ISSN 2229-5518

Steganography based on Adaptive Embedding of Encrypted Payload in Wavelet domain

H S Manjunatha Reddy, K B Raja

Abstract— Steganography is the method of hiding the secrete message in a cover object for covert communication. In this paper we propose Steganography based on Adaptive embedding of Encrypted Payload in Wavelet domain (SAEPW). The LWT2 (dB2) is applied on cover image and only XD band is considered for embedding. The XD band is further decomposed into three blocks say XD0, XD1 and XD2. The payload of different sizes and formats are considered and segmented into two blocks namely block1 and block2. The LWT2 (Harr) is applied on payload block2 to generate wavelet sub bands and considering only XA band. The payload block1 pixel values and block2 XA coefficients are scaled down using key1 and key2 to represent each value by only three bits in binary. Key1 and key2 values are embedded in XD0 of cover image. The scaled down values of payload block1 and block2 are embedded into XD1 and XD2 of cover image respectively to generate stego object. The ILWT2 (dB2) is applied on stego object to generate final stego image. At the destination the embedded payload is retrieved from the stego image by adopting reverse process of embedding. It is observed that the values of PSNR and capacity are better in the case of proposed algorithm compared to existing algorithm.

Index Terms— Stegnography, Stego Image, Payload, Cover Image, Adaptive, Encryption, LWT

1 INTRODUCTION

THE fast developments in resource sharing through network essentially require security. Secured communication is possible by using different techniques such as watermarking, cryptography, Steganography etc. Digital watermark is a perceptually transparent system which is inserted in digital data using an embedding algorithm and key. Digital watermarking is mainly used in copy right protection. Cryptography is the class of information security and associated with scrambling text into cipher text. The various techniques of Cryptography includes such as microdots, merging words with images, and other ways to hide information in storage or transit. Steganography is a technique of hiding confidential information in the cover media. In image steganography the cover media used is an image and confidential may be an image or text. Image is preferred compare to other media because it has more redundant information. The most commonly used cover media are text, audio files, video, images etc. The important aspects of steganography are Security, Capacity and Imperceptibility. The common image steganography techniques are (i) least significant bit insertion: The LSB of the cover image are replaced with the confidential information. (ii) Masking and filtering method: The specific masking algorithms or a mathematical formula is used to select specific pixels to embed the secret information. The secret information looks as an integral part of the cover image after embedding. (iii) Transform techniques: The cover image is converted into transform domain by applying transformation such as Discrete cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT) etc. and then embedding of confidential information into these transformed coefficients of the cover image.

The wavelet transform separates the high frequency and low frequency information on a pixel by pixel basis. DWT is preferred over DCT because image in low frequency at various levels can offer high resolution. The DWT is decomposed into Approximation band (LL), vertical band (LH), horizontal band (HL) and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients which contain significant part of the spatial domain image. The other bands called as detail bands consists of high frequency coefficients which contains the insignificant part and edge details of the spatial domain image. DWT will allow independent processing without significant perceptible interaction between them and hence making the process imperceptibility with more effective.

Applications of steganography are in digital copy right protection, digital media content surveillance, content authentication and covert communication involving industries like e-pressing, e- government, e- business etc.

Motivation: Due to increasing demand for privacy and security, a need for various data hiding techniques which lead to the development of several techniques for embedding and extraction. Steganography is powerful method of embedding secret information for covert communication.

Contribution: In this paper the steganography algorithm SAEPW is proposed. The payload is divided into block1 and block2. The block 2 is converted into wavelet domain. The coefficient values of block 1 and block2 are scaled down using key1 and key2. LWT2 (dB2) is applied on cover image and XD band is divided into XD0, XD1 and XD2. The key1 and key2 are embedded in XD0. The payload block1 and block2 are em-

- *H S Manjunatha Reddy, Department of ECE, Global Academy of Technology, Bangalore, India, PH-+919448681994. E-mail: manjunathareddyhs@rediffmail.com*
- *K B Raja, Department of ECE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India,*

bedded in XD1 and XD2 respectively.

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 analysis is discussed and conclusion and future work is discussed in section 6.

