iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VII **Month of publication:** July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7071

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Effect of Secret Image Transformation on the Steganography Process by using LSB & DCT Techniques

Miss. Gayatri Ganesh Bobade[1], Prof. A. G. Patil [2]
[1]*PG Student,* [2]*Dept. of Electronics & Telecommunications Engineering in P.V.P.I.T Budhgaon*

Abstract: ***Steganography is the art of hiding information in something else. It is favourable over encryption because encryption only hides the meaning of the information; whereas steganography hides the existence of the information. The existence of a hidden image decreases Peak Signal to Noise Ratio (PSNR) and increases***
Mean Square Error (MSE) values of the stego image. We propose an approach to improve PSNR and MSE values in stego images. In this method a transformation is applied to the secret image, concealed within another image, before embedding into the cover image. The effect of the transformation is tested with Least Significant Bit (LSB) insertion and Discrete Cosine Transformation (DCT) techniques. MSE and PSNR are calculated for both techniques with and without transformation. Results show a better MSE and PSNR values when a transformation is applied for LSB technique but no significant difference was shown in DCT technique. Keywords— least significant bit-LSB; discrete cosine transformation-DCT; steganography.

I. INTRODUCTION

Steganography is the technology of secret communication via a digital cover media such as image, audio or video, text files. Embedding secret image into image is known as image steganography. The ultimate goal of an image steganography is to conceal the presence of secret image embedded in the cover media. Image steganography is a powerful tool which increases security in data transferring and archiving. In image steganography, the image signal is called as cover image. The secret image data is embedded into image and form a new signal called as stego image. This image looks same as cover image. At the receiver side, the secret image is extracted from this stego image using extraction method.

It is favourable over encryption because encryption only hides the meaning of the information; whereas steganography hides the existence of the information. The existence of a hidden image decreases Peak Signal to Noise Ratio (PSNR) and increases Mean Square Error (MSE) values of the stego image. We propose an approach to improve PSNR and MSE values in stego images. In this method a transformation is applied to the secret image, concealed within another image, before embedding into the cover image. The effect of the transformation is tested with Least Significant Bit (LSB) insertion and Discrete Cosine Transformation (DCT) techniques. MSE and PSNR are calculated for both techniques with and without transformation.

There are three main issues in designing an image steganography method: undetectability, imperceptibility, and capacity.

1) Undetectability ensures that the stego, containing the secret data, is indistinguishable from the original image.
2) Imperceptibility means the hidden data insertion process makes distortion on the original image.
3) Capacity gives the relative amount of hidden data which can be inserted into the cover image.

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system.

In recent years, several methods have been developed for hiding secret image into the cover image. Some method is developed in the time domain like least significant bit (LSB) substitution, phase coding steganography. LSB substitution is one of the earliest techniques used for the secret image data embedding in audio signals and other media types. The phase coding steganography methods are other time domain image steganography schemes which hide secret data in the phase of the cover image. Transform domain image steganography methods are the ones in which various transform domains such as Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), and Discrete Wavelet transformation (DWT) are used to embed the secret image data in the coefficients of the cover image.

The goal of this work is to present an image steganography method which is less detectable, so more secure than existing popular methods.

II. LITERATURE REVIEW

Mohamed Buker., et al. [1] proposed an approach to improve PSNR and MSE values in stego images. The effect of the transformation is tested with Least Significant Bit (LSB) insertion and Discrete Cosine Transformation (DCT) techniques.

Soni, A., et al. [2] illustrated the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The simulation result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key i.e. order parameter of this transform.

Deepesh Rawat et al. [3] have proposed a steganographic technique by using improved LSB (least significant bit) replacement method for 24-bit colour image capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. In addition, this paper shows that how improved LSB method for 24-bit colour image is better than LSB technique for 8 bit colour image. Experimental results show that the stego-image is visually indistinguishable from the original cover-image in the case of 24 bit.

Ms.G.S.Sravanthi, et al. [4] have proposed a new method of information hiding in digital image in spatial domain. This method uses Plane Bit Substitution Method (PBSM) technique in which message bits are embedded into the pixel value(s) of an image. These experimental techniques are sufficient to discriminate analysis of stego and cover image as each pixel based PBSM and operand with LSB.

