iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** I **Month of publication:** January 2017

DOI:

www.ijraset.com

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

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

Steganography for Secure Communication Using BPCS and HDWT

Siddalingesh Bandi[1], Manjunatha Reddy. H S[2]
Department of ECE, Global Academy of Technology, Bengaluru

Abstract— Steganography is an invisible communication for hiding existence of communicated information bits. In this paper, we propose Steganography for Secure Communication using BPCS and HDWT (SSCBH). The Bit Plane Complexity Splicing (BPCS) is applied on the cover image of size 512 x 512 to generate bit planes. The HDWT is applied on each bit plane to generate four subbands. The HH subband of the cover image is used to embed the payload. The permutation process is used to generate stego key which is used to extract the payload. The payload is converted into binary form and last 4-LSB bits of each column are embedded into the HH band of cover image. It is observed that the value of PSNR is high for the payload image of size 90 x 90 for different images of cover image.

Key words—Steganography, Cover image, Payload image, Stego image, BPCS, HDWT.

I. INTRODUCTION

In any communication, security is the most important task over past few decades. With the advancement of communication technology and use of internet has grown extremely to exchange information without any distance barrier. However, such network is most popular for fast and easy process to exchange information over the long distance but still the message transmissions over the internet have faces a lot of concerns brought up in the security of information transmitted over the channel. Therefore the applications of cyber world needs high level of safeguard for data and produce explosive growth to the field of information hiding [The three fundamental routines for secured correspondence accessible are Cryptography, Steganography and Watermarking. The Cryptography manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures. Steganography is a procedure for concealing and separating data to be passed on utilizing a transporter signal. The Watermarking is a method for creating legitimate strategies for concealing restrictive data in the perceptual information The Steganography means concealed writing i.e. the word “steganos” means “covered “ and “graphy “ means “writing” . Steganography is dealing with writing hidden messages/pictures in a particular way that only the sender and recipient are able to decipher so as to provide security. The common types of Steganography are Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Network or protocol Steganography.Text Steganography: It consists of hiding information inside the text files. The secret data is hidden behind every n^{th} letter of every word of text messages. Image Steganography: Hiding the data by taking the image as cover object, pixel intensities are used to hide the secret data.Audio Steganography: The audio files are used as a cover to hide the secret information. This method hides the data in Waveform Audio File Format (WAV) and MP3 sound filesVideo Steganography: The video files are used as a cover to hide the secret information. The Moving Pictures Expert Group4 (MPEG4) and Audio Video Interleaved (AVI) are the common formats used for video Steganography.Network or protocol Steganography: It involves hiding the secret information by considering the network protocol like Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Internet Protocol (IP) etc. as cover object [3].The Steganography is categorized into Spatial domain Steganography and Transform domain Steganography. In Spatial domain Steganography, the secret image is embedded into the pixel of cover image directly. The commonly used method is Least Significant Bit (LSB) which hides a secret message in the LSBs of pixel values without introducing perceptible distortions. It is used because of high capacity information.The Transform domain is the process of embedding the transformed coefficients of the secrete information into transformed coefficient of the cover image. The various Transform domain techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT) etc. It is preferred because of high ability to tolerate noises.

II. RELATED WORK

A.Prabhune and S. M. Joshi [4] proposed the Diamond Encoding algorithm for hiding the secret image and text file and DCT

algorithm for hiding secret audio file. Video is taken as embedding media, then image frames and audio is extracted from video. Image frames are selected by using password entered for hiding data. Original frame is replaced by stego-frame and stego video form. At the receiver end user enters the password, if that password is correct then that authorize user can be able to extract data from video frame. Kirti D. Nagpal et al., [5] have proposed a hybrid technique in frequency domain for the performance evaluation of image steganography in order to measures the imperceptibility and robustness of the proposed system. The evaluation parameters used are for Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC). R. Rejani et al., [6] Proposed method to protect the software against piracy with the combination of inbuilt hardware, steganography and encryption. The Advanced Encryption Standard (AES) algorithm and geographic location are used.

S. Y. Kanawade et al., [7] presented the LSB algorithm to provide security for wireless communication through Zigbee using Cryptography and Steganography. The information security is the most Significant problems in data Communication nowadays. Dhanya Job and Varghese Paul [8] proposed a video Steganography technique for secured data transmission. Video Steganography refers to the process of hiding the data into video. The proposed method not only hides the data, but also it converts the original data into secret code.

