iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IX **Month of publication:** September 2016

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Data Hiding Using Blind Algorithm of Steganography

Mohit Gupta[1], Praveen Kr. Tripathi[2]
[1]M.Tech Scholar, [2]Asst. Professor, Dept. of Computer Science and Engineering, KIT Kanpur, Uttar Pradesh, India

Abstract— The process of hiding messages or information within other non-secret text or data is called steganography. Steganography may be text, image, audio or video steganography. Digital image Steganography is popular because images have high data hiding capacity and are used for transmission. We propose and implement a data hiding method using blind algorithm of steganography which hides secret data in colour images by maintaining good visual quality and takes very less time in hiding and extraction of message. This method is based on third level two dimensional discrete wavelet transform (DWT) set by Haar wavelet. The main advantage of blind steganography methods is that there is no requirement of original image in extraction process which makes secret communication undetected by third party user or any steganalysis tools. In order to obtain a better imperceptibility result secret message Huffman encoding is used. The security of communication is also increased by these modifications. The experimental activities are carried out by using software MATLAB R2014a.
Keywords— steganography, DWT, data hiding, steganalysis, Haar wavelet

I. INTRODUCTION

Steganography is a process of secret communication where a piece of information (a secret message) is hidden into another piece of innocent looking information, popularly called a cover, in such a way that the very existence of the secret information remains concealed without raising any suspicion in the minds of the viewers.

Steganography Techniques are divided into two categories such as spatial domain techniques and transform domain techniques. In spatial domain methods data is embedded by manipulating the intensities of pixel. In transform domain techniques, the image is first transformed into frequency domain and then data is embedded.

In [1], authors explained the steganography, history of steganography and techniques of steganography such as LSB masking, filtering and other used methods of data hiding. In [2], authors explained the concept of data hiding using LSB technique combined with AES algorithm to obtain better security. In paper [3] compression technique is applied on secret message then hashing and encryption are performed. This method provides privacy and authenticity. In [4], various techniques of image steganography are proposed. In this spatial and frequency domain techniques are discussed. This paper also proposed techniques for steganalysis. The paper [5] discussed the method where secret message is compressed using wavelet transform technique and then embedding into cover image using LSB technique. The authors in paper [6] introduced the method of steganography combined with DES encryption. In [7], authors encrypt the data with RC4 algorithm and then embedding in cover image is performed. In [8], concepts of cryptography were discussed.

In this paper we propose a method, which hides secret message in colour images. This method maintains good visual quality and takes very less time in hiding and extraction of message. The main advantage of this method is full reconstruction of secret message and there is no need of cover image in extraction process.

A. Discrete Wavelet Transform (DWT)

A wave is an oscillating function of time or space. The main advantage of wavelets is that they provide a strong mathematical framework for analysing functions at various scales. This property makes wavelet-based analysis a powerful tool in image processing. Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image.

For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1 as shown in Fig. 1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients.

To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. The frequency domain transform we applied in this paper is 3rd level Haar-DWT. Decomposition of an image into 3rd level DWT is shown in Fig. 2.