Masou d Nosrati, et al. [5] have proposed a system which is achieved by Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). This paper is based to design the enhanced secure algorithm which uses both steganography using Genetic Algorithm and Visual Cryptography to ensure improved security and reliability.

A. SaiKrishna et al. [6] stated, providing security for the message during transmission is a thought-provoking task. To accomplish this goal many cryptographic and steganographic algorithms are being used. Cryptographic algorithms transform the original message into a cipher text before transmission, whereas the basic idea used in Steganography is to hide the existence of the message in a media. This enables the existence of secret data to be known only to the authorized sender and the receiver. In this paper a new-fangled method based on clustering and noise addition is proposed to enhance the security of the hidden data. The proposed method consists of two steps. In the first step the pixels of the cover image are grouped into different clusters using k-means clustering algorithm which is followed by the embedding process. In the Second step a random noise is added to each pixel in all the clusters. Experimental results are compared with existing steganography techniques, which shows the proposed algorithm not only achieves same embedding capacity but also enhances the PSNR of the stego image.

Amritpal Singh et al. [7] proposed a paper in which, Least Significant Bit Steganography method for RGB image is presented. It hides RGB image into three planes of the colour image after bit lane slicing in such a way that induces minimum noise in stego image with the negligible change in the visible quality of the image which cannot be detected by naked eyes.

Lee Y. K. et al. [8] introduced an image steganographic model and have proposed a new high-capacity embedding/extracting module that is based on the Variable-size LSB insertion. In the embedding part, based on the contrast and luminance property, we used three components to maximize the capacity, minimize the embedding error and eliminate the false contours. Using the proposed method, they embedded at least four message bits in each pixel while maintaining the imperceptibility requirement.

Juneja M. et al. [9] introduced the concept of steganography and steganalysis as well as the methods for carrying these out. It also presented the authors' application which was demonstrated to be more secure than current applications against statistical attacks commonly used in steganalysis.

Thangadurai K., et al. [10] discussed the LSB method to hide the secret message in the Least Significant bit of the image. The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded LSB method is applied for various file formats. This method can use for both GIF and PNG file format. PNG does not support animation like GIF. PNG works well in online applications such as World Wide Web. LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a gray scale image.

III. OVERALL DIAGRAM

The performance of the steganographic method in both spatial domain and frequency domain is evaluated. We used LSB insertion and DCT method for spatial and frequency domains, respectively.

For all experiments, we used two colour JPEG images as secret images to be embedded into four colour cover images. These cover images were chosen such that they include different textures and colour distributions. Fig. 1 & Fig. 2 shows four cover images and two secret images selected in this study. In this project, we investigate the effect of transforming the secret image before embedding it into the cover.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

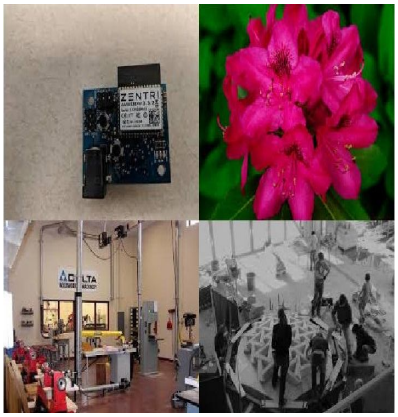


Fig. 1 Cover Image

Fig. 2 Secret Image

Our approach is based on a transformed secret image using an invertible function so that the image can be recovered. The approach is summarized in Fig. 3 & Fig. 4.