Vedanti M Khandare et al., [9] proposed an ECG Steganography to Secure the Patient's Confidential Information. It is very important that patient confidentiality is protected while data are being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. Many times patients ECG signal and other physiological readings are collected by using Body Sensor Networks and that will be transmitted and diagnosed by remote patient monitoring systems.

Essam H. Houssein et al., [10 proposed a technique for encrypting data using Advanced Encryption System (AES) and hiding the data using Haar Discreet Wavelet Transform (HDWT). HDWT aims to decrease the complexity in image steganology while providing less image distortion and lesser detectability. K.S.Seethalakshmi et al., [11] proposed a model for enhancing security in image steganography using visual cryptography and neural networks. During encryption, the image is split into 'n' number of shares. During decryption, these shares are stacked together to get original image. Neural networks are concerned with identifying the best locations in host image in order to embed the secret data thus improving the image quality.

Sandip Bhasme et al., [12] presented an approach which provides limited information for fund transfer using steganography and visual cryptography to ensure the security for the customer's data, decrease customer's risk, prevent identity theft. Major factors that affects to customers in online shopping and payment are fraud in debit card or credit card and personal information security. Utsav Sheth and Shiva Saxena [13], proposed a technique for image Steganography using AES algorithm and least significant nibble. The steganography algorithm used maximizes on data capacity and ensures security. The Java programming language is used for its comprehensive libraries and simple GUI has been developed using Java.

III. PROPOSED MODEL

In this section, the definitions and proposed model of Steganography for Secure Communication using BPCS and HDWT are discussed.

A. Definitions of the Performance parameters

1, Embedding Capacity:

The size of the information bits are embedded into the cover image. The capacity is defined as

$$Capacity = \frac{\text{Size of Payload image}}{\text{Size of cover image}}$$

2.Mean Square Error (MSE): It is defined as the square of error between cover image and Stego image as given in equation (1)

$$MSE = \left[\frac{1}{N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}\left(X(i,j) - Y(i,j)\right)^2 \qquad \text{---------- (1)}$$

Where X (i,j): Value of pixel in cover image, Y(i,j): Value of pixel in stego image, N: Size of an Image.

3. Peak Signal to Noise Ratio (PSNR): It measures the quality of the image by comparing the Cover Image with the Stego Image as given in equation (2). The PSNR is used to measure the quality of image after extraction. The value of PSNR is high for better

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

quality.

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

B. Proposed Embedded model

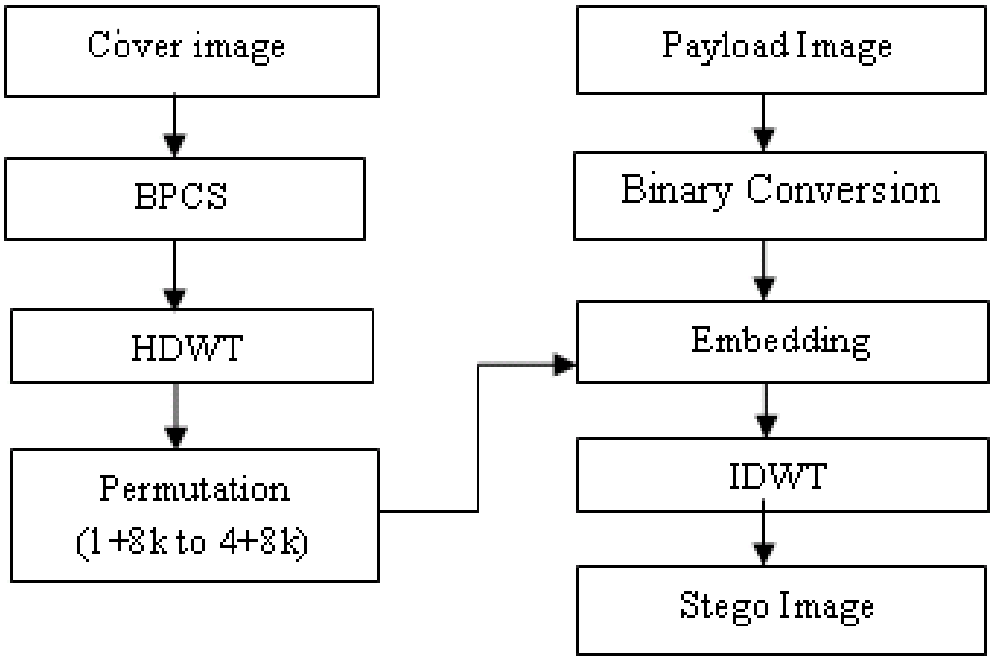


Fig.1 Proposed Embedding model of SCCBH

Cover Image: Cover image of any size isused and it is resized to a standard format/ standard size of 512 X 512.