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

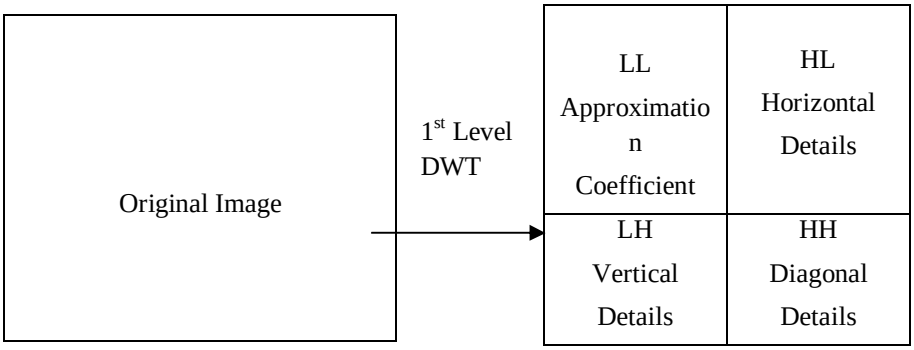


Fig. 1 1st level DWT decomposition of image

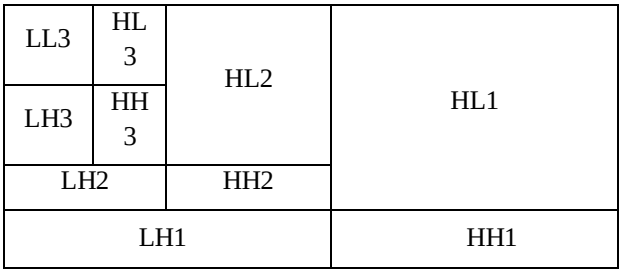


Fig. 2 Third Level Discrete Wavelet Transform

B. Huffman coding

A Huffman coding is a lossless data compression algorithm. The idea is to assign variable-length codes to input characters; lengths of the assigned codes are based on the frequencies of corresponding characters. The most frequent character gets the smallest code and the least frequent character gets the largest code. Efficiency of Huffman coding is defined as the ratio between bit per symbol (BPS) and average length of code word.

II. PARAMETERS USED FOR VISUAL QUALITY

A. Peak Signal to Noise Ratio (PSNR)

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel (dB) scale [10].

Where E is Mean Square Error, f (i, j) is pixel value of original image and f' (i, j) is pixel value of Stego image.

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{E}\right) \text{dB} \quad (1)$$

$$E = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} [f(i,j) - f'(i,j)]^2 \quad (2)$$

The PSNR depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and Stego image. For better steganographic system mean square error (E) should be less and PSNR should be high.

B. Structural Similarity Index (SSIM)

An image quality metric that assesses the visual impact of three characteristics of an image: luminance, contrast and structure. The SSIM index is calculated on various windows of an image [9]. The measure between two windows x and y of common size N×N is

$$\text{SSIM}(x, y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

μ_x is the average of x

μ_y is the average of y
σ_x^2 is the variance of x
σ_y^2 is the variance of y
σ_{xy} is the covariance of x and y
$C_1 = (k_1 L)^2$, $C_2 = (k_2 L)^2$ two variables to stabilize the division with weak denominator
L is the dynamic range of the pixel-values (typically this is $2^{\#\text{ bit per symbol}} - 1$)
k_1=0.01 and k_2 =0.03 by default.
The SSIM index satisfies the condition of symmetry SSIM(x, y) = SSIM(y, x)

III. PROPOSED METHOD

We propose a data hiding method using blind algorithm of steganography which is based on third level two dimensional discrete wavelet transform (DWT) set by Haar wavelet. In order to obtain a better imperceptibility result secret message Huffman encoding is used.

A. Embedding Process

The process of embedding is performed in following steps.

1) Select a cover Image I of size of M×N pixels.

2) We create picture elements I_1, I_2, I_3, I_4 from cover image (I) with same dimension.

I_1 is formed by taking the elements of every odd column and odd lines of I on same position. I_2 is formed by taking the elements of every even column and odd lines of I on same position.I_3 is formed by taking elements of every odd column and even lines of I on same position. Similarly I_4 is formed by taking elements of every even column and even lines of I on same position. Other elements of I_1, I_2, I_3 and I_4 are zeros.

$$I_1(2i-1, 2j-1) = I(2i-1, 2j-1) \quad (4)$$
$$I_2(2i-1, 2j) = I(2i-1, 2j) \quad (5)$$
$$I_3(2i, 2j-1) = I(2i, 2j-1) \quad (6)$$
$$I_4(2i, 2j) = I(2i, 2j) \quad (7)$$

where i=1, 2, 3…M and j=1, 2, 3…N.

3) Apply Third Level Haar DWT on I_1, I_2, I_3 and I4 each and find approximation coefficient LL_1, LL_2, LL_3 and LL_4 respectively.

4) Compute Matrix I_X as $I_X = \begin{pmatrix} LL_1 & LL_2 \\ LL_3 & LL_4 \end{pmatrix}$ (8)

5) We select the secret message M and apply Huffman coding to compress the message and reshape the message vector according to the size of I_x.