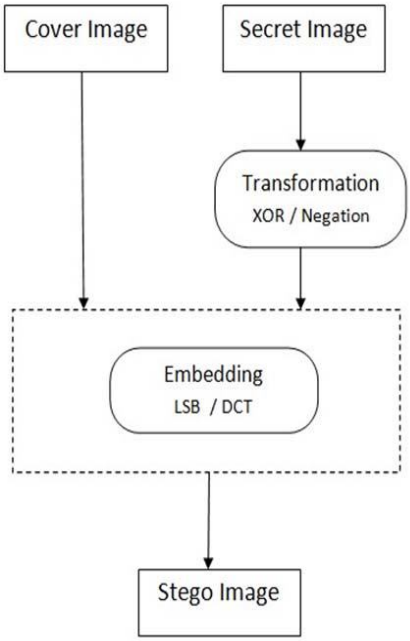


Fig. 3 Embedding Process

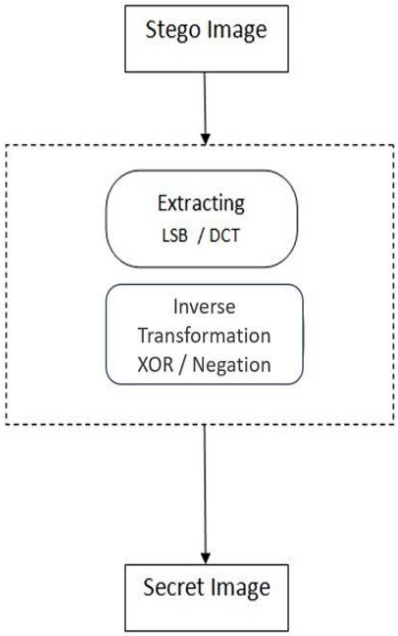


Fig. 4 Extracting Process

The reason to apply a transformation to the secret image is to reduce structural information so that the cover image is less affected. XOR is selected as a transformation function since it is reversible and it reduces the difference between smooth and non-smooth areas.

IV. EVALUATION PARAMETER

The performance of proposed algorithm is analyzed and discussed based on Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). They are employed to measure the quality of a stego-image.

A. Mean Square Error (MSE)

Lower MSE values correspond to better stego images. It is defined as follows,

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [C(i,j) - S(i,j)]\text{^}2 \quad \text{..... (1)}$$

Where, C is cover image, S is a stego image, and m and n represent the number of rows and columns if the image matrix respectively.

B. Peak Signal-to-Noise Ratio (PSNR)

PSNR is often expressed on logarithmic scale in decibels (dB) given in following Eq. 2. The higher the PSNR is, the better the quality of the stego-image is.

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

Where, Cmax is the maximum pixel value in the cover image.

V. RESULTS

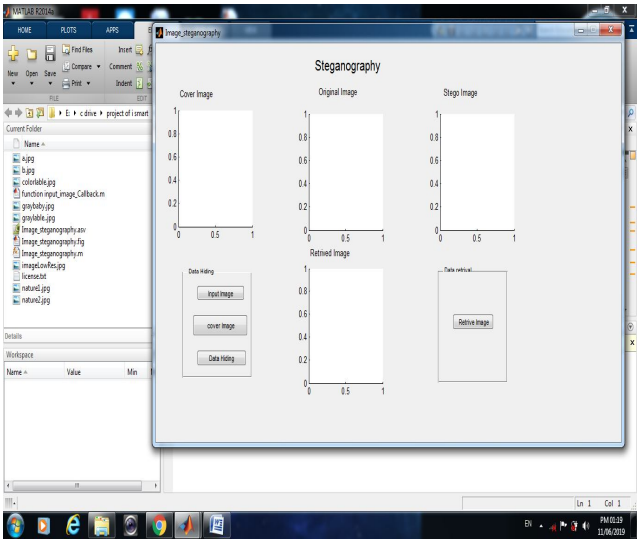


Fig 5. Result Image-1

As shown in above Fig. 5, all images will appear in single window.
It includes Input Image, Cover Image, Stego Image and finally Retrieved Image.

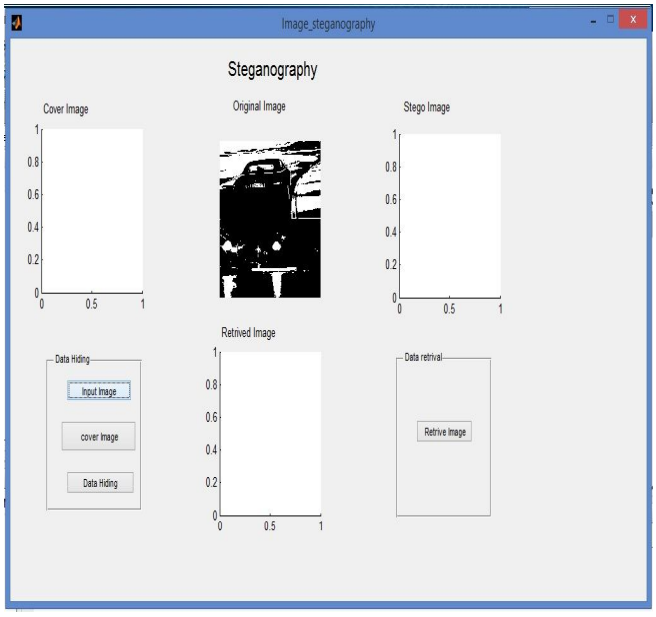


Fig. 6 Result Image-2

In above Fig 6, Input or original Image is given which is greyscale image. This image is used as secret image which is to be transformed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