Bit Plane Complexity Splicing (BPCS): The cover image is a colour image of each pixel of 8 bit to get 24 bits size of Red, Green and Blue. The 24 bits is thus split into 3 planes of RGB of each 8 bits. The 8 bits are further divided into 8 bit planes from 0^{th} bit plane to the 7^{th} bit plane. The 0^{th} bit plane represents the LSB (least significant bits) and the 7^{th} bit plane represents the MSB (most significant bits).

Haar Discrete Wavelet Transform (HDWT): The Haar Discrete Wavelet Transform (HDWT) is applied on each bit planes to generate four subands HH, HL, LH, and LL. The HH band is used to embed the payload. The LL frequency band is also known as Approximate band whereas the HH, HL, LH bands are called as Detail bands. The approximation band contains maximum information of image and other high frequency bands contain redundant information.

Permutation: The idea behind the permutation is that the permutation generator uses the stego key and produces output of different sequences. In this technique the permutation of stego key for encryption and decryption is generated using 1+8k to 4+8k, where k varies from 0 to 31.

Payload Image: Payload image is the secret image that has to be embedded into the cover image of HH Band. The images of different sizes and formats are considered as secrete information to be embedded into the cover image to generate stego image which is communicated to destination.

Binary Conversion: Initially the pixel intensity values are expressed in terms of coefficients of a two – dimensional matrix. These pixels are then arranged column-wise and the pixel values are converted into binary stream. The bits from this column matrix are embedded into the last 4 least significant bits of the cover image of HH Band.

Embedding: The main objective of embedding is to embed the payload image into cover image so that even the existence of the

payload image cannot be detected. The payload bit stream is embedded into the least significant bits of the coefficients of wavelet transformed cover image. The four least significant bits of payload image is embedded into the four most significant bits of cover image in wavelet domain.

Inverse Discrete Wavelet Transform (IDWT): After embedding IDWT is applied to get the stego image.

Stego Image: It is an image obtained after embedded the payload into a given cover image. It has similar statistical properties to that of the cover image.

C. Proposed Extracted Model

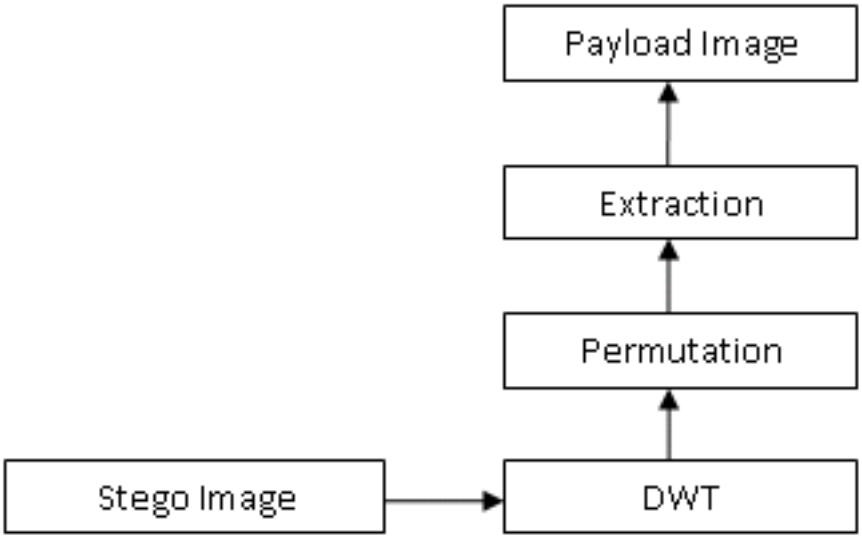


Fig.2 Proposed Extracting model of SCCBH

The extraction is the reverse process of embedding to get the original payload. The DWT is applied on stego image to generate four subbands. The embedded secret information is extracted from the HH band using stego key.

D. Proposed Algorithms

Embedding Algorithm: The cover image is converted from spatial domain to frequency domain using HDWT. The pay load is encrypted and converted into bit stream. The payload bit stream is first embedded into approximation band and remaining bits if any are embedded in the detailed bands to generate stego image in wavelet domain. Inverse wavelet transform is applied to get the stego image in spatial domain. The embedding algorithm for SSCBH is as shown in Table I.