6) The transformation coefficients of the matrix Ix will change according to the bits of secret message and we obtain matrix I_h. Modified coefficients are obtained as follows:

a) $I_x(i,j) = \text{floor}(I_x(i,j))$
b) Sum=0
c) If m(2i, 2j-1) ==1 then sum=sum+0.5
d) If m(2i-1,2j) ==1 then sum=sum+0.25
e) If m(2i, 2j) ==1 then sum=sum+0.125
f) If m(2i-1,2j-1) ==0 and mod(Ix(i,j),2) ==0 then Ix(i,j)= Ix(i,j)+sum
g) If m(2i-1,2j-1) ==0 and mod(Ix(i,j,),2) ==1 then I_x(i,j)= Ix(i,j)-1+sum
h) If m(2i-1,2j-1) ==1 and mod(Ix(i,j),2) ==1 then Ix(i,j)= Ix(i,j)+sum
i) If m(2i-1,2j-1) ==1 and mod(Ix(i,j,),2) ==0 then Ix(i,j)= Ix(i,j)-1+sum
j) I_h=Ix

7) Now we apply inverse discrete wavelet transform (IDWT) on I_h and we obtain image with hidden data i.e. Stego image (I_{hh}). Flow chart of embedding process is shown in Fig. 3.

B. Extraction Process

For extraction on the receiver side, we need stego image and the hiding algorithm's modifications of cover image to reconstruct the

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

secret message. We create four matrices from Stego image (I_{hh}) similarly as they were formed in embedding process then we apply third level Haar DWT on each matrix and create four approximation matrices in similar way of embedding process. Now extraction of secret message is done in opposite manner of embedding process. After that we reshape the obtained message and apply Huffman decoding to obtain original secret message. The flow chart of extraction process is shown in Fig. 4.

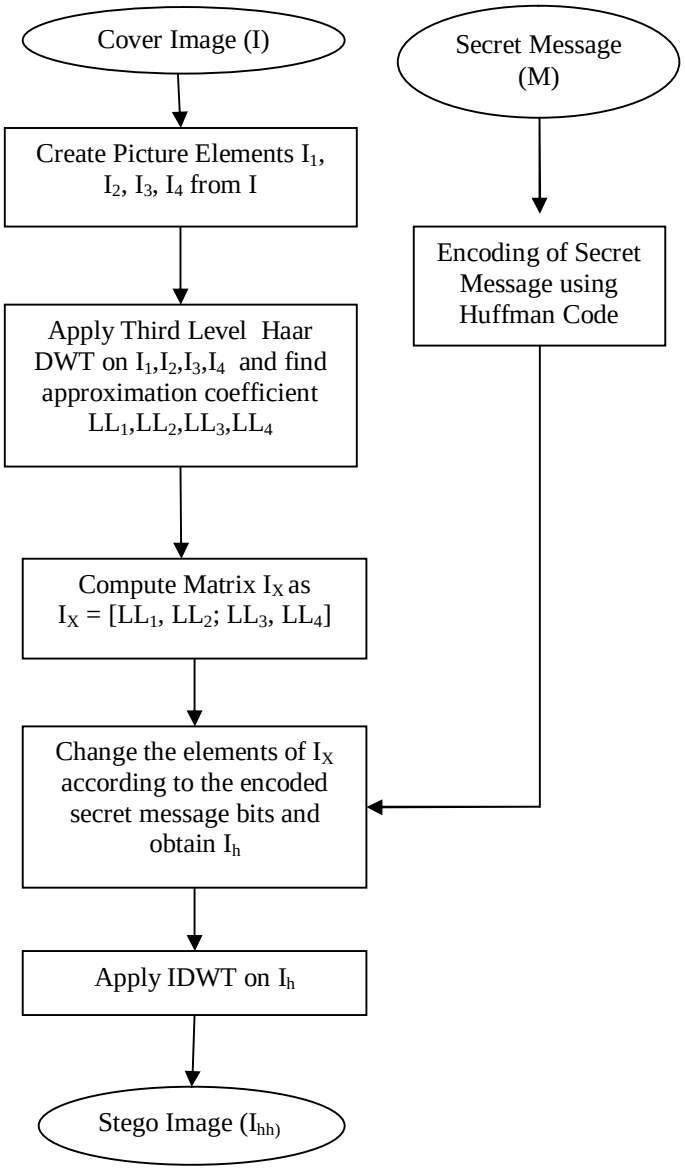


Fig. 3 Embedding Process

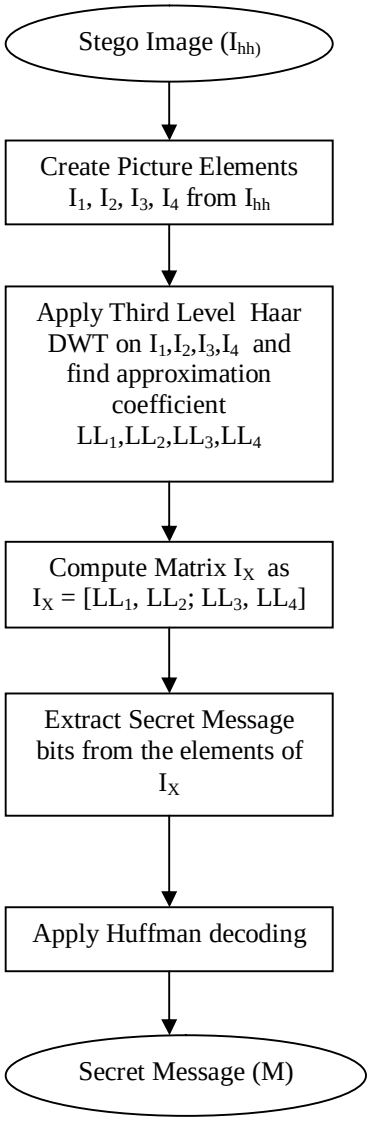


Fig. 4 Extraction Process

IV. EXPERIMENTAL RESULTS

Implementation of proposed method is done by using MATLAB R2014a on a system with hardware configuration Intel(R) Core2Duo CPU with 2.00GB RAM. For testing the performance of proposed system various cover images are taken. The selection of proper Huffman coding alphabet size is also important so we represent performance of Huffman coding based on secret messages of different size.

The Table I contains a Huffman coding efficiency of secret text data in case of different alphabets size. Testing of Huffman coding efficiency was performed with the different size of secret message. It can be observed from Table 1 that with increasing character's size (bit per symbol) the coding efficiency is also increasing. So in our implementation we use character length 16 bit/symbol length.

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The Fig. 5 also shows the Huffman coding efficiency for text messages of different size. It can be observed that with increasing character's size i.e. bit per symbol (BPS) the coding efficiency is also increasing. Plot is drawn for three secret messages of different length.

The Table II contains results of embedding and extraction of a secret message (size 494 bytes) on different cover images of same size (384*384). Alphabet character's length of Huffman code is 16 bit / symbol.

TABLE I
SECRET MESSAGE HUFFMAN CODING EFFICIENCY

Bit Per Symbol (BPS)	Secret Message 1 (198 bytes)	Secret Message 2 (370 bytes)	Secret Message 3 (726 bytes)
	Efficiency	Efficiency	Efficiency
2	1	1	1
4	1.1973	1.1931	1.1924
8	1.844	1.8351	1.8497
16	2.601	2.4026	2.3093

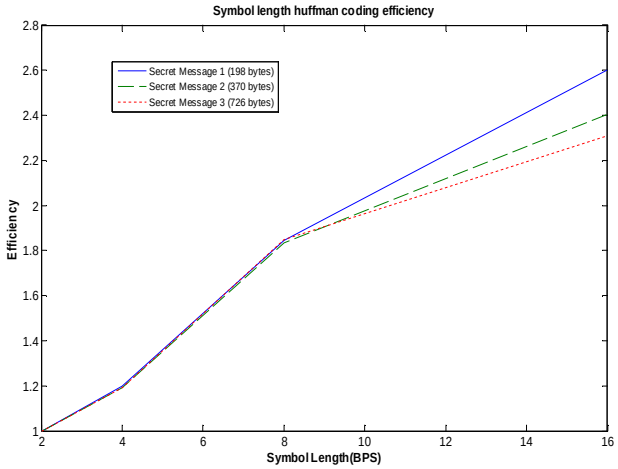


Fig. 5 Symbol length (BPS) Huffman encoding efficiency

TABLE II
EMBEDDING AND EXTRACTION RESULT

Cover Image (384*384)	PSNR(dB)	SSIM	Embedding duration(s)	Extraction duration(s)
Lena	66.834	0.99967	0.63622	0.030499
Baboon	67.694	0.99927	0.54944	0.030594
Desert	78.002	0.99909	0.51138	0.030242
Penguin	89.253	0.99847	0.48713	0.030349

The proposed scheme ensures high embedding and extraction rates and also maintaining high level of security with good PSNR and SSIM index. We observed that the messages were successfully embedded into the cover images and there is no need of cover image at the time of extraction so method is secure against steganalysis. Fig. 6 shows original image, image with hidden data and various parameters for cover image Lena.

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

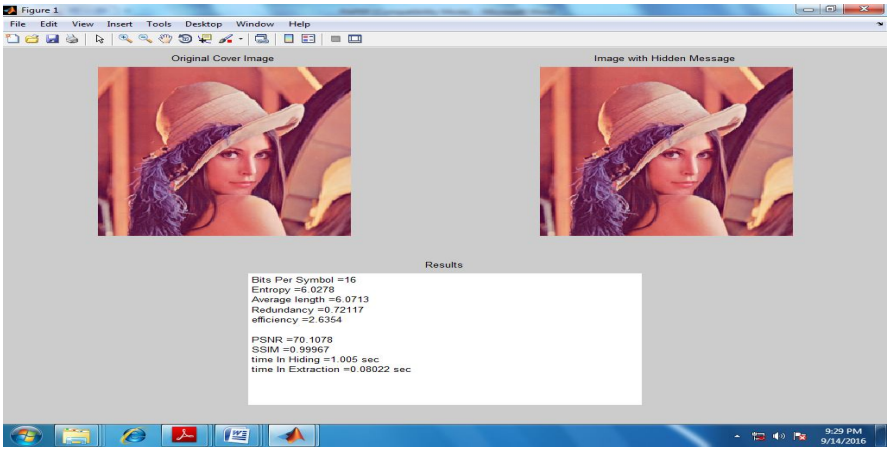


Fig. 6 Original Image, Image with hidden data and parameters

V. CONCLUSION AND FUTURE WORK

We design data hiding method that uses properties of the Haar transform coefficients. The secret message is encoded before embedding in order to increase the capacity of the proposed data hiding system. The main advantage of this method is that at the time of extraction there is no requirement of the original cover image which increases the security of proposed steganography system. Increasing capacity has a negative impact on the visual quality of stego image so the selection of a proper cover image is important in method's capacity and imperceptibility of stego image. In future we can modify embedding & extraction formula for hiding audio data in cover image. The method can further be extended with taking into account other data hiding encryption and compression techniques.