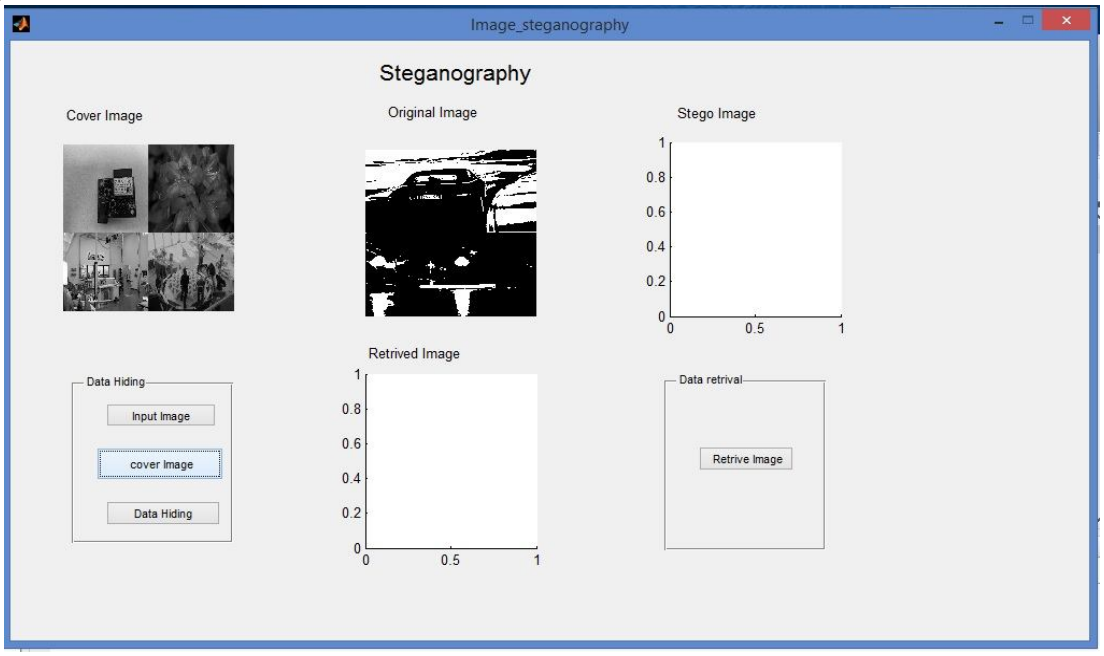


Fig. 7 Result Image-3

As shown in above Fig 7, Cover Image is given. Behind cover image, secret image i.e. input or original image is embedded.