TABLE I: Embedding algorithm

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Input: Cover Image (CI), Payload (PI)

Output: Stego Image(SI)

1. The Cover Image is resized to 512 x 512.
2. Consider the payload of size less than resized cover image.
3. HDWT is applied on to the cover image to generate subbands.
4. In permutation stego key is generated using 1+8k to 4+8k for encryption and decryption.
5. The pixels are arranged in column wise to generate binary stream.
6. The 4 LSB of payload image image is embedded into the 4 MSB of cover image.
7. IDWT is applied to get stego image

Extracting Algorithm: The extracting algorithm for SSCBH is given in Table II.

TABLE II: Extracting algorithm

Input: Stego image

Output: Payload

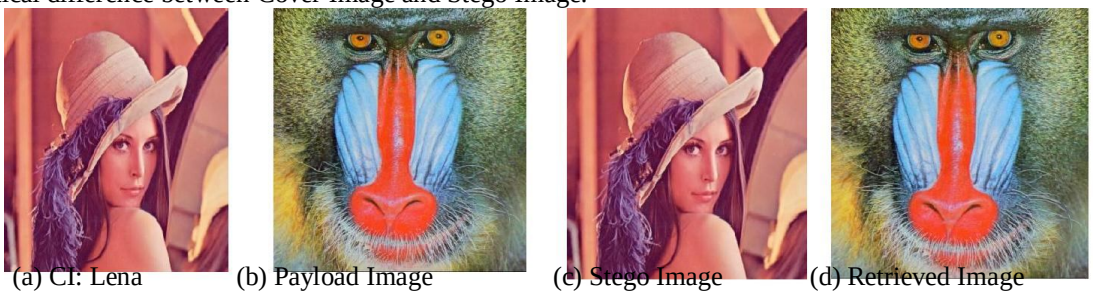
1. DWT is applied on stego- image to generate four subbands.
2. Permutation is applied and same stego key is considered.
3. The hidden bits from the cover image are extracted from MSB of the cover image.
4. The extracted bits are put into LSB bits of payload, rest of the bits are padded with zeros.
5. The payload image is successfully extracted from the stego-image.
6. PSNR and MSE are calculated for different payloads and cover images.

IV. RESULT ANALYSIS

The cover image (CI) of Lena, Forest and Mandril and payload image (PI) of Mandril, Pepper and Parrot are considered for performance analysis of the algorithm. Fig. 3, 4, 5 shows that the payload image is embedded into cover image of different images

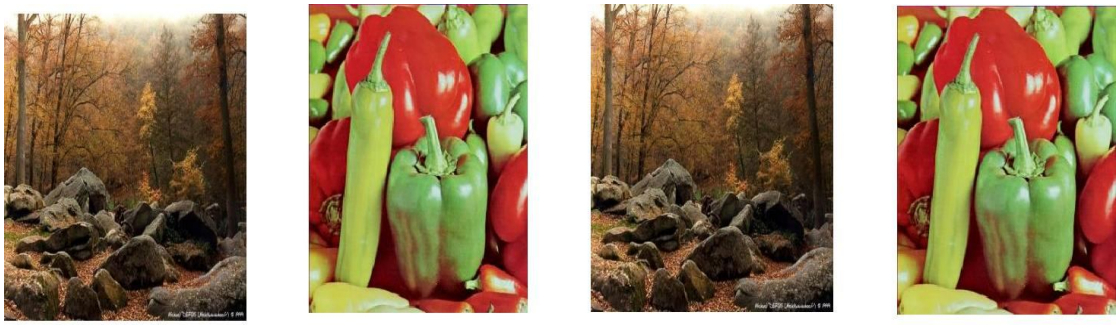
Volume 5 Issue I, January 2017
ISSN: 2321-9653

to generate stego image (SI). It is observed that appearance of stego image is almost same as the cover image and there is no statistical difference between Cover Image and Stego Image.



(a) CI: Lena (b) Payload Image (c) Stego Image (d) Retrieved Image

Fig.3 Lena Image and Mandril Image



(a) CI:Forest (b) Payload Image (c) Stego Image (d) Retrieved Image

Fig.4 Forest Image and Pepper Image

a) CI:Mandril (b) Payload Image (c) Stego Image (d) Retrieved Image

Fig.5 Mandril Image and Parrot Image

TABLE III

Variation of PSNR and MSE of Cover Image (Lena) (512*512) for the increase of Payload Image sizes (Mandril).

