International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Testing of Image Steganography with use of LSB and DCT Techniques

Gayatri G. Bobade, A. G. Patil

***Abstract:** In this growing internet world, secret data communication is increasing day by day. There are various methods to communicate secretly. Steganography is one of those techniques in which data is concealed within cover data such that it cannot get detected. Steganography is usually used today on pcs where digital data is the high-speed distribution channels for carriers and networks. Steganography is the skill of understanding of unnoticeable activity at intervals. Steganalysis is the science of concealed data detection. Steganography of data which is of any form like images, audio, video or text information is done by various techniques. Image steganography is done by various technique. Least Significant Bit (LSB) with XORing and Discrete Cosine Transform (DCT) are used to test the image steganography. Images are converted to grey scale to get better accuracy. Results are tested with mean square error (MSE) and peak signal-to-noise ratio (PSNR) values.*

***Keywords:** Least Significant Bit; Discrete Cosine Transform; Mean Square Error; Peak Signal-to-Noise Ratio; Secret Image; Cover Image; Stego Image.*

I. INTRODUCTION

Steganography is the knowledge of secret communication through a digital concealed media such as image files, audio files, video files or text files. Into cover image, a secret image can be embedded, this process is known as image steganography. Hiding the existence of secret image which is embedded in the cover image is the final intention of an image steganography. Image steganography is a prevailing tool that increases security in data transferring and archiving. In image steganography, the cover image is an image signal. The secret image data is embedded into image and form a new signal called as stego image. This stego image appears identical to cover image. Extraction of the secret image is done at the receiver side by applying extraction technique.

Hiding the meaning of the information is done by encryption while steganography hides the presence of the information. Hence steganography is favourable than encryption. The presence of a secret image reduces values of PSNR and rises MSE values of the stego image. We acclaim a method to upgrade PSNR and MSE values in stego images. On the secret image, a transformation is used by this technique, and then secret image is hide in cover image. The result of the transformation is verified by using LSB insertion and also DCT techniques. MSE and PSNR values are calculated for both techniques.

There are two domain techniques used for image steganography. One is spatial domain and other is transform domain technique. LSB technique is under spatial domain and DCT technique is under transform domain technique.

Manuscript published on 30 August 2019.
***Correspondence Author(s)**

Miss. Gayatri G. Bobade, Electronics and Telecommunication, BATU University, P.V.P.I.T, Budhgaon, Sangli, India.
Mr. A. G. Patil, Electronics and Telecommunication, BATU University, P.V.P.I.T, Budhgaon, Sangli, India.

II. LITERATURE REVIEW

A strategy to stego pictures to enhance PSNR as well as MSE standards is recommended. LSB and DCT methods study the impact of a conversion [2]. A document wherein the RGB picture method Least Significant Bit Steganography is displayed. It conceals RGB image in 3 planes of the color image since bit lane slicing in this way which minimal noise in stego image is induced with minimal change in the image's noticeable quality that could not be identified by bare eyes [7]. Some cryptographic and steganographic techniques are being used to accomplish the objective that providing safety for data or file during processing. Cryptographic techniques turn the initial message into a pre-transmission code signal, while the basic concept used in steganography is to conceal the message's presence in a file. This enables only the formal addressee as well as the recipient to recognize the presence of confidential information. A new clustering and noise-based method is suggested in this article to improve the safety of the concealed information. The above method suggested comprises of two stages. During the first stage, the cover image pixels are collected in to the separate clusters which used the k-means clustering algorithm accompanied by the method of encoding. But in all the clusters, a discrete noise is introduced within each pixel in the second stage. Observational findings are compared with current steganography methods, which demonstrates that the suggested algorithm achieves the same encoding ability and enriches the stego picture PSNR [6].

A steganographic method that used an enhanced LSB method for only a 24-bit colour picture able to produce a hidden inserted picture that is completely indistinguishable from human eye's actual picture. In accumulation, it document demonstrates why the enhanced 24-bit colour picture LSB method is enhanced compared to the 8-bit color picture LSB method. Observational findings indicate that throughout the situation of 24 bit, the stego image is visibly impossible to distinguish from the initial cover image [3].

Retrieval Number: J96590881019/19©BEIESP
DOI: 10.35940/ijitee.J9659.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

III. SOFTWARE DESIGN AND EXPERIMENTAL RESULTS

The aim of steganography is to conceal secret image without harming the cover image. This design of steganography technique is implemented in MATLAB. Image steganography can be implemented as follows:

1. Pre-processing: To convert RGB colour image into greyscale image.
2. Hiding secret image with use of XOR transformation and LSB technique as well as DCT technique.
3. Retrieve secret image successfully without harming cover image.
4. Calculating MSE and PSNR values for both the techniques.

Detailed information of above processes are given below:

1. Pre-processing:

Pre-processing is a common name for operations in image processing. The aim of pre-processing is an improvement of images that remove unwanted noise. Here both secret image and cover are converted to grey scale image as shown in below fig (1), (2), (3) and (4).

Fig (1): RGB cover image

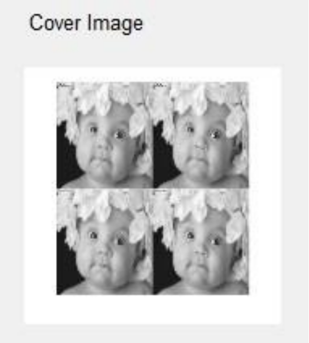


Fig (2): Greyscale cover image

Fig (3): RGB secret image

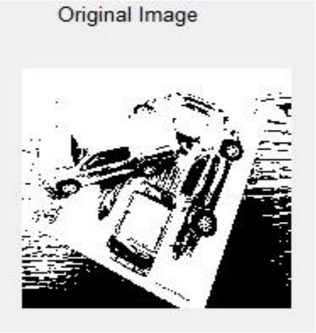


Fig (4): Greyscale secret image.

2. Hiding Secret Image:

After converting colour images to greyscale images, concealing secret image which contains sensitive information is done. There are many techniques used to hide secret image. Here, LSB with XOR as well as DCT techniques are used. LSB technique is based on bit of an image, hence, taking it into consideration, types of LSB hiding techniques are variable size technique and fixed size technique. Variable size technique is implanted when number of bits in every pixel are relies on contrast and luminance qualities. And fixed size technique is implanted when number of bits in secret image's pixel are same as those of cover image. For transforming eight by eight-pixel matrix of an image in to every 64 coefficients of JPEG image for every colour component, Discrete Cosine Transform (DCT) technique is used. The Exclusive-OR, XOR is logical operation for binary numbers. It's an important method of encoding. It's being used for loop codes while connecting to safe data centers, that are widely employed in internet browsers. Strong protection provided by this technique after using correctly. However, once the code is not being used correctly, this privacy is simply beaten. Below table is a truth table of XOR for 2 bits A & B. Let us assume that, A is a cover data bit and B is a bit of a key. The last column is result of XOR operation.

Table 1- Truth Table of Exclusive-OR (XOR)

A	B	⊕
0	0	0
0	1	1
1	0	1
1	1	0

When order of bits of A and B where B is a key is taken simultaneously then only message can be sent from A to B and only key i.e. B knows the arrangement of bits in it. XOR is used to combine message bits and bits of key for encoding purpose. Exchanging message from A to B, it is necessary to use various secret bits.

Secret image after applying XOR and cover image in which secret image is concealed which is called stego image with the use of LSB and DCT techniques are shown in below fig (5) and (6).

Fig (5): XOR secret image

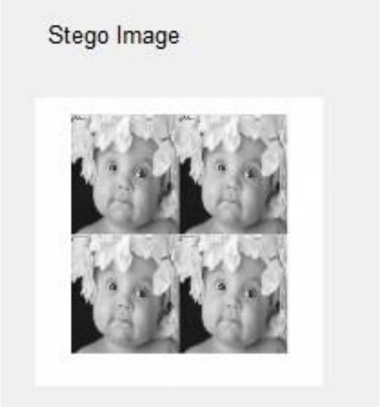


Fig (6): Stego image

3. Retrieving Secret Image:

Concealing secret image in cover image is done successfully. Then that stego image is transmitted to the desired location or area. At the receiver side, secret image is retrieved by removing LSB and DCT techniques. This retrieved image is shown in below fig (7).

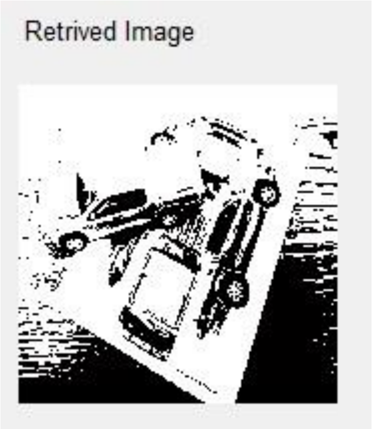


Fig (7): Retrieved Secret Image

Figure (2), (4), (6), (7) would appear in a single figure window of MATLAB as shown in below fig (8).

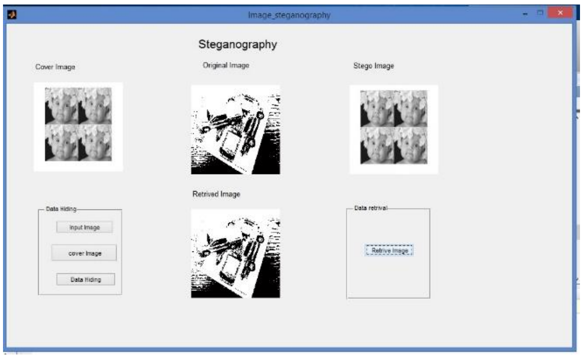


Fig (8): Image Steganography

4. MSE and PSNR Values :

MSE and PSNR are nothing but Mean Square Error and Peak Signal to Noise Ratio respectively. For checking superiority of stego image, these both parameters are used.

Mean Square Error is given by the following equation (1),

MSE=$\frac{1}{ab}\sum_{i=0}^{a-1}\sum_{j=0}^{b-1}[C(i,j)-S(i,j)]$^2 ……….(1)

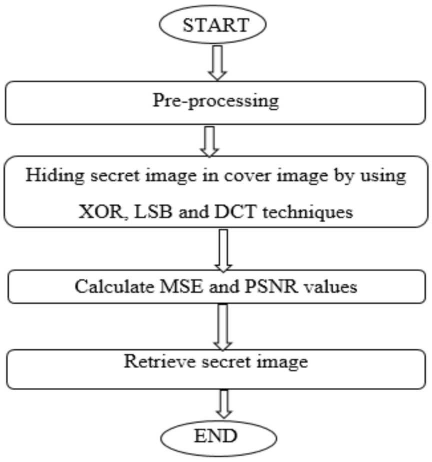
Where, C & S corresponds to pixel value of cover image and stego image respectively and a and b represent total number of rows and columns of the image matrix respectively.

Peak Signal to Noise Ratio is given in following equation (2).

PSNR=10$\log_{10}(\frac{C_{max}^2}{MSE})$ …………...... (2)

C_{max} corresponds to the maximum pixel value in the cover image.

Flowchart


START
Pre-processing
Hiding secret image in cover image by using XOR, LSB and DCT techniques
Calculate MSE and PSNR values
Retrieve secret image
END

IV. EXPERIMENTAL RESULTS

In image steganography by using LSB and DCT techniques, experimental results are tested with mean square error i.e. MSE and peak signal-to-noise ratio i.e. PSNR values. It says that, to get improved quality of stego image, Mean Square Error should be as less as possible and Peak Signal to Noise Ratio as high as possible.

Retrieval Number: J96590881019/19©BEIESP
DOI: 10.35940/ijitee.J9659.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Following table 1 & 2 shows the MSE & PSNR values for both the techniques.

Table 1 MSE & PSNR values for the LSB with XOR transformation technique

MSE	PSNR
1.0061	45.4773
1.0153	45.0639
1.0247	44.6501
1.0343	44.237
1.044	43.8236

Table 2 MSE & PSNR values for the DCT technique

MSE	PSNR
1.002	53.6593
1.0056	53.4684
1.0092	53.2774
1.0128	53.0864
1.0165	52.8955

V. CONCLUSION

From this implementation of image steganography using LSB and DCT techniques, conclusion is, for the technique LSB using XOR gave MSE and PSNR values which decreases as number of bits substituted are increases. For good quality of stego image, MSE should be low and PSNR should be high. This is achieved in both the techniques i.e. LSB and DCT. DCT method gives better performance than LSB technique. Only the two distinct transformations were limited to this research. Furthermore, to discover some other form transformation that causes stronger efficiency, further study is needed.

REFERENCES

1. Bobade G. G. and Patil A. G., "Review: Transformation of the Steganography Image Process", International Journal of Research and Analytical Reviews (IJRAR) ISSN: 2349-5138, Volume-06, Issue-02, May-2019.
2. Mohamed Buker; Hakan Tora; Erhan Gokcay, "Effect of Secret Image Transformation on the Steganography Process," 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 351-355,2017.
3. Deepesh Rawat and Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Technique for 24 Bit Colour Image'', International Journal of Computer Applications (0975-8887) Volume 64- No.20, February 2013.
4. Sheidaee, A., & Farzinvash, L., "A novel image steganography technique based on DCT and LSB," 9th International Conference on Information and Knowledge Technology (IKT), 2017.
5. Ms. G. S. Sravanti, Mrs. B. Sunitha Devi, S.M.Riyazoddin & M. Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plan Bit Substitution Technique", Global Journal of Computer Science and Technology Graphics & Vision Volume 12 Issue 15 Version 1.0 , 2012.
6. A.SaiKrishna Shankar Parimi G. Manikandan. Sairam. N, "A Clustering Based Steganographic Approach for Secure Data Communication", International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015.
7. Singh, A., & Singh, H., "An improved LSB based image steganography technique for RGB images". IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) 2015.

AUTHORS PROFILE

First Author: Miss. Gayatri G. Bobade **Education:** M.Tech II E&TC (appearing) **Publications:** International Journal of Research and AnalyticalReviews (ISSN: 2349-5138)
Second Author: Mr. A. G. Patil

Education: ME Electronics **Designation:** Associate Professor **Publications:** National Journal/Conference- 08 International Journal/conference- 20 **Membership of Professional societies:** ISTE (LM-13649)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)