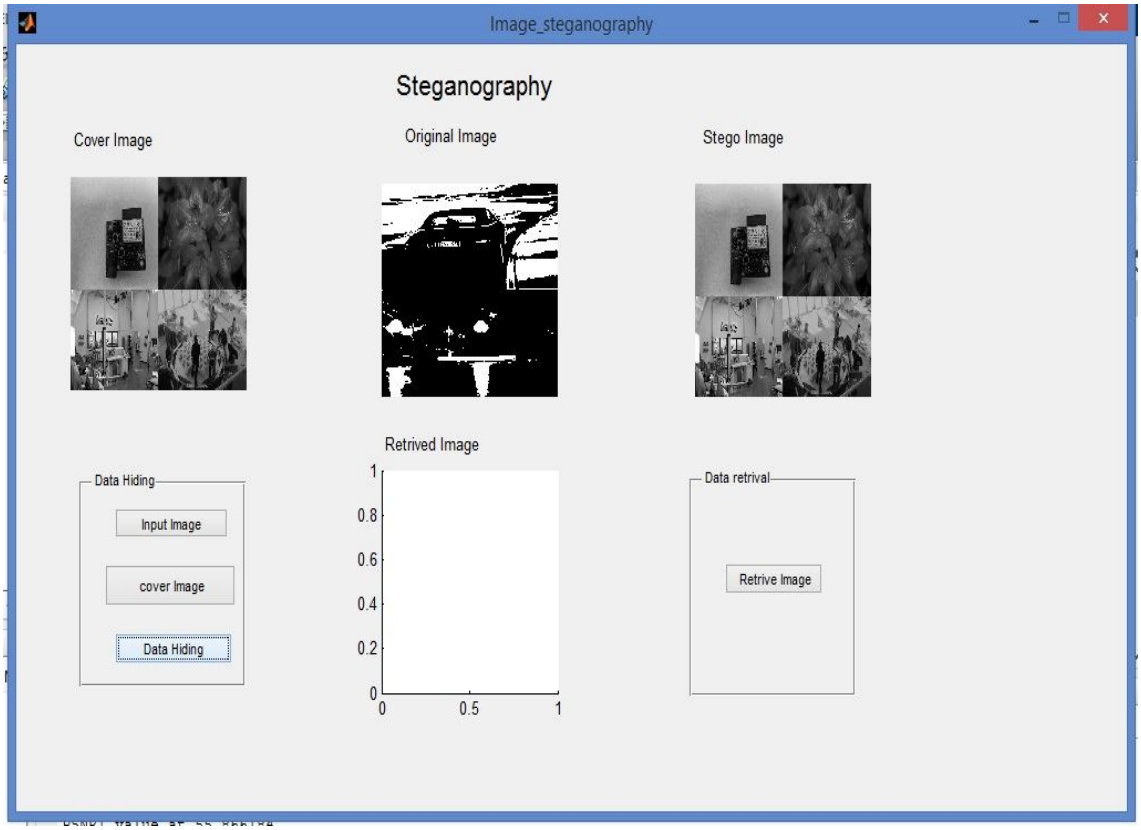


Fig. 8 Result Image-4

Fig.8 is Stego Image which is combination of cover image and secret image i.e. input or original image.

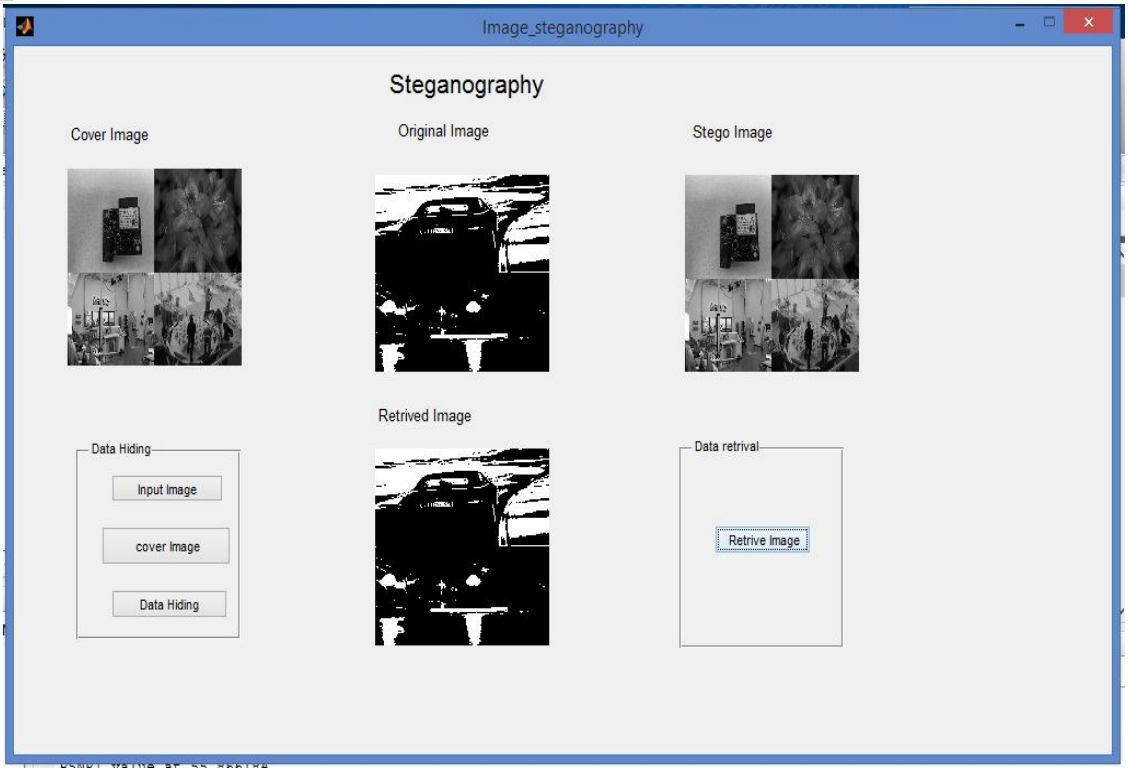


Fig. 9 Result Image-5

Above Fig 9 shows the retrieved image which is same as input image. This retrieved image is extracted from stego image and obtained same as input image.

Resulting MSE and PSNR values for the LSB with XOR Transformation of secret image and cover image are listed in Table 1 and MSE and PSNR values for the DCT technique are listed in Table 2.

Table-1 MSE and PSNR values for LSB with XOR Transformation

Secret Image	Cover Image	1-LSB		2-LSB		3-LSB	
		MSE	PSNR	MSE	PSNR	MSE	PSNR
Car	Gadget	1.0020	53.6593	1.0545	50.9859	3.0276	17.7591
	Flower	1.0056	53.4684	1.0585	50.7949	3.0605	17.5681
	Workshop	1.0092	53.2774	1.0625	50.6040	3.0941	17.3772
	People	1.0128	53.0864	1.0665	50.4130	3.1285	17.1862
Event	Gadget	1.0165	52.8955	1.0706	50.2221	3.1637	16.9953
	Flower	1.0201	52.8955	1.0746	50.0311	3.1996	16.8042
	Workshop	1.0238	52.5136	1.0788	49.8401	3.2364	16.6134
	People	1.0276	52.3226	1.0829	49.6492	3.2740	16.4224

Table-2 MSE and PSNR values for DCT technique

Secret Image	Cover Image	1-LSB		2-LSB		4-LSB	
		MSE	PSNR	MSE	PSNR	MSE	PSNR
Car	Gadget	1.0019	56.0124	1.0233	54.8424	1.0456	53.6724
	Flower	1.0046	55.8661	1.0260	54.6962	1.0485	53.5262
	Workshop	1.0072	55.7199	1.0288	54.5499	1.0513	53.3799
	People	1.0098	55.5736	1.0316	54.4037	1.0542	53.2337
Event	Gadget	1.0125	55.4274	1.0343	54.2574	1.0571	53.0874
	Flower	1.0152	55.2811	1.0371	54.1112	1.0601	52.9412
	Workshop	1.0179	55.1349	1.0400	53.9649	1.0630	52.7950
	People	1.0206	54.9887	1.0428	53.8187	1.0660	52.6487

VI. CONCLUSION

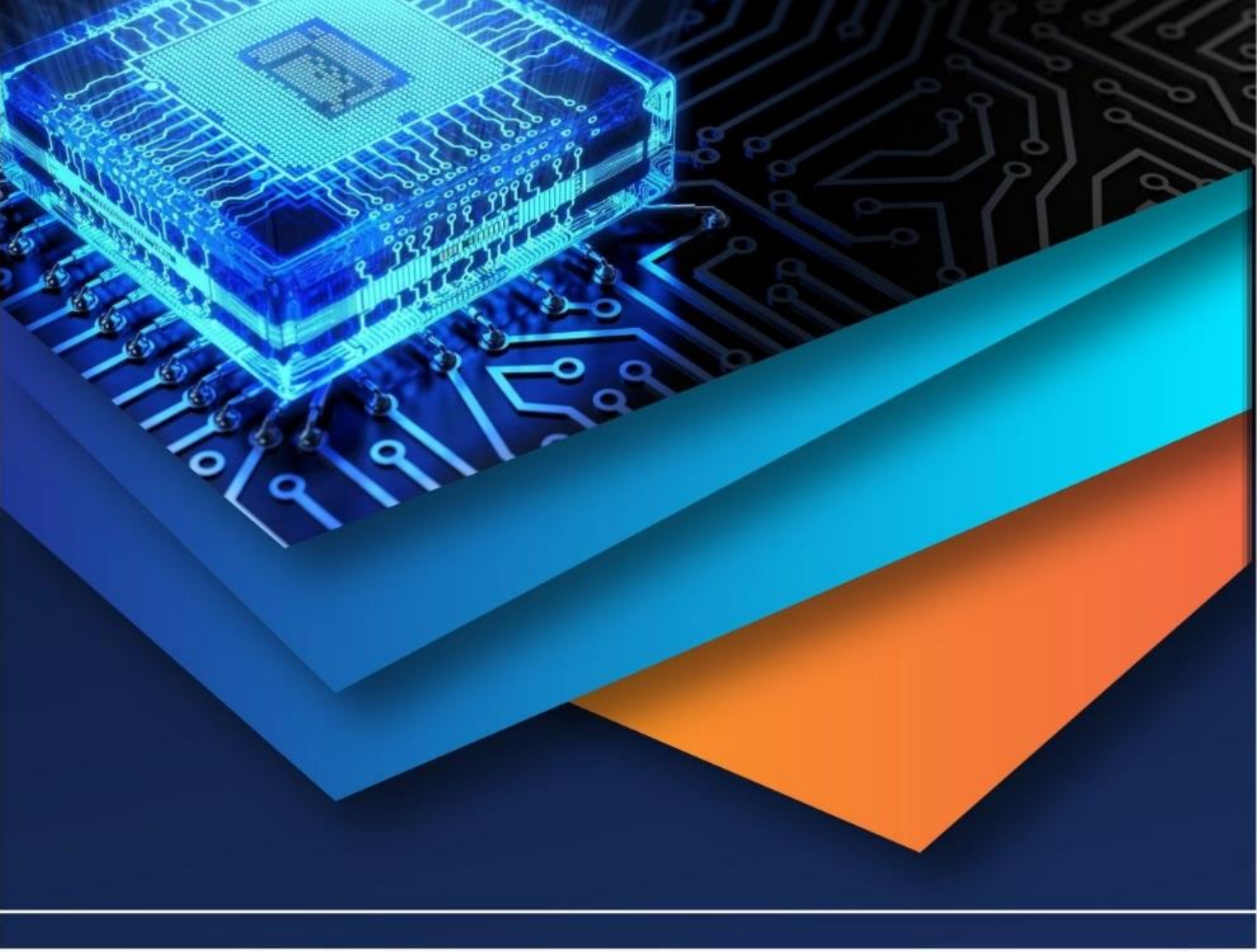
In this paper we presented secret image transformation using steganography. Secret image transformation enters more and more into our everyday soldier and military life, thus there is an urgent need to further develop techniques into practical applications.

This paper is presented steganography. Steganography are ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. These troubles are usually happened in the internet communication. Hence data needs high protection on consistently. Main reason behind using steganography is secret image transformation, non disclaimer, consistency and honesty at any instant of data transfers. Steganography can be described as the skill of protection file and it makes sure that only the related people to access the content.

This paper, we examined the influence of secret image transformation, before embedding the secret image, on stego image quality. XOR is selected as a transformation function and compared to Negation transformation. Experimental results had shown that performing XOR transformation to the secret image gave better performance than Negation in the LSB method especially when embedding more than one bit. On the other hand, the same performance increase was not observed in DCT based implementation. This study was limited only to the two different transformations. However, more research is required to find another type of transformation causing a better performance.

REFERENCES

[1] 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.
[2] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform,'' International Conference on Intelligent System and Signal Processing (ISSP), pp.97,100, March 2013.
[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] 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.
[5] Masoud Nosrati, Ali Hanani , Ronak Karimi , "Steganography in Image Segment using Genetic Algorithm" , Fifth International Conference on Advanced Computing & Communication Technology, 2015.
[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.
[8] Lee, Y. K. & Chen, L. H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.
[9] Juneja, M.; Sandhu, P. S. "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.
[10] Thangadurai, K., & Sudha Devi, G., "An analysis of LSB based image steganography techniques," International Conference on Computer Communication and Informatics, 2014.
[11] Devi, M., & Sharma, N., "Improved detection of least Significant bit steganography algorithms in color and gray scale images," Recent Advances in Engineering and Computational Sciences (RAECS), 2014.
[12] Menon, N., & Vaithiyanathan., "A survey on image steganography," International Conference on Technological Advancements in Power and Energy (TAP Energy), 2017.
[13] Sugathan, S., "An improved LSB embedding technique for image steganography," 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016.
[14] Sheidaee, A., & Farzinvash, L., "A novel image steganography technique based on DCT and LSB," 9th International Conference on Information and Knowledge Technology (IKT), 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY