Hybrid Domain based Steganography using BPS, LSB and IWT

H S Manjunatha Reddy
Global Academy of Technology/Department of ECE, Bangalore, India

K B Raja
University Visvesvaraya College of Engineering/Department of ECE, Bangalore University, Bangalore, India

ABSTRACT

The Steganography used to transport information from one place to other place through public channel in covert way. In this paper we propose Hybrid domain Steganography using BPS, LSB and IWT (HSBLI). The payload is decomposed into two equal parts say part 1 and part 2. The cover and payload (PL) part 1 pixel intensity value are observed and if intensity values are more than or equal to 128 then Bit Plane Slicing (BPS) algorithm is used to embed payload in to cover image. If the intensity values of cover image and PL part 1 are less than 128, square root is applied to compress 8 bit pixel length to 4 bit pixel length and LSB technique is used to replace PL part 1 value by cover image LSB values. The BPS stego object is merged with LSB stego object to obtain intermediate stego object. The IWT is applied on intermediate stego object to derive four sub bands. The PL part 2 is considered and embedded into LL sub band of intermediate stego object using LSB replacement method to obtain final stego object. The inverse IWT is applied on final stego object to get stego image in spatial domain. The payload is extracted at the destination by applying reverse process of embedding. It is observed that the values of PSNR better in the case of proposed algorithm compare to existing algorithms.

Keywords

Steganography, BPS embedding, IWT, Payload, Cover Image.

1. INTRODUCTION

The growing possibilities of modern Communications and use of Internet needs special means of security especially on computer network. The network security is becoming more important task as the information transferred through internet increases. Therefore maintaining the confidentiality and data integrity is to require protecting against unauthorized access and use. In cryptography, important information is protected by scrambling the message which can arise suspicion for hackers. This necessitated the need for hiding intermediate stego object information rather than modifying the information. Steganography is the effective means of data hiding that protects data from unauthorized or unwanted persons. It works by hiding secret information into carrier object. The basic method used in steganography is that the secret message to be transmitted is embedded into a cover image by using a suitable algorithm and at the destination the data is retrieved by use of reverse embedding process. To increase security, the data can be encrypted before embedding and at the destination it can be decrypted. The cover object used can be image or a video file or even an audio file. Images are the most widely used covers, because of their inherent nature to provide high security, robustness and capacity since images has more redundant information.

Based on choosing the hiding medium, the steganographic techniques are classified as (i) Text-based Steganography: In this method the message to be sent is embedded in a text file by formatting it based on line shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the embedded content hence the technique is not robust. (ii)Audio Steganography: It alters the audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding. (iii) Image Steganography: It hides message in the digital images. This technique is the most popular because of the fact that almost no perceivable changes occur in images after hiding a large amount of data with wide variety of available images. (iv) Document based steganography: It embed the data in document files by adding tabs of spaces to text or doc files. (v) File structure based steganography: It embeds secret data in the redundant bits of cover file. The method is immune to visual attack and the statistical detection.

The steganography is categorized into (i) Spatial domain steganography which mainly includes LSB steganography and Bit Plane Complexity Segmentation (BPCS) algorithm. Spatial domain is frequently used because of high capability of hidden information and easy realization. (ii) Transform domain steganography: The secret information is embedded in the transform coefficients of the cover image. Discrete Cosine Transform, Discrete Wavelet Transform and Discrete Fourier Transform are examples of transform domain. The advantages of transform domain techniques are high ability to tolerate noises and some signal processing operations. But transform domain techniques are computationally complex and hence slower. (iii) Hybrid domain: It is a combination of both Spatial and Transform domain. The part of cover image and payload image are converted into transform domain and remaining part of cover image and payload are retained in the spatial domain itself

Steganography can be used for wide range of applications such as defence organisations for safe circulation of secret data, intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient’s details are embedded within image providing protection of information and reducing transmission time and cost, online voting system so as to make the online election secure and robust against a variety of fraudulent behaviours, for data hiding in countries where cryptography is prohibited, improving mobile banking security, tamper proofing so as to prevent or detect unauthorised modifications and other numerous applications.

Contribution: In this paper HSBLI algorithm is proposed. The payload is decomposed in to two equal parts say part 1 and part 2. The PL part 1 is embedded into cover image based on BPS embedding and LSB embedding with square root depends on intensity value of PL part 1 and cover image to derive BPS and LSB stego objects. The intermediate stego object is derived by merging BPS and LSB stego objects and IWT is applied. The PL part 2 in spatial domain is embedded into LL band of intermediate stego object using LSB technique to get final stego object.

Organization: This paper is organized into following sections. Section 2 is an overview of related work. The steganography definitions, proposed embedding model and extraction model are discussed in section 3. The algorithms used for embedding and extracting are discussed in section 4. In section 5 Performance analyses are discussed.

2. LITERATURE SURVEY

Eiji Kawaguchi and Richard Eason [1] have proposed Principle and applications of Bit Plane Complexity Segmentation (BPCS) Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans cannot see any information in the bit planes of an image if it is very complex. The bit planes of a natural image are divided as informative areas and noise like areas by the complexity threshold. The complex regions are replaced with secret information in the bit planes of a natural image without changing the image quality. Sarreshtedari S and Ghammaghami, [2] have proposed high capacity image steganography in wavelet domain which works on the wavelet transform coefficients of the original image to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding. Kumar V and Kumar D [3] have proposed Performance Evaluation of DWT Based Image using the Discrete Wavelet Transform for hiding the secret message into the higher frequency coefficient of the wavelet transform while leaving the lower frequency coefficient sub band unaltered. In contrary, steganalysis is a process of detecting the secret communication, against Steganography. R O El Safy et al., [4] have proposed an adaptive steganographic technique based on integer wavelet transform in which the bits of the payload are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm.

Shrikant S. Khaire and Sanjay L. Nalbalwar [5] have proposed Steganography with Bit Plane Complexity Segmentation (BPCS) technique in which the binary image is divided into informative and noise like region. The secret data is hidden into noise like region of the vessel image without any deterioration. Marghny Mohamed and Mohamed Bamatraf [6] have proposed Data Hiding by LSB Substitution using Genetic Optimal Key-Permutation. Both normal and optimized methods are tested with standard images, varying both data size as well as key space. Rohini Sharma and Ekta Walia [7] have proposed Analysis of non adaptive and adaptive edge based LSB Steganography for colored images used for edge based LSB steganography. Both these algorithm have been slightly modified for colored image implementation and are compared on the basis of various evaluation parameters like PSNR and MSE.

Rupinder Kaur et al., [8] have proposed efficient approach towards steganography uses shared key between the sender and the receiver. The image is used only to encode text and the index array generated after encoding. There is no need to compare the original and encoded image because there is no change in the image used. To increase the complexity of the index array divide and mean method are applied. Joyshree Nath and Sankar Das [9] have proposed advanced steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2 and LSB+3 bits in non standard Cover Files. The secret message is encrypted and hidden in some standard cover files such as .exe, .com, .pdf, .doc, .xls, .ppt files using LSB replacement method. The size of the secret message must be small compared to the cover file. This method increases the capacity. Lifang Yu et al., [10] have proposed improved adaptive LSB steganography based on chaos and genetic algorithm.. This method improved adaptive LSB steganography, which can achieve high capacity while preserving the first order statistics. Secondly, in order to minimize visual degradation of the stego image, shuffle bit order of the message based on chaos whose parameters are selected by the genetic algorithm.

Sanjive Tyagi and Ajay Agarwal [11] have proposed multi layers security scheme for embedding Secrets in cover image in which the image segmentation method has been introduced to decompose cover image into two regions, i.e., foreground and background region. Then hide encrypted text into background region of cover image using LSB Steganography algorithm. The proposed method is enhanced or characterised by robustness, larger amount of secret data, less time complexity and especially high security. Souvik Bhattacharya and Aparajit khan [12] have proposed Pixel Mapping Method based Bit Plane Complexity Segmentation Steganography. The proposed approach works by selecting the embedding the bit planes using mathematical function and then applies the pixel mapping method in a 8x8 blocks of the each selected plane. The integrated approach of PMM and BPCS produces a robust image based steganography method which is independent of the nature of the data to be hidden and produces a stego image with minimum degradation.

Anita Christaline and Vaishali [13] have proposed Image Steganographic Techniques with Improved Embedding Capacity and Robustness. The method uses two steganographic techniques, one is the filter method and the other is wavelet transform method. Filter method used to embed the text information into image and discrete wavelet transforms method to increase the security. Ramani et al., [14] have proposed Steganography using BPCS to the integer wavelet transformed image in which the data hiding is realized in bit planes of sub band wavelets coefficients obtained by using the integer wavelet transform. The proposed system shows a high data hiding capacity.

El-Sayed M, et al., [15] have proposed Comparative Study of Pixel Value Differencing (PVD) based schemes for Data Hiding in Digital Images that depend on the pixel value differencing scheme. PVD approach indicates the pixels that may support larger changes in their least significant bits. This allows increasing the embedding capacity without significant quality loss. Elham Ghasemi et al., [16] have proposed Steganographic method based on Integer Wavelet Transform and Genetic Algorithm. The scheme embeds data in integer wavelet transform coefficients by using a mapping function based on Genetic Algorithm in an 8x8 block on the cover image. The optimal pixel adjustment process is applied after embedding the message. Integer wavelet transform avoids the floating point precision problems of the wavelet filter. Optimal Pixel Adjustment Process is used to reduce the difference error between the cover and the stego image and to increase the hiding capacity with low distortions respectively.