2 Related Work

JiFeng Huang, [1] has proposed a method to detect the location of pixels in which secret message embedding is performed using LSB techniques in a JPEG cover image. The quality index of the JPEG image is calculated depending on the cover image recovered and a comparison between stego image and cover image is performed. This comparison results in identification of locations, where embedding is done and even the length of the message can be determined. Nedal M. Kafri1 and Suleiman, [2] have developed a method to hide the confidential information in such a way that stego analysis becomes complicated. The cover image is transformed to frequency domain using DCT and depending on the message bits, the 4th bit of coefficient is modified and a corresponding modification is done on 1st, 2nd, 3rd and/or 5th bits of coefficients of cover image. This results in minimal changes in the cover image without any suspicions. Izadinia et al. [3] have proposed a method on the basis of predictive coding to perform simultaneous data embedding and quantization of error values using Quantization Index Modulation (QIM). Further a protection against histogram attacks is provided using a correction mechanism. This method is resistant to histogram attack with a good visual quality and robustness

Ghoshal and Mandal, [4] proposed authentication technique which demonstrates the colour image authentication technique in frequency domain based on the Discrete Fourier Transform (DFT). The DFT is applied on sub-image block called mask of size 2 × 2 for frequency components of corresponding spatial component. This transforms process done from beginning to end mask in row major order of the carrier image. Image authentication is done by hiding secrete message into the transformed frequency components of carrier image. Four secrete message bits are fabricated within the transformed real frequency component of each carrier image byte except the LSB of first frequency component of each mask. After embedding, a delicate re-adjust phase is incorporated in all the frequency component of each mask, to keep the quantum value positive and non fractional in spatial domain.
. Yicong zhou and Agaian, [5] introduced a encryption algorithm called Parameterized Logarithmic Image Processing (PLIP) addition. The original secret information is scrambled to change the image pixel locations. The scrambled secret information is embedded into the cover image using PLIP addition via specific parameters. Adel Almohammad and Chinea[6] proposed two steganography methods JSteg and JMQT are used to investigates the pros and cons of colour and grayscale versions of images when used as steganography covers. It evaluates the performance of both grayscale and colour versions of a given cover image when they are used with a given steganography method. As a result colour images are better than using grayscale images for data hiding. In order to increase the hiding capacity, chrominance components can be used for data hiding.

Elham Ghasemi et al., [7] presented an embedding algorithm using mapping function based on genetic algorithm. The cover image is divided into 8 x 8 blocks and transformed using IWT. The data is embedded into coefficients of cover image. Genetic algorithm and optimal pixel adjustment provides optimal mapping function to reduce the difference error between the cover and the stego image and to increase the hiding capacity with low distortion respectively. Yong Hong Zhang [8] implemented a digital image encryption using chaotic cryptography. The chaotic cryptography technique is used as a key cryptography. The extended chaotic sequences are generated using-rank rational Bézier curve.
. Swain [9] presented secure communication method by combining cryptography and image steganography. The confidential information is encrypted and embedded in sixth, seventh and eighth LSB location of darkest and brightest pixel which is randomly spread across. Weiming Zhang et al., [10] proposed to construct binary stego codes for LSB embedding in grayscale signals, which can be generated from a covering code by combining Hamming codes and wet paper codes. Performances of stego code families of structured codes and random codes are analyzed

Gopalan, [11] implemented a method of embedding data into color image for applications such as authentication of an employee carrying a picture identification card. color image is converted into a one dimensional signal red, green or blue. Audibly masked frequencies in one dimensional signal are determined for each segment. The confidential information is embedded by modifying the spectral power at a pair of commonly occurring masked frequencies. Cui-ling Jianget al., [12] presented a steganographic method based on modification of jpeg quantization tables. The cover image is divided into non overlapping 16 x 16 quantization table. The DCT coefficients are quantized by quantization table. Secret information is embedded into DCT coefficients of cover image. Yan-ping Zhang et al., [13] proposed a technique for information hiding into still digital images based on (7, 4) Hamming Code and Wet Paper Codes. It is by embedding seven secret bits into a pixel group of several cover pixels at a time, if that is unsuccessful then it embeds the first three secret bits into that pixel-group once again.

Septimiu Fabian et al., [14] proposed a technique states the usage of cryptographic algorithms Ron Rivest Adishamir Len Adleman (RSA) algorithm with asymmetric keys and Advanced Encryption Standard (AES) with symmetric key together with steganography. The combining of these three

techniques builds a robust steganography based communication system. The secret data is encrypted using AES with a strong key prior to being embedded using a steganographic algorithm. The key used for the data encryption uses a combination between a random generated sequence and a hash of the cover image's color information that remains untouched throughout the entire embedding process. Chen Gouxi et al., [15] proposed a scheme in which the cover image is marginalized and reconstructed through mathematical morphology and block markers, then embedding the secret message into the cover image successfully with F5 steganographic algorithm. The technique has advantages such as the small changes in image quality, strong ability in anti-attack, and the secret information can be extracted completely from the carrier image. Anita Christaline and Vaishali [16] proposed a technique comprising of two methods. First is filter method to embed text information into image .The second is the wavelet transform method which proves to be more secured than any other method of image steganography. Wien Hong and Tung Shou Chen [17] have proposed data-hiding method based on pixel pair matching and use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given information digit. Then the pixel pair is replaced by the searched coordinate to conceal the digit. Che-Wei Lee and Wen-Hsiang Tsai [18] have developed blind authentication method based on the secret sharing technique with a data repair capability for grayscale images via the use of the Portable Network Graphics (PNG) image. An authenticated signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares using the secret sharing scheme. Lionel Fillatre [19] deals with the detection of hidden bits in the Least Significant Bit (LSB) plane of a natural image. The mean level and the covariance matrix of the image, chosen as a quantized Gaussian random matrix, are unknown. An adaptive statistical test is designed such that its probability distribution is always independent of the unknown image parameters, while ensuring a high probability of hidden bits detection.

3 MODEL

In this section definition of the evaluation parameters, proposed embedding and extraction models are discussed.

3.1. DEFINITIONS.

(i) Mean Square Error (MSE): It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE and it can be calculated using Equation 1.

$$MSE = \left[\frac{1}{N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N} \left(X_{ij} - \overline{X}_{ij}\right)^2 \quad (1)$$

Where N: Size of the image.

X_{ij} : The value of the pixel in the cover image.

$\overline{X}_{ij}$: The value of the pixel in the stego image.

(ii) Peak Signal to Noise Ratio (PSNR): It is the measure of quality of stego image as compared to cover image ie, the percentage of noise present in the stego image is given in an Equation 2.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \; db \quad (2)$$

(iii) Capacity: It is the size of the payload data that can be embedded into a cover image without deteriorating the integrity of the cover image. The steganographic 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) and calculated using Equation 3.

$$Capacity = \frac{P_{ij}}{C_{ij}} \quad (3)$$

Where, Pij is the size of the payload image,
Cij is the size of the cover image.

3.2. PROPOSED EMBEDDING MODEL

The flow chart of the proposed algorithm is as shown in Figure 2

(i) Cover image: The cover image of size (a*a) is resized to Mc x Nc to attain optimum PSNR.
Where Mc = Nc = n * p
n is the even value and P is the number of rows in the payload.

(ii) Payload: It is the secret image which is to be embedded in a cover image. If 'P' is the number of rows in the payload and it must be an even number. The size of the payload is (P*1.5P) as shown in Figure 1.

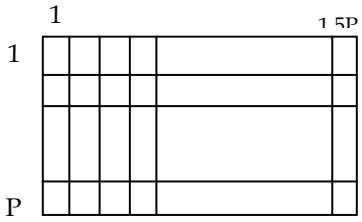


Fig.1. Payload dimensions

(iii) Lifted Wavelet Transform 2 (LWT2) using dB2: Daubechies wavelet transform is applied to the resized cover image to generate XA, XV, XH and XD bands. The XD band is divided into three parts say XD0, XD1 and XD2 of sizes (Mc/4 x Nc/4), (Mc/2 x Nc/4), and (Mc/4 x Nc/4) respectively as shown in Figure 3 to accommodate the bits of spatial and transformed domain payload properly. Daubechies wavelet gives a good precision of 4 digits after decimal point.

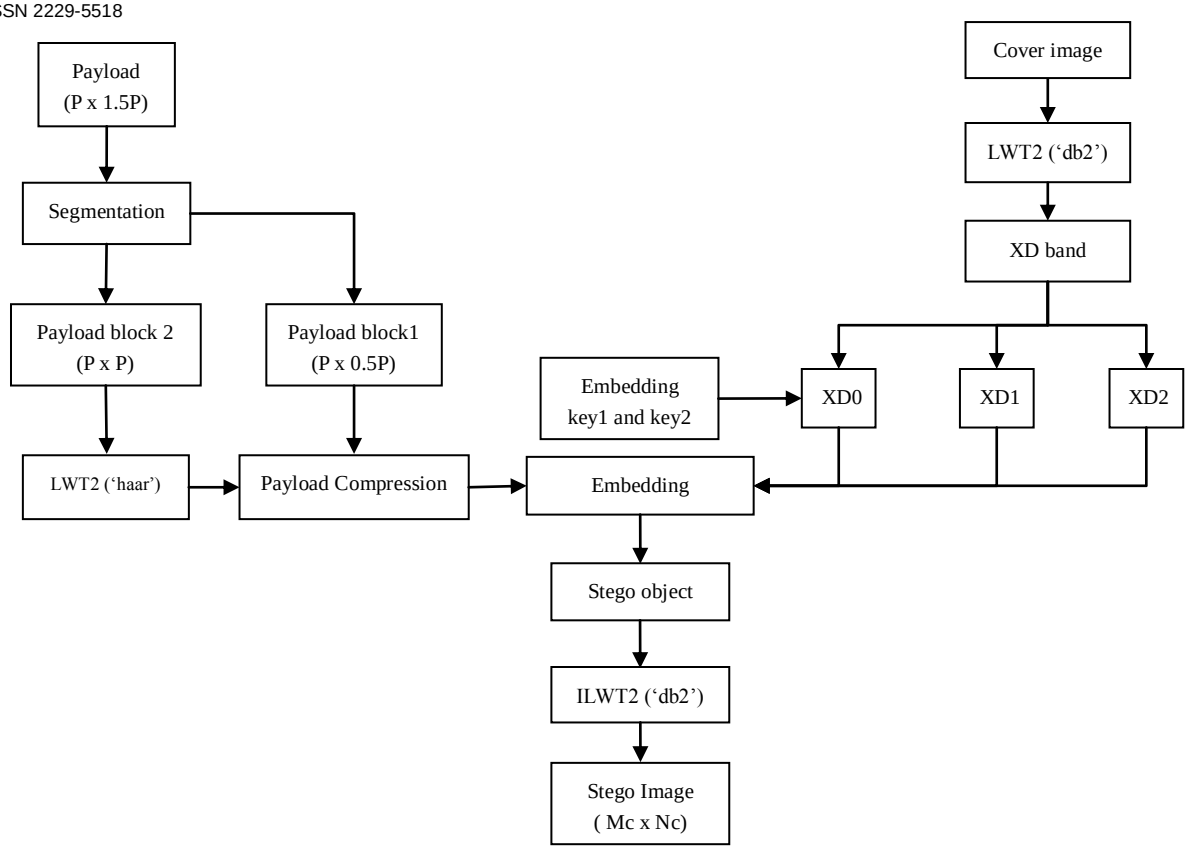


Fig.2. Embedding flowchart of proposed SAEPW algorithm

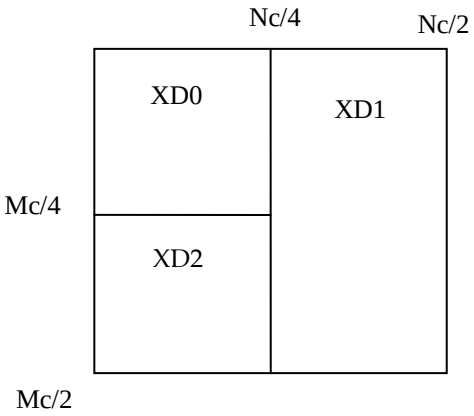


Fig.3. Regions of XD0, XD1 and XD2 of XD band

(iv) Segmentation: Original payload of size P*1.5 P decomposed into two blocks viz., (i) the first block of size is original rows of payload and 1/3rd of columns of pay load (P*0.5P) and (ii) the second block of size the original rows of pay load and 2/3rd columns of original payload (P*P).
Payload Block 1: The payload image sixe of P*0.5P is retained in the spatial domain itself.
Payload Block 2: The payload image size of P*P is converted into wavelet domain using LWT2 Harr wavelet to generate four sub bands say XA, XV, XH and XD.

(v) Lifted Wavelet Transform 2 (LWT2) using Haar: The Harr wavelet is applied to payload block 2 to generate four sub blocks XA, XV, XH and XD. The low frequency band XA coefficients are considered to be embedded into cover image.

(vi) Compression on payload: The pixel intensity values of payload block 1 and XA coefficients of payload block 2 are divided by the maximum intensity value 255 to reduce actual values and compute percentage of obtain values to generate percentage value between 0 and 100. The percentage values are scale down further by dividing the value of 15 to generate values between 0 and approximately 7. The maximum scale down value 7 is represented by only 3 bits in binary. The fractional part of each scale down values is also considered and embedded in to cover image. The two level scale down improves the security level to payload and also the 8 bit binary of each pixel is converted into 3 bits which improves capacity. The two keys are used viz., (i) Key1 for first level scale down value 255 and (ii) Key2 for second level scale down value 15. As each pixel of payload are represented by only 3 bits in binary instead of 8 bits in binary for original payload. All 3 bits can be embedded in to the cover image hence retrieval of payload quality improves.

(vii) Embedding Algorithm: The Key1 and Key2 values are embedded into first 3 coefficients of XD0 of cover image by replacing 4 LSB bits in each pixel. The payload blocks 1 pixels with 3 bits for integer parts and are embedded into XD1 band of cover image by replacing LSBs of each coefficients. The payload block 2 coefficients with 3 bits are embedded into XD2 band of cover image by replacing LSBs of each coeffi-

cients. The embedding process is performed based on size of the cover image
(i) If n = 2, ie., the size of the cover image is 2P*2P, then embed payload continuously in every pixels of cover image.
(ii) If n = 4, ie., the size of the cover image is 4P*4P, then embed payload in alternative pixels of rows and columns.
(iii) If n = 6, ie., the size of the cover image is 6P*6P, then embed payload in alternative pixels with a gap of two rows and two columns.

(viii) Inverse Lifted Wavelet Transform 2 (ILWT2): Inverse LWT2 is applied on stego object to convert into spatial domain stego image.

3.3. PROPOSED EXTRACTION MODEL

The embedded payload in the cover image is retrieved from the stego image by adapting reverse process of embedding. The block diagram is shown in Figure 4.

(i) Lifted Wavelet Transform 2 (LWT2) using dB2: Daubechies level 2 wavelet transform is applied on stego image of size (Mc x Nc) to generate XA, XV, XH and XD bands. The XD band of size (Mc/2 x Nc/2) is divided into three parts of XD0, XD1 and XD2 of each size (Mc/4 x Nc/4), (Mc/2 x Nc/4) and (Mc/4 x Nc/4) respectively.

(ii) Extracting key: Key1 and Key2 are extracted from first three coefficients of XD0 band.

(iii) Extract payload bits: The three bits of payload are extracted from LSB's of XD1 coefficients and converted to decimal values of payload and fractional value of XD1 coefficients are appended with decimal value of payload. Each payload value is multiplied by 15 (key2) and 255 (Key1) and divide by 100 to generate payload pixel values. The three bits of payload are extracted from LSB's of XD2 coefficients and converted into decimal values and the fractional values of XD2 coefficients are appended with decimal value of payload. Each payload value is multiplied by 15 (key2) and 255 (Key1) and divide by 100 to generate payload pixel values. The ILWT2 (Harr) is applied on the total decimal values obtained from XD2 band to derive payload value in spatial domain.

(iv) Fusion: The extracted payload pixel values from XD1 and XD2 are concatenated to generate payload image.

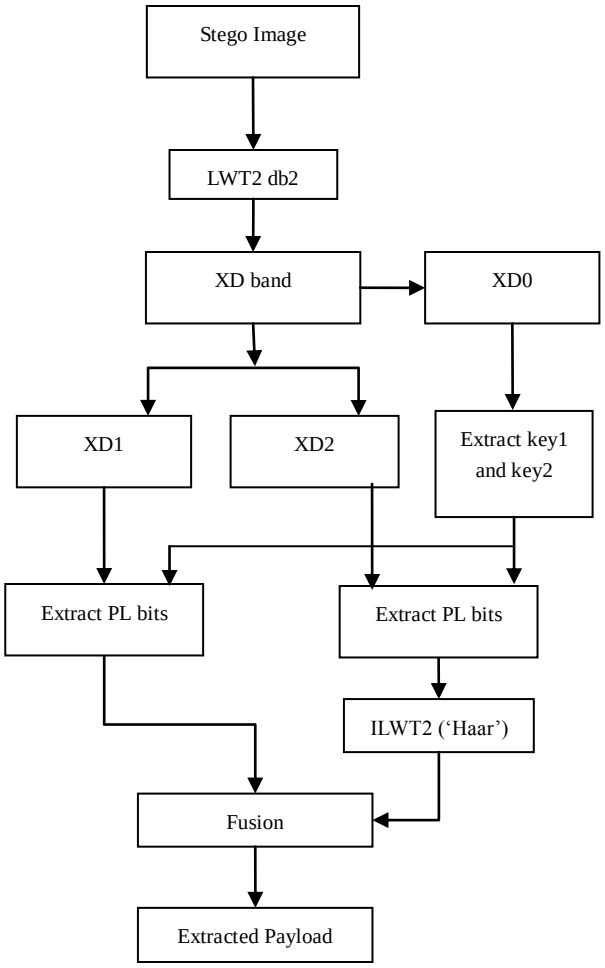


Fig.4. Retrieval flow chart of proposed SAEPW

4 ALGORTITHM

Problem definition: The encrypted payload in spatial and transform domain is embedded into cover image to generate stego image for secure communication.

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

The objectives are
(i) To decrease MSE
(ii) To increase capacity
(iii) To increase PSNR

The embedding and retrieval algorithms of SAEPW is shown in Table 1 and Table 2

TABLE 1:- Embedding algorithm of SAEPW

Input: Cover image, payload
Output: Stego image

1. Apply LWT2 using dB2 wavelet on the cover image.
2. XD band is segmented into into XD0 (Mc/4 x Nc/4), XD1 (Mc/2 x Nc/4) and XD2. (Mc/4 x Nc/4).
3. Key1 and key2 is embedded into XD0.
4. Payload is segmented into block 1 (P x 0.5P) and block 2 (P x P).
5. Apply LWT2 (Harr) on block2.
6. Payload block1 pixel values and payload block2 XA coefficient values are divided by key1 and 2 and multiply by 100 to compress eight bits of payload to three bits.
7. Payload bits of block1 and block2 are embedded into XD1 and XD2 respectively to generate stego object.
8. Apply ILWT2 (dB2) on stego object to generate Stego image in spatial domain.

TABLE 2:- Retrieving algorithm of SAEPW

Input: Stego image, Output: Payload

1. Apply LWT2 (dB2) on the stego image and consider the XD band.
2. The XD band is partitioned into three parts of XD0, XD1 and XD2 of each size (Mc/4 x Nc/4) and (Mc/2 x Nc/4) and (Mc/4 x Nc/4) respectively.
3. Extract key1 and key2 from first three coefficients of XD0.
4. Extracted three LSB bits from XD1 coefficients payload value is multiplied by 15 (key2) and 255 (Key1) and divide by 100 to generate payload pixel values.
5. Extracted three LSB bits from XD2 coefficients payload value is multiplied by 15 (key2) and 255 (Key1) and divide by 100 to generate payload pixel values.
6. XD1 and XD2 payload pixel values are concatenated to generate payload image.

5 PERFORMANANCE ANALYSIS EQUATIONS

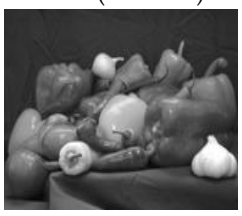
Cover image (CI) of different sizes and formats viz., JPEG, PNG, TIFF, GIFF and BMP images are considered for performance analysis. The payload (PL) Pepper is embedded into the cover image Barbara to generate stego image Barbara. The payload peppers are retrieved from stego image is shown in Figure 5.

Table 3 gives the PSNR values of cover image with stego image and extracted payload with actual payload for different formats. It is observed that the value of PSNR between cover image and stego image varies slightly with image formats. The PSNR value between payload and Extracted payload are also varies with image formats.

(a) Cover image: Barbara.png
Size: (512*512)

(b)Payload: Peppers.png
Size :(256*384)

(c)Stego image: Barbara.png
Size: (512*512)



(d)Retrieved: Peppers.png
Size :(256*384)

Fig.5. Barbara cover image with Peppers payload

Table 3. PSNR values of the proposed work

Cover image (512*512)	Payload (256*384)	PSNR (SI)	PSNR (EPL)
JPEG	JPEG	44.9221	23.2842
	PNG	48.4534	26.3024
	TIFF	45.9001	24.0101
	GIFF	44.9193	23.2040
	BMP	45.9001	24.0101
PNG	JPEG	47.1966	31.2965
	PNG	47.8110	34.1786
	TIFF	47.2584	30.9932
	GIFF	47.2009	30.7435
	BMP	47.2584	30.9932
TIFF	JPEG	47.1240	31.2960
	PNG	48.0572	34.1771
	TIFF	47.2946	31.0738
	GIFF	47.1269	30.7430
	BMP	47.2946	31.0738
GIFF	JPEG	47.1210	27.7671
	PNG	48.0527	30.8205
	TIFF	47.2907	28.1168
	GIFF	47.1239	27.5237
	BMP	47.2907	28.1168
BMP	JPEG	47.1240	31.2960
	PNG	48.0572	34.1771
	TIFF	47.2946	31.0738
	GIFF	47.1269	30.7430
	BMP	47.2946	31.0738

The Table 4 gives PSNR and capacity values for different sizes of cover image and payload of size 256 x 384. The value of

PSNR increases as the size of the cover image increases but capacity decreases.

Table 4 PSNR for different sizes of cover image.

Cover image (JPEG)	PSNR (stego to cover Image)	Capacity (bpp)
512 x 512	48.4534	0.375
1024 x 1024	54.2509	0.09375
1536 x 1536	57.6576	0.04166
2048 x 2048	60.0901	0.02343

The graph of capacity and PSNR is shown in Figure 6 it is seen that as capacity increases the values of PSNR decreases.

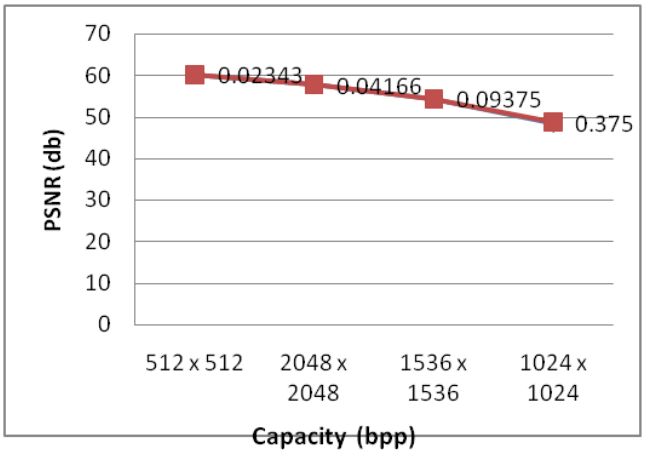


Fig.6. The variation of PSNR values with capacity.

Table 5 shows the comparison of PSNR for the existing Pixel Bit Manipulation for Encoded Hiding - An Inherent stego (BMEH) [20] and the proposed algorithm SAEPW. It is observed that the PSNR is higher in the case of proposed algorithm compared to the existing algorithm for all image formats due to the payload splitting and the use of Daubechies wavelet transforms.

Table 5. Comparison of PSNR of proposed algorithm with existing method [20]

Method	Size	PSNR (dB)
Existing method [20]	CI: 128 * 128 PL: 64 * 64	40.719
proposed method (SAEPW)	CI: 512 * 512 PL: 256 * 384	48.453

6 Conclusion and Future Work

The steganography is used to transmit the secret information through communication channel in a covert manner. In this paper the steganography technique SAEPW is proposed. LWT2 (dB2) is applied on cover image and XD band is decomposed into XD0, XD1 and XD2. The payload is decomposed into block1 and block2. The LWT2 is applied on block 2 while block 1 is retained in spatial domain. The binary eight bits for each pixel in payload block1 and coefficients in block2 are scaled down to three bits using key1 and key2. The key1 and key2 are embedded into XD0 band. The three binary bits of payload block 1 and block2 are embedded adaptively based on cover image size into XD1 and XD2 of cover image respectively by replacing three LSB bits to generate stego object. The ILWT2 (dB2) is applied on stego object to create stego image in spatial domain.

It is observed the values of PSNR and capacity with different image formats are improved in the proposed technique compared to the existing method. In future Dual Tree Complex Wavelet Transform (DTCWT) can be used and also improve in choosing the key.

References

[1] Jifeng Huang, "The Algorithm of Estimating Location of the Embedded Secret Message in Stego Image," International Conference on Information Technology and Computer Science, pp. 205 – 208, 2009.

[2] Kafri N and Suleiman H Y, "Bit-4 of Frequency Domain-DCT Steganography Technique," First International Conference on Networked Digital Technologies, pp. 286 – 291, 2009.

[3] Izadinia H, Sadeghi F and Rahmati M, "A New Secure Steganographic Method based on Predictive Coding and Quantization Index Modulation," International Conference of Soft Computing and Pattern Recognition, pp. 234 – 238, 2009.

[4] Ghoshal N and Mandal J K, "A Steganographic Scheme for Colour Image Authentication," IEEE International Conference on Recent Trends in Information Technology, pp. 826-831, 2011.

[5] Yicong Zhou and Agaian S, "Image Encryption using the Image Steganography Concept and PLIP Model," International Conference on System Science and Engineering, pp. 699-703, 2011.

[6] Almohammad A, and Ghinea G, "Image Steganography and Chrominance Components," IEEE International Conference on Computer and Information Technology, pp. 996 - 1001, 2010

[7] Ghasemi E, Shanbehzadeh J and Zahir Azami B, "A Steganographic Method Based on Integer Wavelet Transform and Genetic Algorithm," International Conference on Communications and Signal Processing, pp. 42-45, 2011.

[8] Yong-Hong Zhang, "Image Encryption Using Extended Chaotic Sequences," International Conference on Intelligent Computation Technology and Automation, vol. 1, pp.143-146, 2011.

[9] Swain G and Lenka S K, "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels," International Conference on Communication and Computational Intelligence, pp. 529-534, 2010.

[10] Weiming Zhang, Xinpeng Zhang and Shuozhong Wang, "Near-Optimal Codes for Information Embedding in Gray-Scale Signals," IEEE Transactions on Information Theory, pp.1262-1270, 2010.

[11] Gopalan K, "An Image Steganography Implementation for JPEG-Compressed Images," International Symposium on Communications and Information Technologies, pp.739-744, 2007

[12] Cui-ling Jiang, Yi-lin Pang and YuZhu Y, "A Steganographic Method based on the JPEG Digital Images," Third International Conference on Computer Research and Development, pp.35-38, 2011.

[13] Yan-Ping Zhang, Juan Jiang, Chao Xu, Bo Hua and Xiao-yan Chen, "A New Scheme for Information Hiding Based on Digital Images," Seventh International Conference on Computational Intelligence and Security, pp. 512 – 516, 2011.

[14] Septimiu Fabian, Mare Mircea Vladutiu and Lucian Prodan, "Secret Data Communication System Using Steganography, AES and RSA," Seventeenth International Symposium for Design and Technology in Electronic Packaging, pp. 339 – 344, 2011.

[15] Chen Gouxi, Cao Min, Fu Donglai and Ma Qiaomei, "Research on An Steganographic Algorithm Based on Image Edge," International Conference on Internet Technology and Applications, pp. 1 – 4, 2011
[16] 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, 2011.
[17] Wien Hong and Tung Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, vol.7, no.1, pp.176-188, 2012.
[18] Che-Wei Lee and Wen-Hsiang Tsai, "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability," IEEE Transactions on Image processing, vol.21, no12, pp.207-218, 2012.
[19] Lionel Fillatre, "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images," IEEE Transactions on Signal Processing, vol. 60, no.2, pp.556-569, 2012.
[20] Siva Janakiraman, Anitha Mary, Jagannathan Chakravarthy, Rengarajan Amirtharajan, K.Thenmozhi and John Bosco Balaguru Rayappan, "Pixel Bit Manipulation for Encoded Hiding - An Inherent stego," International Conference on Computer Communication and Informatics, 2012.

AUTHORS BIOGRAPHY

H S Manjunatha Reddy is a Professor in the department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore. He obtained his B.E. Degree in Electronics from Bangalore University, Bangalore. His specialization in Master degree was Digital Electronics from Visvesvaraya Technological University, Belgaum. He is pursuing research in the area of Steganography and Steganalysis for secured communication. His area of interest is in the field of Digital Image Processing, Communication Networks and Biometrics. He is life member of ISTE, New Delhi.

K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering and Master of Engineering in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 100 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.