SL.No	Size of Payload	PSNR	MSE
1	90 x 90	44.25	1.56

Volume 5 Issue I, January 2017
ISSN: 2321-9653

2	110 x 110	43.08	1.78
3	130 x 130	42.05	2.01

TABLE IV

Variation of PSNR and MSE of Cover Image (Forest) (512*512) for the increase of Payload Image sizes (Pepper).

SL.No	Size of Payload	PSNR	MSE
1	90 x 90	44.13	1.77
2	110 x 110	42.39	1.93
3	130 x 130	41.62	2.11

TABLE V

Variation of PSNR and MSE of Cover Image (Mandril) (512*512) for the increase of Payload Image sizes (Parrot)

SL.No	Size of Payload	PSNR	MSE
1	90 x 90	43.32	1.73
2	110 x 110	42.52	1.90
3	130 x 130	41.69	2.09

Table III, IV and V shows the variation of PSNR and MSE for the increase of payload image sizes. It is observed that the value of PSNR is high for the payload size of 90 x 90. The value of PSNR is decrease with increase in payload size. The value of PSNR is high for the payload size of 90 x 90 due to use of BPCS and HDWT Technique.

V. CONCLUSION

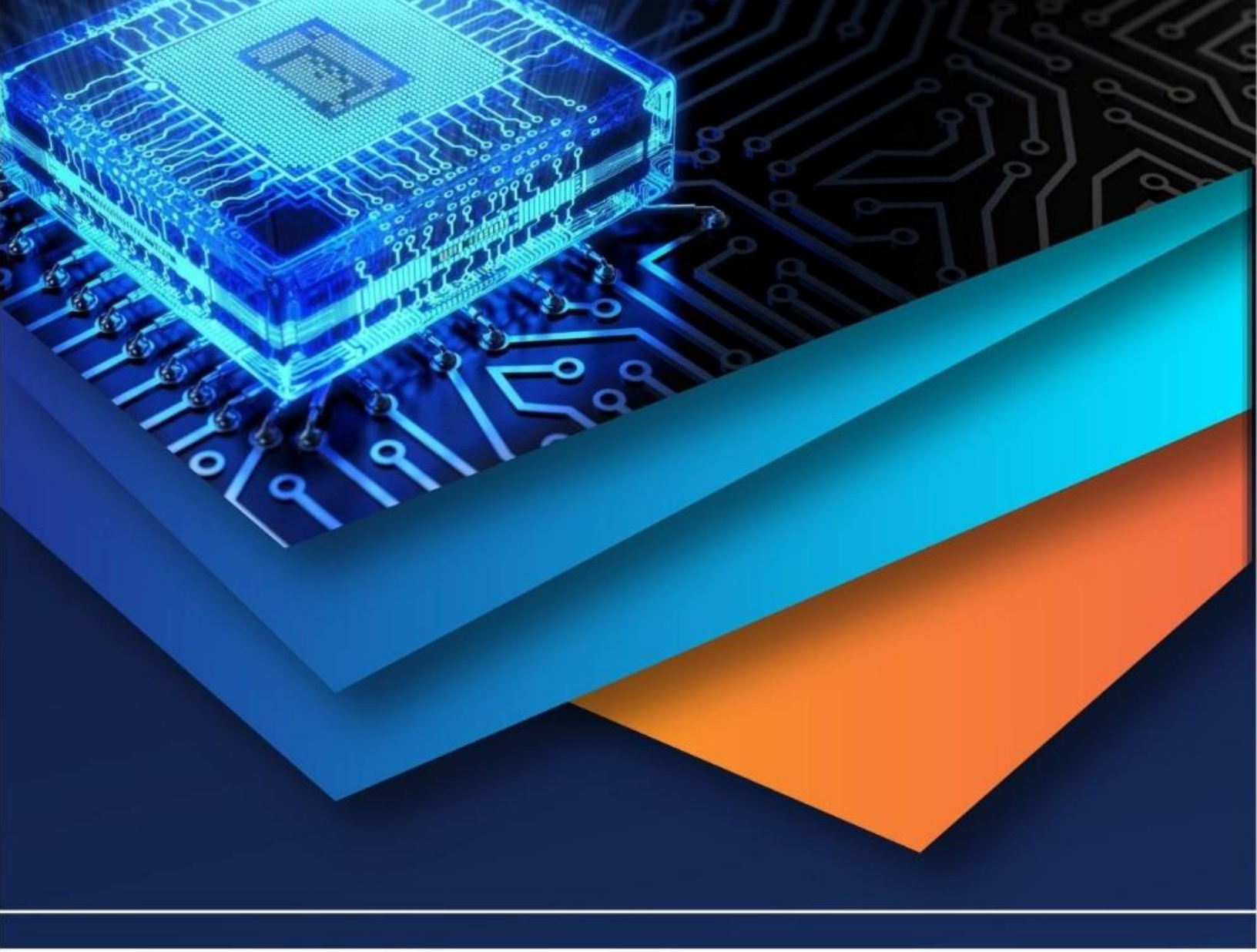
Steganography is a method of transporting significant information from one place to another place through open channel in the covert manner. The digital images are commonly used as a cover image for Steganopgraphic techniques. In this paper we proposed a image Steganography using BPCS and HDWT. The HDWT is applied on each bit plane of the Cover Image to generate four subbands. The HH subband of cover image is used to embed the 4-LSB bits of payload. The stego key is generated using permutation and which is used to extract the payload. The value of PSNR is high for the payload image of size 90 x 90 for all images due to the use of BPCS and HDWT.