Siva Janakiraman et al., [17] have proposed Pixel Bit Manipulation for Encoded Hiding in spatial domain, to improve Imperceptibility, Security and payload using specialized Encoder/Decoder circuit for gray image. In this proposed method, a maximum of 1 or 2 bits has been altered to embed 4 bits of secret data. Furthermore this method would not just embed secret data in Least Significant Bits, it might be embedding the data in 1, 2, 3 and 5 or any one of the 15 possible combinations. Yedla dinesh and Addanki purna ramesh [18] have proposed Efficient Capacity Image Steganography by using Wavelets based on the haar and daubechies wavelet transform coefficients of the original image to embed the secret image. Here discrete wavelet transforms is used to transform the both original image and secret image. Discrete wavelet transforms allows perfect embedding of the hidden message and reconstruction**.** This scheme can provide an efficient capacity for data hiding without sacrificing the original image quality.

3. PROPOSED MODEL

In this section, the definitions and proposed model are discussed.

3.1 Definitions of Performance Analysis:

3.1.1 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. Capacity is represented by bits per pixel (bpp) using Equation 1.

$$Capacity = \frac{No\ of\ bits\ per\ pixel\ in\ payload image}{No.\ of\ bits\ per\ pixel\ in\ \mathrm{cov}er\ image} \quad (1)$$

3.1.2 Mean Square Error (MSE): It is defined as the square of error between cover image and the stego image. The distortion in the image can be measured by using Equation 2.

$$MSE = \sum_{i=1}^{all\ pixels} \sum_{j=1}^{all\ pixels} \frac{[C(i,j) - S(i,j)]^2}{N * N} \quad (2)$$

Where C (i, j) is the cover image pixel
S (i, j) is the stego image pixels
N ∗ N is the image size.

3.1.3 Peak Signal to Noise Ratio (PSNR): It is the ratio of the maximum signal to noise between stego image and cover image can be measured in db using Equation 3.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (3)$$

3.2 Proposed Model

The payload is embedded into cover image using LSB, BPCS and IWT to generate stego image with high PSNR and Capacity.

3.2.1 Embedding Model

The block diagram of embedding model is shown in Figure 1. The payload is more secure in the proposed model since

(i) The BPS embedding technique is used for cover image pixel intensity values more than or equal to 128.
(ii) The LSB embedding technique is used on square root intensity values less than 128 of PL part 1.
(iii) The IWT is applied on both BPS stego object and LSB stego object. The spatial domain PL part 1 is embedded into coefficient of transform domain stego object.

3.2.1.1 Payload (PL): The gray scale image of suitable sizes and different formats which is to be transmitted in covert way is considered as a payload.

3.2.1.2 Cover Image (CI): The cover image can either be color or grayscale image, provided color image is converted into gray scale image, before secret image is hidden. The cover images of any size and formats are considered.

3.2.1.3 Segmentation: The payload is equally decomposed into two parts say part-1 and part-2.

3.2.1.4 BPS Embedding [5]: The gray scale image is represented by pixels with intensity values vary between zero and 255 with each pixel is represented by 8 bits. In bit plane slicing, the eight bits of a pixel are split into its constituent binary planes varying from MSB to LSB. For example, the gray scale matrix of size 4*4 is converted into 8 matrices of single bit planes using bit plane slicing as shown in Figure 2.

The part 1 of payload and cover image is considered and the intensity values of each pixel is observed and if intensity value of a pixel is greater than or equal 128, then consider those pixels for BPS embedding. The intensity values greater than or equal 128 of both PL part 1 and cover image are split in 8 bit planes using BPS. The four LSB bit planes of cover image are replaced with four MSB bit planes of PL part 1 respectively to generate BPS stego object. The eight bit planes of BPS stego object are merged to obtain single BPS stego object with 8 bits per pixels.

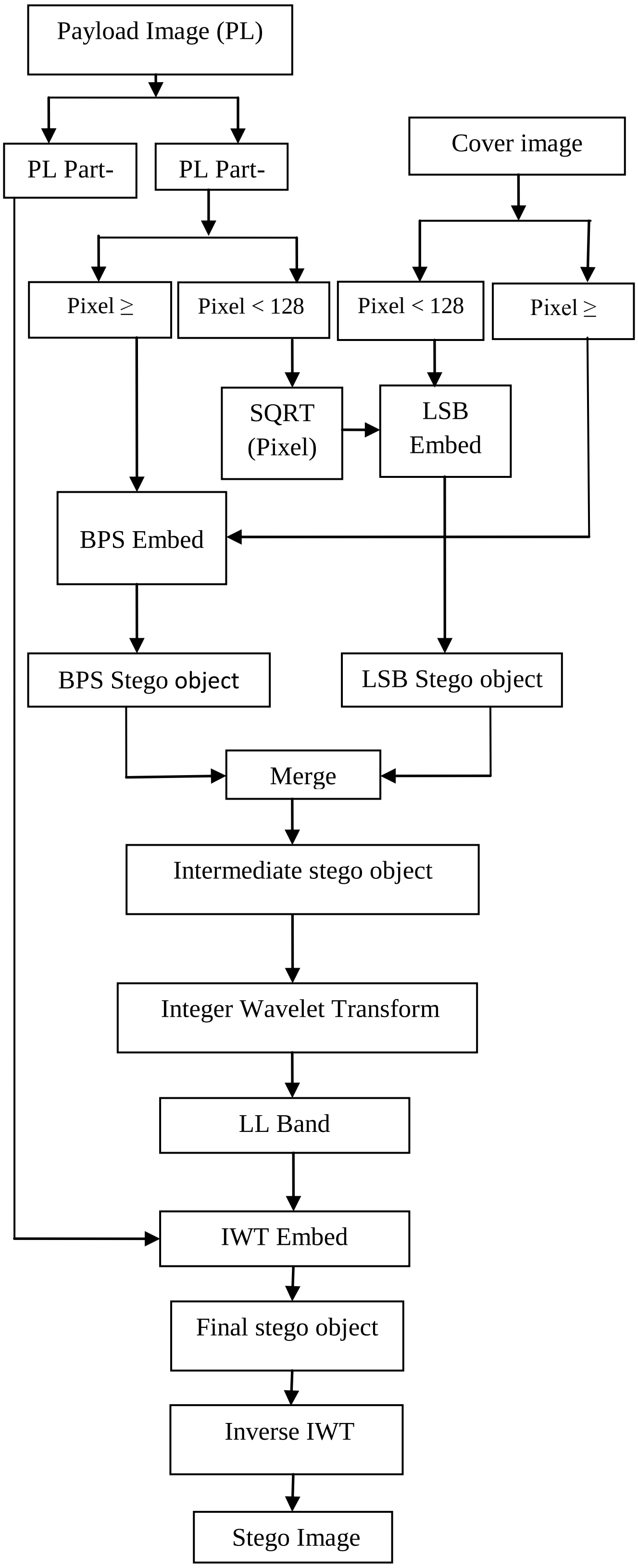


Fig 1: Flowchart for embedding system of HSBLI.

$$\begin{bmatrix} 98 & 255 & 55 & 28 \\ 00 & 127 & 48 & 128 \\ 128 & 212 & 240 & 11 \\ 212 & 171 & 130 & 161 \end{bmatrix}$$

(a)

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

(b) (c) (d) (e)

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

(f) (g) (h) (i)

Fig 2: (a) Original matrix, (b)-(i) Constituent bit plane of (a)

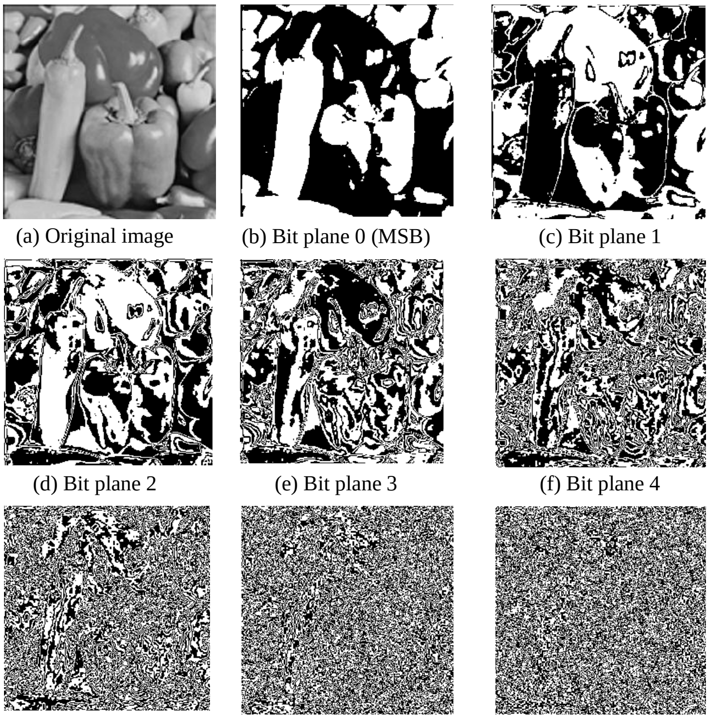

(a) Original image (b) Bit plane 0 (MSB) (c) Bit plane 1
(d) Bit plane 2 (e) Bit plane 3 (f) Bit plane 4
(g) Bit plane 5 (h) Bit plane 6 (i) Bit plane 7 (LSB)

Fig 3: BPS Technique

The BPS is applied an image Pepeer.jpg to derive corresponding binarized 8 bit planes as shown in Figure 3. The MSB bit plane image has significant information of original image compare to other 7 bit plane images. The LSB bit plane image has no information/insignificant information of original image.

3.2.1.5 LSB Embedding: The intensity values of each pixel of PL part 1 and cover image are observed and if intensity values are less than 128, then consider the pixels for LSB embedding. The square root is applied on each pixel value of PL part 1to compress 8 bits into 4 bits. The four LSB bits of cover image pixels are replaced by four bits of PL part 1 to generate LSB stego object.

3.2.1.6 Merge: BPS Stego object and LSB Stego object are added to generate intermediate stego object.

3.2.1.7 IWT Embedding: The two- dimensional integer wavelet transform is applied on intermediate stego object to generate four sub bands such as LL, LH, HL, and HH. The LL band represents the low frequency coefficients and three other bands represent the high frequency coefficients. The PL part 2 is embedded into the LL band coefficients using 4 bit LSB replacement method. The four MSB's of PL part 2 are embedded into four LSB bits of LL band coefficient of intermediate stego object to generate final stego object. The inverse IWT is applied on final stego object to derive stego image in spatial domain.

3.2.2 Proposed Extraction Model

The embedded payload is extracted from stego image at the destination by applying reverse process of embedding. The extraction model is as shown in Figure 4. The IWT is applied on stego image to generate four sub bands say LL, LH, HL and HH. The four LSB coefficient of LL band has the MSB bits of PL part 2, hence extract to get PL part 2. The inverse IWT is applied on MSB coefficients of LL band along with all three sub bands LH, HL and HH to generate intermediate stego image. The intensity values of intermediate stego image are observed, if values are less than 128 then apply square to decompress to generate pixel length to 8 bits. The four MSB's are extracted to generate part of PL part 1. If pixel values are more than or equal to 128 then apply BPS to generate 8 bit planes. The four LSB bit planes are considered to obtain MSB part of PL part 1. The matrix of part of PL part 1 of LSB method is merged with the matrix of part of PL part 1 BPS method to derive final PL part 1 image. The final PL part 1 image is merged with PL part 2 images to extract original payload.

4. ALGORITHM

Problem definition: The payload is embedded into cover image using BPS, LSB and IWT to generate stego image for secure communication

The objectives are

(i) To increase capacity
(ii) To increase PSNR

Assumptions:

(i) Both cover and payload objects are gray scale images with different dimensions and formats.
(ii) The stego image is transmitted over an ideal channel.

4.1Embedding algorithm: The payload is embedded into the cover image using spatial domain and transform domain techniques are given in the table 1. The proposed stegnography algorithm is more secured as three different techniques are used to embed payload along with some part of payload and cover image are compressed.

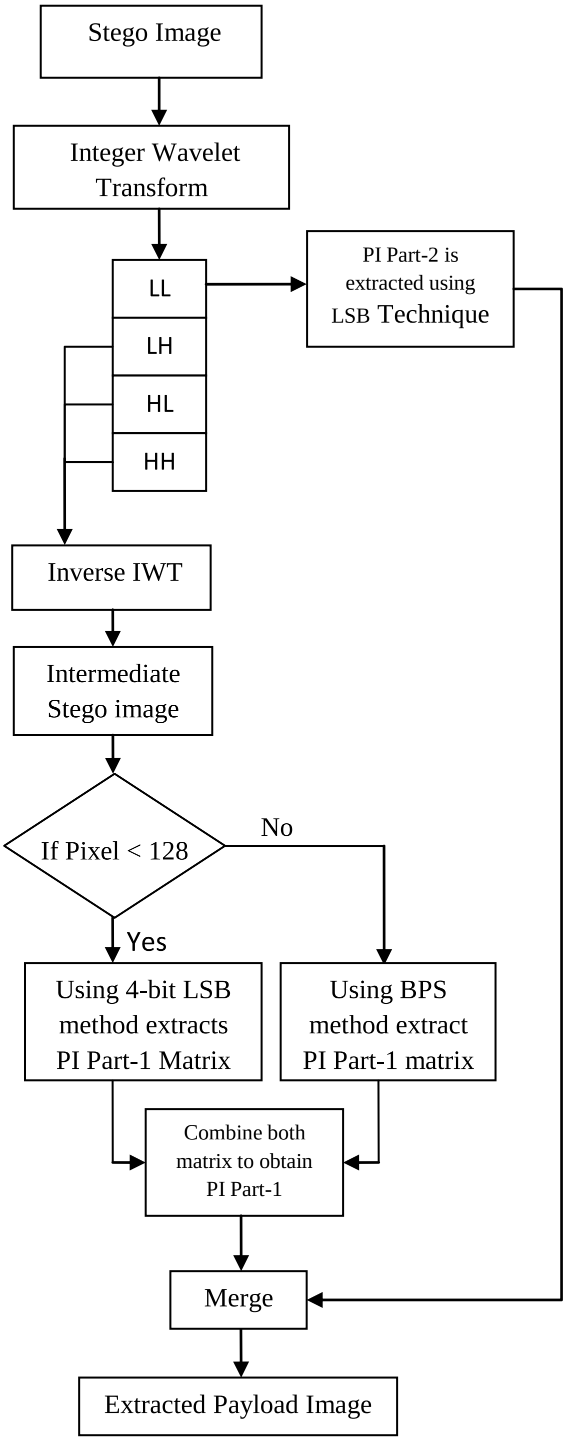

Stego Image
Integer Wavelet Transform
LL
LH
HL
HH
PI Part-2 is extracted using LSB Technique
Inverse IWT
Intermediate Stego image
If Pixel < 128
No
Yes
Using 4-bit LSB method extracts PI Part-1 Matrix
Using BPS method extract PI Part-1 matrix
Combine both matrix to obtain PI Part-1
Merge
Extracted Payload Image

Fig 4: Flowchart of Extraction Process of HSBLI

Table 1: Embedding Algorithm of HSBLI

Input**:** Cover image and Payload
Output: Stego image.

1. Read the cover image and payload.
2. Decompose payload into PL part 1 and PL part 2.
3. Check intensity values of PL part 1 and cover image.
4. If intensity values less than 128 then apply square root to compress pixel length from 8 to 4 bits.
5. The 4 bits of cover image are replaced by 4 bits of PL part 1 to generate LSB stego object.
6. The BPS embedding is applied on pixels having intensity values greater than or equal to 128 of PL part 1 and cover image.
7. The 4 LSB planes of cover image are replaced by 4 MSB planes of PL part 1 and convert 8 bits per pixel to generate Bps stego object.
8. The intermediate stego object is obtained by merging BPS and LSB stego object.
9. IWT is applied on intermediate stego object and consider LL band.
10. The MSB bits of PL part 1 are embedded into four LSB's of LL band coefficient to generate final stego object.
11. Apply inverse IWT to generate stego image.

*4.2 Extracting Algorithm***:** The payload is extracted from the stego image by the reverse process of embedding as given in table 2.

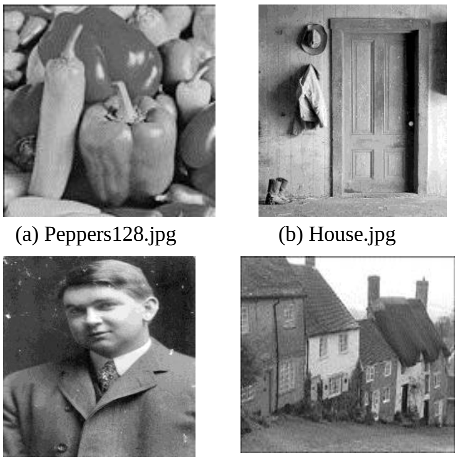
Table 2: Extracting Algorithm of HSBLI

Input : Stego Image
Output : Extracted Payload Image

1. Read the stego image.
2. IWT is applied to generate four sub bands and extract four LSB coefficient of LL band which has the MSB bits of PL part 2.
3. The inverse IWT is applied on MSB coefficients of LL band along with all three sub bands LH, HL and HH to generate intermediate stego image.
4. The intensity values of intermediate stego image are less than 128 then square it to decompress to generate pixel length to 8 bits
5. The four MSB's are extracted to generate part of PL part 1.
6. If pixel values are greater than or equal to 128 then apply BPS to generate 8 bit planes
7. The 4 LSB bit planes are considered to obtain MSB part of PL part 1.
8. Both LSB and BPS matrices are merged to derive final PL part 1 image.
9. The final PL part 1 image is merged with PL part 2 images to extract original payload.

5. PERFORMANCE ANALYSIS

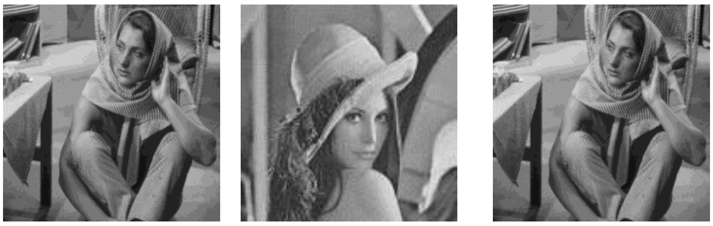
The several cover images such as peppers, house, old image and gold hill shown in Figure 5 and payload images of different sizes and different formats are considered for performance analysis. The payload Lena image is embedded in the cover image Barbara using proposed algorithm to generate stego image Barbara as shown in Figure 6. It is observed that perceptibility of stego image and cover image are same. The quality of stego image is same as cover image by appearance and also statistical characteristic of stego image is almost same as cover image, since the PSNR value in the proposed algorithm is more than 40 dB.



(a) Peppers128.jpg (b) House.jpg

(c) Old Image.jpg (d) Goldhill1.jpg

Fig 5: Cover images



(a) CI Barbara (b) Payload Lena (c) SI Barbara

Fig 6: CI, PL and SI

The PSNR values between cover image and stego image as well as PSNR values between original payload and extracted payload for different payload sizes with constant cover image size are tabulated in Table 3. The payload image Lena. jpg is embedded into cover image Barbara.bmp (512 * 512) to generate stego image Barbara.bmp. The PSNR of cover image and stego image values are decreases as capacity increases where as the PSNR values between payload and extracted payload are almost constant with respect to the capacity.

The variation of PSNR between cover image and stego image with capacity are plotted in the Figure 7. The PSNR values decreases as capacity increases. The variation of PSNR of cover image Barbara.bmp (512*512) and stego image Barbara.bmp (512*512) and PSNR between original payload with different image formats having size of 64*64 with extracted payload are tabulated in Table 4. It is observed that the payload formats does not affect the quality of stego image i.e., PSNR between cover image and stego image having value around 43 dB and the PSNR between original payload and extracted payload having value of around 31 dB are almost constant for different payload image formats.

The PSNR value between cover image & stego image and payload & extracted payload for different cover image formats with constant capacity are given in Table 5. It is seen that different cover image formats has least effect on the quality of stego image as PSNR values are almost constant. The PSNR value between cover & stego image and payload & extracted payload for different cover images is almost constant are given in Table 6.

Table 3: PSNR Variations for different payload sizes with cover Image Barbara.bmp (512 x512)

Payload Image size[lena.jpg]	PSNR of CI and SI	Capacity	PSNR of PL and EPL
64 X 32	45.8296	0.0078	30.9900
64 X 64	42.7816	0.0156	30.7907
64 X 128	39.7085	0.0313	30.8540
128 X 128	36.6551	0.0625	30.7849
128 X 256	33.6315	0.125	30.8326

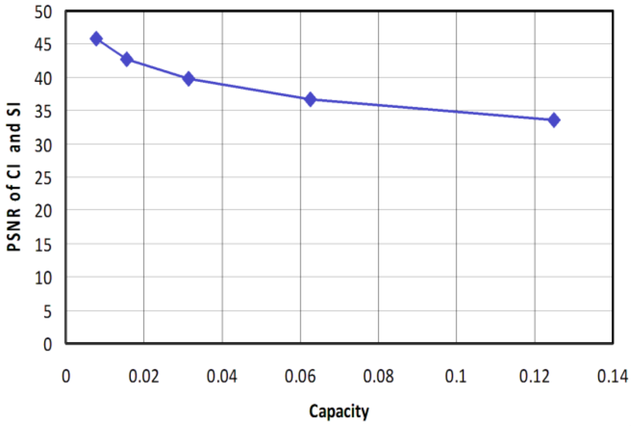


Fig 7: PSNR variations with Capacity

Table 4: PSNR Variations for different payload formats with cover image Barbara.bmp (512 x 512)

Payload Image formats Lena(64 x 64)	PSNR of CI and SI	PSNR of PI and EPL
Png	42.8781	30.4224
Jpg	42.7816	30.7907
Bmp	42.9250	30.3722
Tif	42.9215	30.5171
Gif	42.9198	30.4496

Table 5: PSNR Variations for different cover image formats with payload image Lena.jpg (64 x 64)

Cover Image formats	PSNR of CI and SI	Capacity	PSNR of PL and EPL
Bmp	42.5629	0.0156	29.6189
Tif	42.5753	0.0156	29.6189
Gif	42.5906	0.0156	29.6189
Png	42.9973	0.0156	29.6189
Jpg	43.4194	0.0156	29.6189

Table 6: PSNR values for different cover images

Cover image (512 x 512)	Payload (64 x 64)	PSNR (CI & SI)	PSNR(PL & EPL)
Goldhill1.jpg	Lena.png	41.276	30.96
House.jpg	Lena.png	42.719	30.962
Old Image.jpg	Lena.png	42.6646	30.837
Peppers128.jpg	Lena.png	42.5471	29.05
Barbara.bmp	Lena.png	42.8781	30.422

Table 7: Comparison of PSNR for existing and proposed technique

Methods	PSNR
El.Sayed M El. Alfy et.al [15]	38.354
Elham Ghasemi et.al.[16]	35.17
Sivajanakiraman et.al.[17]	34.8605
Yedla Dinesh and Addanki Purna Ramesh [18]	26.30
Proposed method	43.4194

The value of PSNR for existing methods and proposed HSBLI method are compared in Table 7. It is observed that the value of PSNR is better in the case of proposed algorithm compared to existing algorithms. The security to the payload in the propose algorithm is better since (i) Spatial domain and Transform domain concepts are used (ii) The part of the payload is compressed using square root before embedding.

6. CONCLUSION

The Steganography is covert communication to protect confidential information. In this paper HSBLI is proposed. The cover image and PL part 1 intensity values are observed and the intensity values more than or equal to 128 are used for BPS embedding to generate BPS stego object. The intensity values of PL part 1 and cover image are less than 128 are considered and applied square root on each pixel value of PL part 1 to convert 8 bits length to 4 bits. The 4 bits of cover image are replaced by 4bits of PL part1 to generate LSB stego object. The intermediate stego object is obtained by merging both BPS and LSB stego object. The IWT is applied on intermediate stego object. The spatial domain PL part 2 is embedded into LL sub band of intermediate stego object to derive final stego object. The inverse IWT is applied on final stego object to derive stego image in spatial domain. The payload is extracted at the destination by applying reverse process of embedding. It is observed that the values of PSNR are better in the case of proposed algorithm compare to existing algorithm. In future the embedding technique can be verified with Dual Tree Complex Wavelet Transformation.

7. REFERENCES

[1] Eiji Kawaguchi and Richard O. Eason “Principle and Applications of BPCS-Steganography,” Proceedings of SPIE: Multimedia Systems and Applications, Vol.3528, pp.464-463, 1998.

[2] Sarreshtedari S and Ghaemmaghami S, “High Capacity Image Steganography in Wavelet Domain,” International Conference on Consumer Communications and Networking, pp.1-6, 2010.

[3] Kumar V and Kumar D, “Performance Evaluation of DWT Based Image Steganography,” IEEE International Conference on Advance Computing, pp. 223-228, February 2010.

[4] R O El Safy, H H Zayed and A El Dessouki “An Adaptive Steganographic Technique Based on Integer Wavelet Transform,” International Conference on Networking and Media Convergence, pp.111-117, March 2009.

[5] Shrikant S. Khaire and Sanjay L. Nalbalwar “Review: Steganography-Bit Plane Complexity Segmentation

Technique," International Journal of Engineering Science and Technology, Vol.2 (9), pp. 4860 – 4868, 2010.

[6] Marghny Mohamed and Mohamed Bamatraf, "Data Hiding by LSB Substitution using Genetic Optimal Key-Permutation," International Arab Journal of e-Technology, Vol-2, No.1, January 2011.

[7] Rohini Sharma and Ekta Walia, "Analysis of Non-Adaptive and Adaptive Edge based LSB Steganography for Colored Images," International Journal of Computing and Business Research, Vol-2, 2011.

[8] Rupinder Kaur, Mandeep Kaur and Rahul Malhotra "A New Efficient Approach towards Steganography," International Journal of Computer Science and Information Technologies, Vol.2(2), pp 673-676 , 2011.

[9] Joyshree Nath and Sankar Das "Advanced Steganographic Approach for Hiding Encrypted Secret Message in LSB, LSB+1, LSB+2 and LSB+3 bits in Non Standard Cover Files," International Journal of Computer Applications , Vol. 14, No.7, pp 31-35, February 2011.

[10] Lifang Yu, Yao Zhao and Rongrong Ni "Improved Adaptive LSB Steganography based on Chaos and Genetic Algorithm," Journal on Advances in Signal Processing, pp. 1-6 , 2010.

[11] Sanjive Tyagi and Ajay Agarwal, " Multi layers Security Scheme for Embedding Secrets in Stego image," International Journal of Advanced Engineering Sciences and Technologies, Vol.3 Issue. 1, pp. 029-033, 2011.

[12] Souvik Bhattacharya and Aparajit Khan "Pixel Mapping Method (PMM) based Bit Plane Complexity Segmentation (BPCS) Steganography," World Congress on Information and Communication Technologies, pp. 36-41, 2011.

[13] J.Anita Christaline and D.Vaishali, "Image Steganographic Techniques with Improved Embedding Capacity and Robustness," International Conference on Recent Trends in Information Technology, pp. 97-101 june, 2011.

[14] K Ramani, E V Prasad and S Vardarajan "Steganography using BPCS to the Integer Wavelet Transformed Image," International Journal of Computer Science and Network Security, vol. 7, No.7, July 2007.

[15] El-Sayed M. El-Alfy, Azzat A. and Al-Sadi "A Comparative Study of PVD-Based Schemes for Data Hiding in Digital Images," IEEE International Conference on Computer Systems and Applications, pp. 144-149, 2011.

[16] Elham Ghasemi, Jamshid Shanbehzadeh and Bahram Zahir Azami "A Steganographic Method Based on Integer Wavelet Transform and Genetic Algorithm," International Conference on Communications and Signal Processing, pp. 42-45, 2011.

[17] Siva Janakiraman, Anitha Mary A and Jagannathan Chakravarthy, "Pixel Bit Manipulation for Encoded Hiding - An Inherent stego," International Conference on Computer Communication and Informatics pp. 1-6 Jan 2012.

[18] Yedla Dinesh and Addanki Purna Ramesh, **"**Efficient Capacity Image Steganography by Using Wavelets," International Journal of Engineering Research and Applications, vol. 2, issue 1, pp.251-259 Feb 2012.