REFERENCES

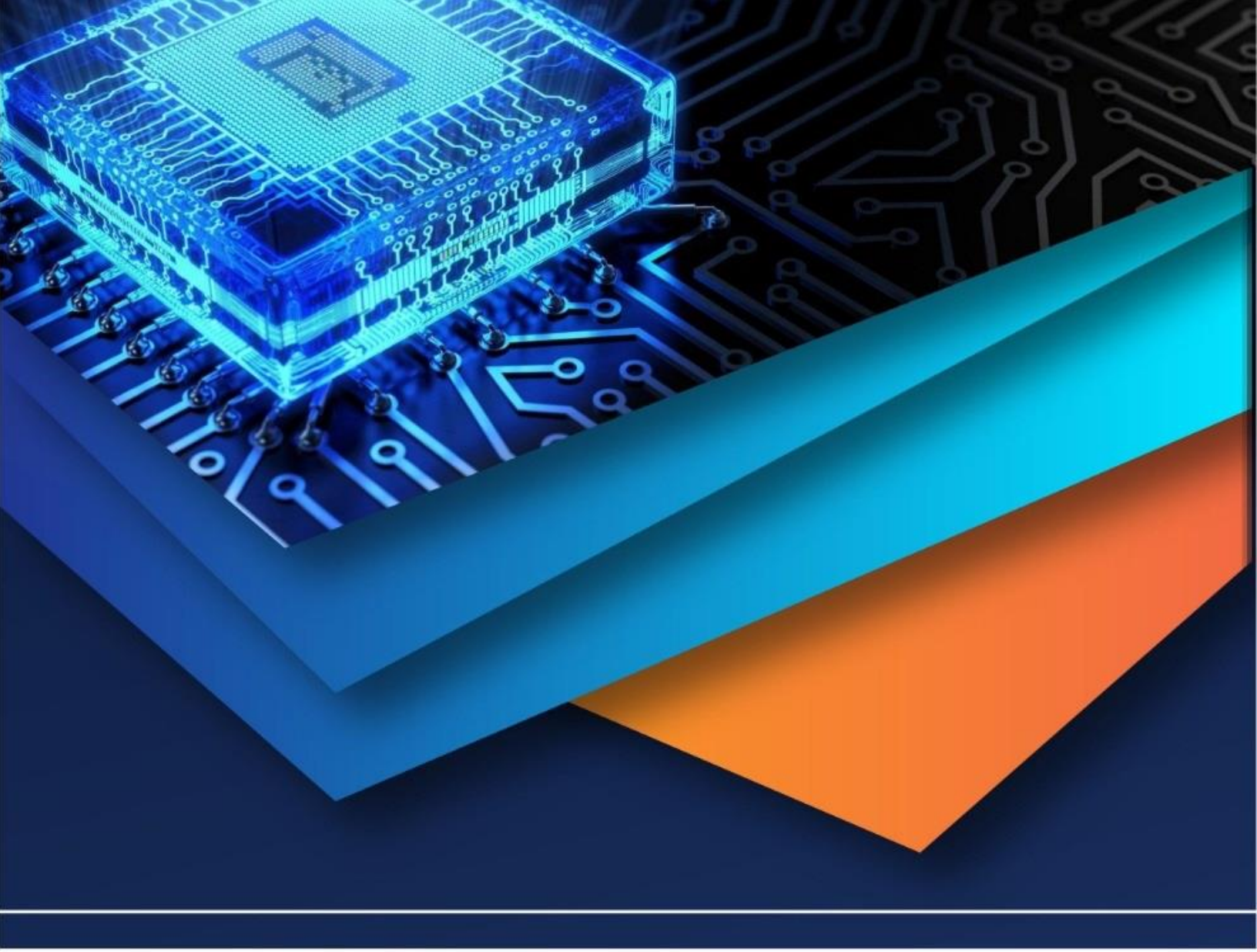
[1] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.
[2] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, ISSN: 22773061, Vol.9, July 2013, pp. 976-984.
[3] H.Al-Barhmtoshy, E.Osman and M.Ezzaand, "A Novel Security Model Combining Cryptography and Steganography", Technical Report, 2004, pp. 483-490.
[4] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, Dec 2012, pp. 171-177.
[5] Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Pwer and Computing Technologies, March 2013, pp. 1197-1200.
[6] R.Nivedhitha, Dr.T.Meyyappan, "Image Security using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, ISSN: 2231-5381, Vol.7, 2012, pp. 366-371.
[7] Wai Wai Zin, "Implementation and Analysis of Three Steganographic Approaches", IEEE Xplore International Conference on Computer Research and Development, March 2011, pp. 456-460.
[8] F. Piper, "Basic Principles of Cryptography", IEEE Colloquium on Public uses of Cryptography, April 1996, pp. 2/1-2/3.
[9] https://en.wikipedia.org/wiki/Structural_similarity
[10] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

AUTHOR'S PROFILE

Mohit Gupta is currently M.Tech scholar in computer science and engineering department at Kanpur Institute of Technology, Kanpur, India. He has completed B.Tech in computer science and engineering from A.K.T.U., Lucknow, India in 2011.

Volume 4 Issue IX, September 2016
ISSN: 2321-9653

Praveen Kr. Tripathiis presently working as a Assistant Professor in computer science and engineering department in Kanpur Institute of Technology,Kanpur. He is having more than 8 years of teaching experience.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY