value of the PSNR, MSE and Correlation Coefficient are as shown in the Table. This algorithm is easy for detection/extraction.

For comparison with paper [1] we have taken the text hidden inside the Data Base Images is “hello how are uu my name is neha” (32 characters).In paper [1] the value of PSNR is **83.51** but in our algorithm the value of PSNR is **88.85**. The greater is the value of PSNR, the more will

be the image quality. Mean square error is used to measure the distortion in the image by performing byte by byte comparison between the original image and stegoimage.The value of Correlation coefficient is approximately equal to unity.

Table 3.1: Same image and same key but different messages[10]

Image name	Image size (bytes)	Message	Message size (characters)	key	Cover image entropy	Stego image entropy	Entropy (image-a)
bird	605673	Hide.txt	10452	8765432112345678765	6.3853	6.3840	.2003
bird	605673	Secret.txt	1050	8765432112345678765	6.3853	6.3853	.0311
bird	605673	Message.txt	518	8765432112345678765	6.3853	6.3853	.0170
scene	2152812	Hide.txt	10452	12345623	7.6434	7.6433	.0740
scene	2152812	Secret.txt	1050	12345623	7.6434	7.6434	.0106
scene	2152812	Message.txt	518	12345623	7.6434	7.6434	.0055
neha	2152812	Hide.txt	10452	675432187653423456	7.5236	7.5258	.0705
neha	2152812	Secret.txt	1050	675432187653423456	7.5236	7.5238	.0099
neha	2152812	Message.txt	518	675432187653423456	7.5236	7.5237	.0053

Table 3.2: Same message and same keybut different images[10]

Image name	Image size(bytes)	Message	Message size	key	Cover image entropy	Stego image entropy	Entropy
deer	605673	Hide.txt	10452	65432714325	7.4613	7.4593	.2004
neha	2152812	Hide.txt	10452	65432714325	7.5236	7.5258	.0708
koala	2359296	Hide.txt	10452	65432714325	7.8364	7.8367	.0669
scene	2152812	Hide.txt	10452	65432714325	7.6434	7.6433	.0736
bird	605673	Secret.txt	1050	2345615432	6.3853	6.3853	.0306
green	2359296	Secret.txt	1050	2345615432	7.0202	7.0203	.0109

Table 3.3 Same image and same message but different keys[10]

Image name	Image size(bytes)	Message	Message size	key	Cover image entropy	Stego image entropy	Entropy
koala	2359296	Hide.txt	10452	872345167543278	7.8364	7.8367	.0671
koala	2359296	Hide.txt	10452	12342378	7.8364	7.8367	.0673
Deer	605673	Secret.txt	1050	45678321436754321	7.4613	7.4612	.0307
Deer	605673	Secret.txt	1050	654321784	7.4613	7.4612	.0310
green	2359296	Message.txt	518	321445678432567	7.0202	7.0202	.0057
green	2359296	Message.txt	518	5432178	7.0202	7.0202	.0058

Table 3.4 Performance Evalutation of LSB Based Steganography Algorithm[10].

Image name	Image size	Message size (characters)	PSNR	MSE	Correlation coefficient
Lenna	3145728	10452	66.58	2.1978e-07	1
scene	2152812	1050	74.77	3.3350e-08	1
Green1	1512900	32	88.85	1.3027e-09	1
bird	605673	518	72.25	5.9542e-08	1
Lenna1	921600	298	75.74	2.6666e-08	1

Figure3.1.Stego image

Figure 3.2: Cover image

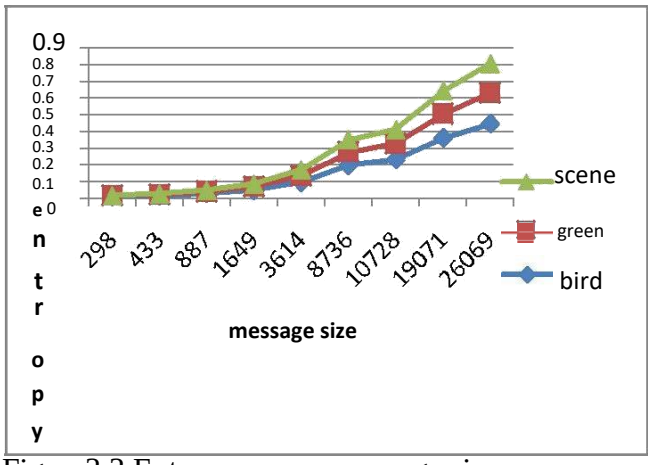

Figure3.3 Entropy versus message size

This figure shows that entropy increases as message size(characters) increased. In this figure we have taken 3 sample images. Sizes of images are in bytes scene(2152812), green(2359296), and bird(605673).

CONCLUSION

In this paper the improved LSB based steganography is used. It is observed that if PSNR ratio is high then images are of better quality. Both cover image and Stego image looks identical by applying our algorithm. The amount of secret data that can be hidden by using this technique is large as compared to other steganography algorithm. Increasing the capacity beyond certain level will create detectable distortion in the stego image. But detectable distortion is very less and capacity is more in our algorithm. We can improve the security further by using other statistics (rotations etc.) to change the LSB of cover image.

REFERENCES

1. StutiGoel, Arun Rana, Manpreet Kaur "ADCT-based Robust Methodology for Image Steganography"I.J. Image, Graphics and Signal Processing, pp. 23-34, 2013.
2. Se-Min Kim; Ziqiang Cheng; Kee-Young Yoo "A New Steganography Scheme Based on an Index-Color Image" Information Technology: New Generations, ITNG pp. 376 – 381, 2009.
3. Rui Miao; Yongfeng Huang "An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP" Communications (ICC) pp. 1-5, 2011.
4. Premkumar, S.; Narayanan, A.E. "New visual Steganography scheme for secure banking application" Computing, Electronics and Electrical Technologies (ICCEET) pp. 1013 – 1016, 2012.
5. HongmeiTang, GaochanJin, Cuixia Wu; Peijiao Song "A New Image Encryption and Steganography Scheme" Computer and Communications Security, ICCCS pp. 60-63, 2009.
6. Yongzhen Zheng, Fenlin Liu, Xiangyang Luo, Chunfang Yang "A Method Based on Feature Matching to Identify Steganography Software" Multimedia Information Networking and Security (MINES), pp. 989-994, 2012.
7. A.Gupta, S.Mahapatra and K.Singh "Data hiding in color image using cryptography with help of ASK algorithm" Emerging Trends in Networks and Computer Communications (ETNCC), pp. 15-17, 2011.
8. Akhtar, N.,Johri, P.,Khan, S. "Enhancing the Security and Quality of LSB Based Image

Steganography" Computational Intelligence and Communication Networks (CICN), pp. 385 – 390, 2013.

9. Rai, S.,Dubey, R. "A novel keyless algorithm for steganography" Engineering and Systems (SCES),pp. 1-4,2012.
10. Neha Jain; SudhirGoswami "An Improved Steganography Technique of LSB Substitution Method" International Journal Of Engineering And Computer Science ISSN:2319-7242, pp. 9912-9915, January 2015.
11. Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.
12. Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.
13. K.B.Shiva Kumar, K.B.Raja, R.K.Chhotaray, SabyasachiPattnaik, "Coherent Steganography using Segmentation and DCT", IEEE-978-1-4244-5967-4/10,2010.