VI. ACKNOWLEDGMENT

We are grateful to the Management and Principal, Global Academy of Technology, Bengaluru, Affiliated to Visvesvaraya Technological University, Belagavi, for providing the facilities and inspirations to carry out Research work.

REFERENCES

[1] Pramendra Kumar and Vijay Kumar Sharma, "Information Security Based on Steganography &Cryptography: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, pp. 246-250, 2014.
[2] Apoorva Shrivastava and Lokesh Singh, "A new hybrid encryption and Steganography technique: a survey", International Journal of Advanced Technology and Engineering Exploration, Volume 3, Issue 14, pp. 8-13, 2016.
[3] T.Pandikumar and Tesfay Gebreslassie, "Information Security using Image based Steganography", International Research Journal of Engineering and Technology Research, Volume 3, Issue 6, pp. 2839-2844, 2016.
[4] A. Prabhune and S. M. Joshi, "Information Hiding Techniques for Data Security using FPGA", International Journal of Adavnced Research in Computer science and Software Engineering , Volume 6 Issue 1, pp. 226-230, 2016.
[5] Kirti D. Nagpal, Vijay R. Wadhankar and D. S. Dabhade, "Performance Evaluation of image Steganography using Hybrid technique in frequency Domain", International Journal on Future Revolution in computer science and communication Engineering, Volume 1 Issue 4, pp. 011-015, 2015.
[6] R. Rejani, D. Murugan and Deepu V. Krishnan, "Digital Data Protection using Steganography", ICTACT Journal on Communication Technology Advanced Technology and Engineering Exploration, Volume 7, Issue 11, pp. 1245-1254, 2016.
[7] S. Y. Kanawade, Anupam Kumar, Vikas Nagare and Swapnil Dhakane, "Secured Wireless Communication through Zigbee using Cryptography and Steganography", International Journal for Innovation in Science and Technology, Volume 2, Issue 11, pp.686-688, 2016.
[8] Dhanya Job and Varghese Paul, "An Efficient Video Steganography Technique for Secured Data Transmission", International Conference on data mining and Advanced Computing, pp. 298-305, 2016.
[9] Vedanti M Khandare, Siddharth A. Ladhake, and U.S. Ghate, "An Approach of ECG Steganography to Secure the Patient's Confidential Information", International Research Journal of Engineering and Technology, Volume 3, Issue 3, pp. 1867-1871, 2016.
[10] Essam H. Houssein, Mona A. S. Ali and Aboul Ella Hassanien, "An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System", IEEE International Conference on Computer science and Information systems, pp. 641-644, 2016
[11] K.S.Seethalakshmi, Usha B A and Sangeetha K N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", International Conference on Computational Systems and Innovation Systems for sustainable Solutions, pp. 396-403, 2016.
[12] Sandip Bhasme, Arvind Abu, Kaustubh Gandhi and Ritu Phadnis, "Visual Cryptography and Stegaographic techniques for secure E-Payment Systems", International Research Journal of Engineering and Technology, Volume 3, Issue 3, pp. 1018-1021, 2016.
[13] Utsav Sheth and Shiva Saxena, "Image Steganography sing AES Encryption and Least significant Nibble", International Conference on Communication and Signal Processing, pp. 876-879, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY