Wavelet based Secure Steganography with Scrambled Payload

H S Manjunatha Reddy, K B Raja

Abstract– ***The Steganography is used for secure communication of information by embedding information in a cover object. In this paper we propose Wavelet based Secure Steganography with Scrambled Payload (WSSSP). The Daubechies Lifting Wavelet Transform (LWT) is applied on cover image. The XD band is decomposed into upper and lower bands for payload embedding. The payload is segmented into four equal blocks. The Harr LWT is applied on alternate blocks of payload to generate F1 and F2 wavelet transform bands. The remaining blocks of payload are retained in spatial domain say S1 and S2. The bit reversal is applied on each coefficient of payload blocks to scramble payload. The cube root is applied on scrambled values to scale down the number of coefficient bits. The payload the embedded into XD band of cover image to generate step object. The decision Factor Based Manipulation (DFBM) is used to scrambled stego object. The Daubechies ILWT2 is applied on stego object to obtain stego image in spatial domain. It is observed that PSNR and capacity of the proposed algorithm is better compared to existing algorithm.***

Index Terms- Steganography, wavelets, Stego image, Payload, Cover Image.

I. INTRODUCTION

The use of internet in the world becomes the prime mode of communication and subsequently digital crime becomes the major threat to the mankind. Therefore it is most essential to have a secured data communication. The development of computer networking and expanding its use in different areas of life and work, the issue of information security has become increasingly important [3]. The commonly used information securities are Cryptography, Steganography, Coding, etc. The Cryptography scrambles the data which makes eavesdropper difficult to interpret the data but existence of communication is known to the hackers and this may lead to attempts to decrypt, modify or destroy the data. This lead to evaluation of a technique called Steganography for data hiding. The data hiding techniques [9] is used to embed the secrete data into cover object such as images, videos audio files, sounds etc. They are two types of information hiding technology namely Watermarking and Steganography. The Watermarking is used to embed a distinguishable symbol such as signature, logo of the organization or any trademark into host signals to recognize the ownership of the signals. Watermarking is to concentrate to get high robustness against attacks and also to ensure that the embedded information can be successfully extracted from the watermarked signals.

Manuscript received on July, 2012.

H S Manjunatha Reddy[1], Department of ECE, Global Academy of Technology, Bangalore, India.

K B Raja[2], Department of ECE, [2]University Visvesvaraya College of Engineering, , Bangalore University, Bangalore, India.

The shifts from cryptography to stegnography are that concealing the image existence and enable to embed the secret message to cover objects. Steganography implies that the message to be transmitted is not visible to the informal eye. The main goal of Steganography is mainly concerned with the protection of contents of the hidden information [10]. Usually images are ideal for information hiding because of the large amount of redundant space is created in the storing of images. Secret information is transmitted through unknown cover carriers in such a way that the existence of the embedded messages is undetectable.

The advancements in computer networks, internet, and digital media lead to the wide range development of the steganographic techniques. The strength of steganography can be improved by combining it with cryptography. Most steganography uses different cover media like text, image, audio, video or any other digitally represented code. Steganography used in a large amount of data formats in the digital world such as bmp, gif, .jpeg, .mp3, .txt, .wav etc. The redundant or noisy data can be removed from these formats easily and replaced with a hidden message.

However the main difference between them is the encryption can see anybody but both parties are communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. The steganography techniques must satisfy the following requirements; (i) the integrity of the hidden message after it has been embedded inside the cover object must be correct. (ii) The cover object must remain unchanged or almost unchanged to the naked eye.

The Steganography Techniques are broadly classified (1) Binary File Technique: In this approach the embedding is performed by changing the binary code that does not affect the execution of the file and it is simple to implement. (ii) Text Technique: Is to embed the information inside a document by alter some of its characteristics i.e., either the formatting text or characteristics of the characters. (iii) Image hiding technique: Uses the least significant bits of each pixel in one image to hide the most significant bits of another or embeds the information by altering the transformed DCT coefficients. The various image hiding techniques are LSB, DCT, and Wavelet transform etc. (IV) Sound technique: Embeds data as a binary sequence of sounds like noise but which can be recognized by a receiver with the correct key. (v) Video technique: Uses the combination of sound and image techniques.

Contribution: In this paper WSSSP algorithm is proposed. The payload is segmented into four blocks. The Harr LWT is applied on alternate blocks of payload to generate F1 and F2 wavelet transform bands. The remaining blocks of payload are retained in spatial domain say S1and S2. The bit reversal is applied on each coefficient of payload blocks to scramble payload and scale down the number of coefficient bits.

The stego object is further scrambled and applied ILWT to generate stego image.

Motivation: Developments in modern communication like wireless and internet communication requires security. Steganography plays an important role in secure communication. The survey of many techniques made us to develop new algorithm. The proposed algorithm shows better performance compare to the available methods, which proves to be more secure, high capacity and robust against attacks.

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

II. RELATED WORK

Guangjie Liu et al., [1] have introduced optimal adjustment step into the system to preserve the prediction errors' distribution by elaborately chosen statistical features. The secret message hidden by PCB steganography can be easily detected with very small error probability. Yuan-Hui Yu et al., [2] proposed steganographic method for embedding a color or a gray scale image in a true color image. The secret images can be carried either by hiding a color secret image or hiding a palette-based 256-color secret image or hiding a gray scale image in a true color image. Munivara Prasad et al., [4] proposed Blind Consistency Based Steganography (BCBS), which provides high imperceptibility and security for information from subterfuge attack. To improve the imperceptibility of the BCBS, DCT is used in combination to transfer stego image from spatial domain to the frequency domain. The hiding capacity of the information is improved by introducing Fractal Compression and the security is enhanced using by encrypting stego-image using DES.

Weiqi Luo et al., [5] proposed an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. Der Chyuan et al., [6] have proposed a scheme of novel adaptive steganographic is capable of both preventing visual degradation and also providing a large embedding capacity. The embedding capacity of each pixel is dynamically calculated by the local complexity of the cover image in order to maintain good visual quality and embedding a large amount of secret information. The pixels are classified into three levels based on the variance of the local complexity of the cover image. The human vision sensitivity is taken into consideration when determining which level of local complexity a pixel should belong to it.

Zaidan et al., [7] have developed four novel concepts for secure communication. The first concept based on multi-cover steganography using remote sensing image taken from the satellite in a manner of three shots and images generate one false color image. The second concepts are recursion neural cryptosystem to defeat the problem of exchange cryptography keys through the network and same key used decrypt the data. The combination of multi-cover steganography and neural cryptosystem results in third novel concept. The fourth concept is based irregular encoding method using LSB algorithm. Pei-Yu Lin et al., [8] proposed a technique of invertible image sharing approaches is that the revealed content of the secret image must be lossless and the distorted stego images must be able to be reverted to the original cover image. They first transform the secret pixels into the m-ary notational system and then calculate the information data used to reconstruct original pixels from camouflaged pixels such that the information data and transformed secret data are shared using the (t,n) threshold sharing scheme to achieve the lossless secret image and reverse the stego image to the original image.

Amitava Nag et al., [11] proposed novel technique for Image steganography based on DWT, where DWT is used to transform original image from spatial domain to frequency domain. Firstly 2D- Discrete Wavelet Transform is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages before embedding. Then each bit of Huffman code of secret message is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub band. Chia Chun Wu et al., [12] have proposed a scheme of secret image sharing by applying optimal pixel adjustment process to improve the image quality for different payload capacity and various bits conditions. Yuting Su et al., [13] have developed a steganalytic method to detect information hidden in the motion vectors of video bit-streams. Which is based on the statistical analysis of relative properties, the feature classification technique is adopted to determine the existence of hidden messages and Support Vector Machine (SVM) is used as the discriminator.

Zhili Chen et al., [14] developed a steganalysis technique against substitution-based linguistic steganography based on context clusters. The context clusters to estimate the context fitness and indicates how to use the statistics of context fitness values to distinguish between normal texts and stego texts.

III. PROPOSED MODEL

In this section definition of evaluation parameters, embedding model and extraction model are discussed.

A. 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 is calculated using Equation 1.

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

Where N: Size of 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, i.e., the percentage of

noise present in the cover image is given in an Equation 2.

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

(iii) Capacity: It is the size of the payload data in a cover image that can be modified 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, P_ij is the size of the payload image,
C_ij is the size of the cover image.

B. Proposed Embedding Model

The block diagram of the proposed embedded algorithm is as shown in Figure. 3.

Cover image: It is the given space for embedding the payload. The important property of the cover image is that its statistical properties cannot be altered significantly by embedding the secret information into it the cover image sizes of 2^N X 2^N is considered for embedding process with different image formats like JPEG, GIF, BMP and PNG

Payload: It is the secret information that is to be hidden in the cover image. The size of payload is half or less than half of cover image. Here, the payload is fragmented into four equal halves as shown in Figure 1. The payload blocks F1 and F2 are processed using frequency based transformation and Payload blocks S1 and S2 are processed using spatial domain.

F1	S1
S2	F2

Fig. 1: Payload structure

Lifting Wavelet Transformations 2 (LWT2): Wavelet transform provides time frequency representation. The wavelet transform of an image is created by repeated filtering the image coefficients on a row by row and column by column basis. To generate four wavelet bands such as Approximation band, Vertical band, Diagonal band and Horizontal band. The approximation band has low frequency component and significant information is present in this band. The vertical, diagonal and horizontal bands has insignificant information of an image such as detailed and minute information such as edge information, corner detailed information etc., Daubechies (db2) wavelet transform is applied on cover image to convert into wavelet domain and Haar wavelet (Daubechies db1) is used to transform payload into wavelet domain. Harr wavelet is discontinuous and resembles a step function which represents the same wavelet as Daubechies (db1).

Fragmentation: The given payload is divided into blocks of four equal dimensions to extract features from two blocks with spatial domain S1 and S2 and extract features from another two blocks with frequency domain F1 and F2. The integer LWT is applied on F1 and F2 to derive four sub bands in each block. The approximation sub band from each block are considered and resized to the original size of F! and F2. S1 and S2 blocks are retained in the spatial domain itself.

Index Reversal (IR): The blocks S1, S2, F1 and F2 rows are converted into single column. The index value of each element in a column is converted into binary equivalent. The bit reversal is applied on each binary index value and converts back to decimal index value. The index reversal is used to scramble payload pixel positions.

Pre processing: The intensity values of each pixel in the column vector are considered and cube root is applied to scale down the intensity value. The integer part of scale downed value can be represented by 3 bits for intensity value varies from minimum value 0 and maximum of 255. The cube root of maximum 255 intensity value is 6.342, ie., the maximum.

Embedding Procedure: For embedding of alternate 2 blocks of payload (F1 and S1) in upper half of XD band and other 2 alternate 2 blocks of payload (S2 and F2) in lower half of XD band are considered. The embedding pattern employed is shown in Figure 2.

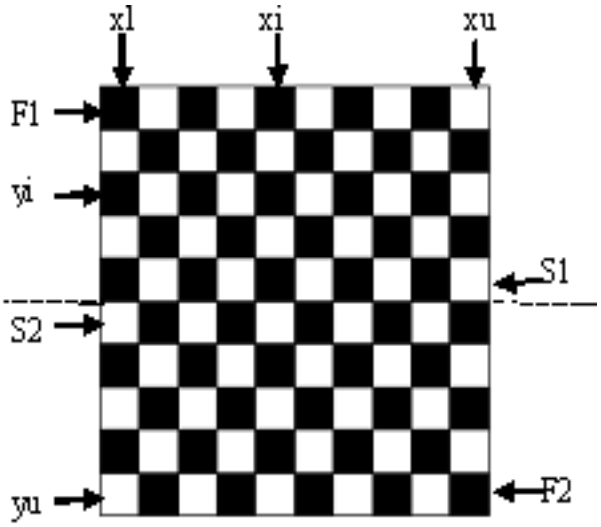


Fig. 2: XD band of Cover image

(i) Embedding of F1 and S1 payload blocks into the XD band of the cover image starting from the top left corner of the upper half band. The equation 4 shows the embedding pattern of the payload blocks. Initialise xi and yi.

for (i mod 2 ≠ 0)

$$x_i + SS \le xu - 1$$
$$y_i + SS \le yu - 1$$

for (i mod 2 = 0)

$$x_i + 1 + SS \le xu$$
$$y_i + 1 + SS \le yu \quad (4)$$

Where,
i = current row/column index
x_i = current index of row, Range of x_i : $xl \le x_i \le xu$.
y_i = current index of column, Range of y_i : $yl \le y_i \le yu$
xu = upper bound of rows
yu = upper bound of columns
Step Size (SS) = Total embedding positions available/Dimensions of block to be embedded.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

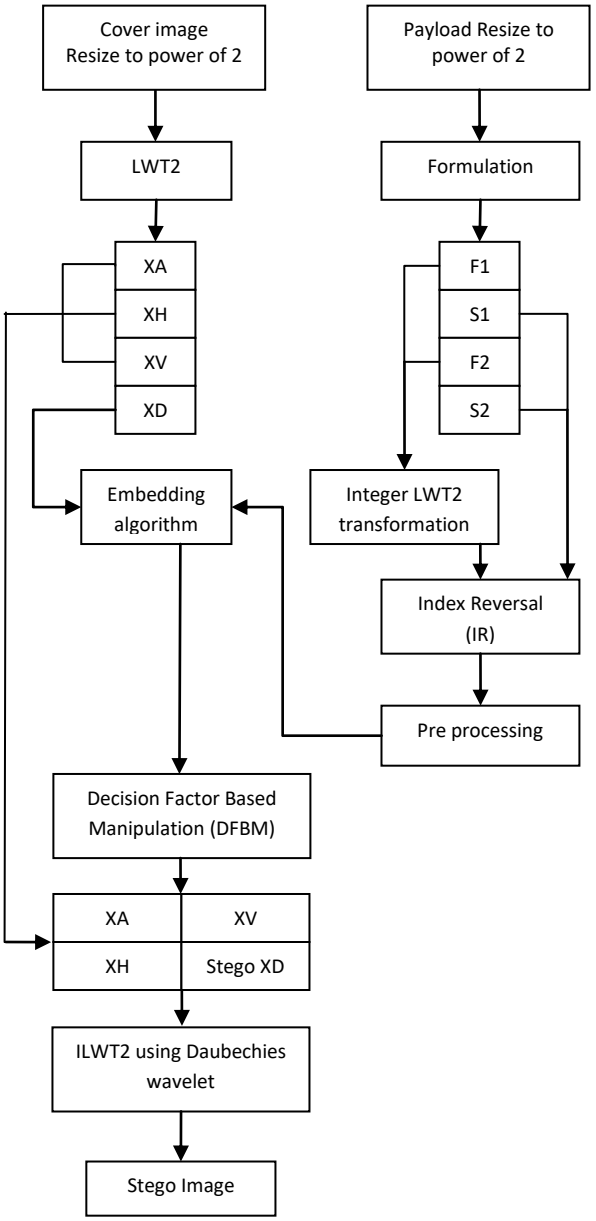


Fig 3: Embedding system of WSSSP Model

(ii) Embedding of F2 and S2 payload blocks into the XD band of the cover image starting from the bottom right corner of the lower half band. The equation 5 shows the embedding pattern of the payload blocks. Initialise xi and yi.

$$\begin{aligned} &\text{for (i mod 2 = 0)} \\ &\quad x_i - 1 - SS \geq xl \\ &\quad y_i - 1 - SS \geq yl \\ &\text{for (i mod 2} \neq 0) \\ &\quad x_i - SS \geq xl + 1 \\ &\quad y_i - SS \geq yl + 1 \end{aligned} \quad (5)$$

Where,

i = current row/column index

x_i = current index of row, Range of x_i : $xl \leq x_i \leq xu$.

y_i = current index of column, Range of y_i : $yl \leq y_i \leq yu$

xl = lower bound of rows

yl = lower bound of columns

Step Size (SS) = Total embedding positions available dimensions of block to be embedded.

The three bits of payload are embedded into three LSB bits of XD band cover image. The scale downed decimal (fraction) value of payload is added to the cover image to obtain stego object.

Decision Factor Based Manipulation (DFBM): The decision factor is used to modify the stego object image which is obtained after the embedding process. The objective of this process is to increase security level to the payload bits.

Decision Factor (DF) is calculated by and operation of Current Coefficient value of XD band with 48D i.e., 0011 0000B (in binary). Let CCV is the Current Coefficient Value of XD stego object and MCV is the Modified Coefficient Value of XD stego object. Table 1 shows the different cases of interchanging bits with reference to the DF value.

Table 1: DF values and MCV exchange

DF Decimal Value	MCV Exchange
00	No change in coefficient value
16	1st and 2nd bits are interchanged
32	3rd and 4th bits are interchanged
48	1st and 2nd : 3rd and 4th bits are interchanged

Case (i): If DF == 00d i.e. 0000 0000B

No change.

Eg: if CCV = 0000 0110B

DF = 0000 0110 bit and 0011 0000

DF=0000 0000b or 00d

So, MCV = 0000 0110b with no change.

Case (ii): If DF == 16d i.e. 0001 0000b

Interchange 1st and 2nd bit of stego object.

Eg: Let CCV = 0001 0110b

DF = 0001 0110b bit and 0011 0000

DF = 0001 0000b or 16d

So, MCV = 0001 0101 with interchanging 1st and 2nd bit of stego object.

Case (iii): If DF == 32d i.e. 0010 0000b

Interchange 3rd and 4th bit of stego object.

Eg: Let CCV = 0010 0110b

DF = 0010 0110b bit and 0011 0000

DF = 0010 0000b or 32d

So, MCV = 0010 1010 with interchanging 3rd and 4th bit of Stego object

Case (iv) If DF == 48d i.e. 0011 0000b

Interchange 1st and 2nd bit of stego object.

Interchange 3rd and 4th bit of stego object.

Eg: Let CCV = 0011 0110b

DF = 0011 0110b bit and 0011 0000

DF = 0011 0000b or 48d

So, MP = 0011 1001 with interchanging 1st and 2nd bit: 3rd and 4th bit of stego object.

Inverse Lifting Wavelet Transformations 2 (ILWT2): performs a 2-D lifting wavelet reconstruction of stego image in spatial domain. The size and format of stego image is same as cover image.

C. Proposed Extraction Model

In this section the proposed extraction model has been discussed. The block diagram of the proposed extraction algorithm is shown in Figure 4.

Lifting Wavelet Transformations 2 (LWT2): Daubechies (db2) wavelet transform is applied on stego image to generate four wavelet bands such as Approximation band, Vertical band, Diagonal band and Horizontal band. Out of four bands XD band is considered since the payload is embedded into XD band.

Decision Factor Based Manipulation: The Decision Factor (DF) is used to modify back the XD band of the stego image.

Calculation of DF is done by masking the coefficients of XD band by AND operation with 48d i.e., 0011 0000b.

Case (i): If DF == 00d i.e. 0000 0000b
No change.

Case (ii): If DF == 16d i.e. 0001 0000b
Interchange 1st and 2nd bit of stego image.

Case (iii): If DF == 32d i.e. 0010 0000b
Interchange 3rd and 4th bit of stego image.

Case (iv): If DF == 48d i.e. 0011 0000b
Interchange 1st and 2nd bit of stego image.
Interchange 3rd and 4th bit of stego image.

Extraction Procedure: For extraction of alternate 2 blocks of payload (F1 and S1) from the upper half of XD band and other 2 alternate 2 blocks of payload (S2 and F2) from the lower half of XD band. The extraction pattern employed is same as followed during embedding.

1. Extraction of F1 and S1 payload blocks from the XD band of the cover image starting from the top left corner of the upper half band. The equation 6 shows the extraction pattern of the payload blocks. Initialise xi and yi.

$$\text{for } (i \bmod 2 \neq 0)$$
$$xi + SS \leq xu - 1$$
$$yi + SS \leq yu - 1$$

$$\text{for } (i \bmod 2 = 0)$$
$$xi + 1 + SS \leq xu$$
$$yi + 1 + SS \leq yu \qquad (6)$$

2. Extraction of F2 and S2 payload blocks from the XD band of the cover image starting from the bottom right corner of the lower half band. The equation 7 shows the extraction pattern of the payload blocks.

$$\text{for } (i \bmod 2 = 0)$$
$$xi - 1 - SS \geq xl$$
$$yi - 1 - SS \geq yl$$
$$\text{for } (i \bmod 2 \neq 0)$$
$$xi - SS \geq xl + 1$$
$$yi - SS \geq yl + 1 \qquad (7)$$

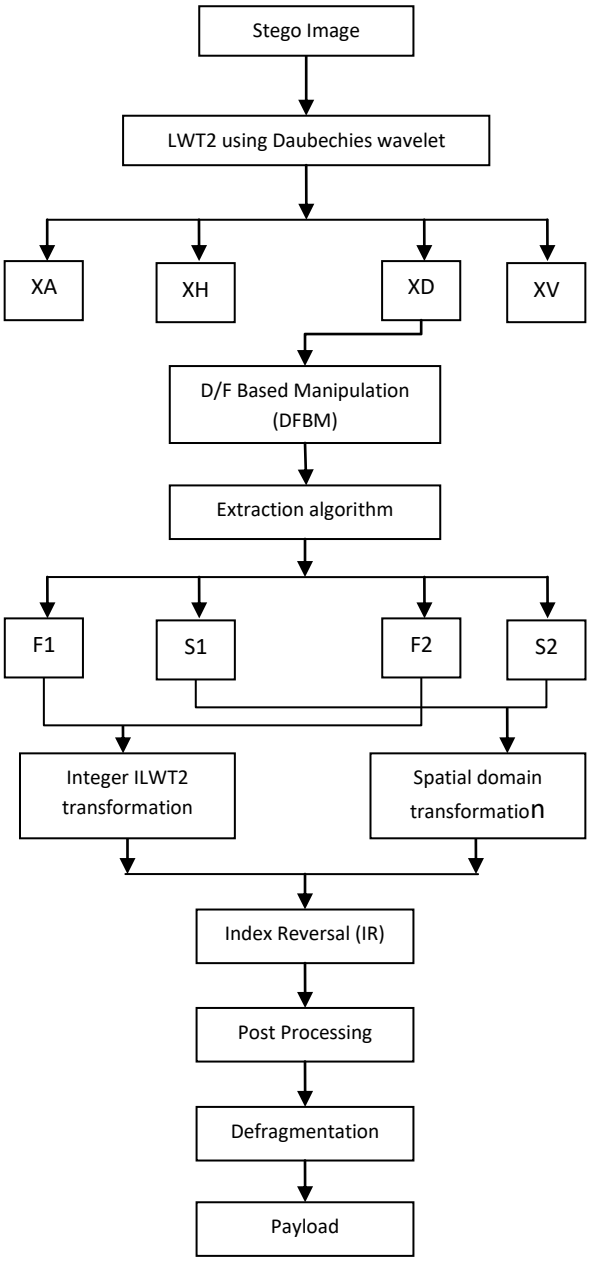


Fig 4: Retrieval system for WSSSP Model

Index Reversal (IR): It is used for regaining original index of random embedded payload blocks. It permutes the input block into index reversed order.

Post processing: It evaluates the cubes of the input block and adds the integer as well as the decimal part. It is done to get back the embedded payload; it scales up the input block.

Defragmentation: It combines the obtained payload blocks of four equal dimensions into payload. The dimensions of the retrieved payload are same as the dimensions of the embedded payload.

Payload: The retrieved payload is of same dimensions and format as the original embedded payload (512 x512).

IV. ALGORITHMS

Problem definition: the information is communicated securely using steganography. The spatial domain and transform domain techniques are used to generate stego image from cover image and payload

The objectives are

(i) improve PSNR
(ii) increase capacity
(iii) improve security

Assumptions:

(i)The stego image is transmitted over an ideal channel.

Table2: Embedding algorithm

Input: Cover image
Output: Stego image

1. Decompose the cover image into four bands using Daubechies LWT. Detail XD band is rounded up to nearest integer value and is used for embedding payload blocks.
2. Sign of each coefficient is stored in a temporary matrix. Payload is fragmented into four equal dimension blocks.
3. For two alternate payload blocks Haar using Lifting Wavelet Transformation using is applied. Only approximation bands are used for embedding in cover image.
4. Index Reversal is applied to all four blocks of payload.
5. In pre-processing, cube roots of all four blocks are evaluated and decimal as well as integer part is stored.
6. Using the embedding equations (EE) each block of payload is embedded by replacing the least three bits of XD band of cover image with the integer part obtained in previous step.
7. To the obtained XD band DFBM is applied to modify it using decision factors. It is done to shuffle the original embedded payload bits position.
8. Add the decimal part obtained in step5 to the modified XD band.
9. The XD band is combined with its sign value stored in step2.
10. Inverse Daubechies Lifting Wavelet Transformation is applied on XA, XH, XV and modified XD band to obtain the stego image.

Table 2 and Table 3 give the payload embedding in decision factor based manner and retrieval of payload from cover image at the destination respectively.

Table3: Retrieval algorithm

Input: Stego image
Output: Payload

1. Decompose the stego image into four bands using Daubechies Inverse Lifting Wavelet Transformation. Detail XD band is used for extracting payload blocks.
2. Retrieve the decimal part of embedded payload blocks from the XD band.
3. To the obtained XD band DFBM is applied to remodify it using decision factors. It is done to get back the original embedded payload bits position.
4. Using the extracting equations (EE), integer part of each block of payload is extracted by retrieving the least three bits of XD band of stego image.
5. In post processing, cube of all four blocks is evaluated and decimal as well as integer part is added correspondingly.
6. Index Reversal is applied to all four blocks of payload.
7. For two alternate extracted payload blocks Haar using Inverse Lifting Wavelet Transformation using is applied.
8. Obtained four payload blocks are defragmented to get the extracted payload image.

V. PERFORMANCE ANALYSIS

The cover images of 1024 x 1024 size and payload images of size 512 x 512 are considered with different image formats. The payloads Boat.jpg, Pepper.tif, Baboon.gif and Camaraman.png are embedded into cover images Lena.jpg, Barbara.tif, Boat.gif and Lena.png respectively to generate corresponding stego images and extracted payloads are shown in Figs. 5-8.

The Table 4 shows the values Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) of cover and stego images as well as original payload and extracted payloads for proposed algorithm. The PSNR of cover image and stego image is calculated and it varies from 48.27db to 49.91db ie., almost independent of cover image formats. The PSNR of original payload and extracted payload is calculated and it varies from 38.61db to 62.59db ie., extracted payload quality depends on payload image formats. The embedding capacity(C) is 0.25bpp. The values of MSE are less than one and vary with payload image formats.

Table4: MSE, PSNR for proposed algorithm

cover image (1024 x 1024)	Format	Payload (512 x 512)	Format	MSE	PSNR (db) Stego image	PSNR (db) Extracted pay load
Lena	JPEG	**Boat**	**JPEG**	**0.9680**	**48.27**	**61.36**
		Baboon	*BMP*	*0.8298*	*48.94*	*38.68*
		Barbara	GIFF	0.7423	49.42	40.36
		Peppers	TIFF	0.9187	48.49	46.72
		Cameraman	PNG	0.8763	48.70	53.92
Boat	BMP	**Lena**	**JPEG**	**0.7363**	**49.46**	**62.59**
		Baboon	*BMP*	*0.7111*	*49.61*	*38.61*
		Barbara	GIFF	0.6632	49.91	40.36
		Peppers	TIFF	0.7580	49.33	46.72
		Cameraman	PNG	0.7420	49.53	53.92
Lena	PNG	**Boat**	**JPEG**	**0.8442**	**48.86**	**61.36**
		Baboon	*BMP*	*0.7507*	*49.37*	*38.68*
		Barbara	GIFF	0.6824	49.79	40.36
		Peppers	TIFF	0.8125	49.03	46.72
		Cameraman	PNG	0.7672	49.28	53.92
Boat	GIFF	**Lena**	**JPEG**	**0.7805**	**49.20**	**62.59**
		Baboon	*BMP*	*0.7486*	*49.38*	*38.68*
		Peppers	GIFF	0.7305	49.49	46.34
		Barbara	TIFF	0.7559	49.76	40.36
		Cameraman	PNG	0.7760	49.23	53.92

Barbara	TIFF	**Boat**	**JPEG**	**0.7760**	**49.23**	**61.36**
		Baboon	*BMP*	*0.8115*	*49.03*	*38.68*
		Barbara	GIFF	0.7593	49.32	40.36
		Peppers	TIFF	0.8626	48.77	46.72
		Cameraman	PNG	0.8320	48.92	53.92

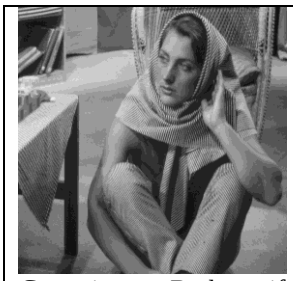
Cover image: Lena.jpg

Payload: Boat.jpg

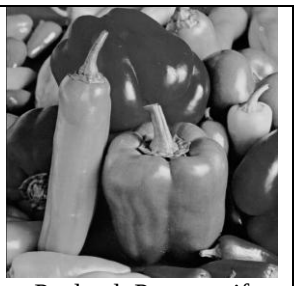
Stego image: Lena.jpg

Retrieved payload Boat.jpg

Fig. 5: Lena (1024 x 1024) and Boat (512 x 512) payload



Cover image: Barbara.tif

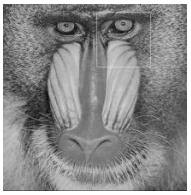


Payload: Peppers.tif

Stego image: Barbara.tif

Retrieved payload Peppers.tif

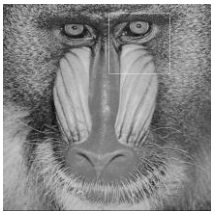
Fig. 6: Barbara (1024 x 1024) and peppers (512 x512) payload



Cover image: Boat.gif

Stego image: Boat.gif

Payload**:** Baboon.tif



Retrieved payload Baboon.tif

Fig. 7: Boat (1024 x 1024) and baboon (512 x512) payload

Cover image: Lena.png

Payload: Cameraman.png

Stego image: Lena.png

Retrieved payload Cameraman.png

Fig. 8: Lena (1024 x 1024) and cameraman (512 x512) payload

The Table 5 shows the results of PSNR for the different cover image formats and size 1024 x 1024 with boat as the payload of JPEG format with size 512 x 512. The quality of extracted payload and stego image are good in the proposed algorithm since PSNR are 48.86 and 61.36 respectively

Table: 5 PSNR variations with cover image formats for Payload Boat. jpg (512 x 512)

Cover image (1024 x 1024)	Capacity (bpp)	PSNR (db) (Cover to Stego image)	PSNR(db) (Original Payload to extracted payload)
Lena. JPEG	0.25	48.27	61.36
Lena. PNG	0.25	48.86	61.36
Barbara.TIFF	0.25	48.63	61.36

The Table 6 shows the PSNR with variable payload sizes for the cover image Lena. jpg format and size 1024 x 1024 with boat as the payload of jpg format with different sizes.

As payload size increases PSNR of cover and stego images decreases whereas PSNR of original Payload and extracted payload increases.

TABLE 6 PSNR with variable payload sizes

Cover image	Payload	Payload Size	PSNR (Cover to Stego image)	PSNR (Payload to extracted payload)
Lena. JPEG (1024 x 1024)	Boat JPEG	32 x 32	53.9361	42.5202
		64 x 64	53.7944	44.3152
		128 x 128	53.2435	44.9541
		256 x 256	51.5732	55.2538
		512 x 512	48.2756	61.3622

Table 7 shows the comparison of PSNR and capacity for the existing Authentication/ Secret Message Transformation through Wavelet Transform based Sub band Image Coding (WTSIC) [21] and the proposed algorithm for Lena JPEG format. It is observed that the PSNR and Capacity is higher in the case of proposed algorithm compared to the existing algorithm for jpg image format with cover image size 512 x 512 and payload size 128 x 128.

Table7: Comparison of PSNR and capacity

Algorithm	PSNR	Capacity
Existing (WTSIC) [15]	42.04	0.0625
Proposed WSSSP	48.25	0.25

VI. CONCLUSION AND FUTURE WORK

Steganography is a technique to hide messages, where the messages can be an image or an audio file transmitted in a suitable carrier. In this paper WSSSP Steganography algorithm is proposed. The Dubechies LWT is used for cover image and Haar Integer LWT is used for payload to convert spatial domain to frequency domain. The bit reversal is applied on each coefficient of payload blocks to scramble payload and scale down the number of coefficient bits. The one more level of scrambling DFBM is done on stego object to increase security level to payload. The ILWT is applied to generate stego image in spatial domain. It is observed that the value of PSNR and capacity are better in the proposed method compared to existing method with high security to the payload. In future the proposed algorithm can be verified with different transform domain techniques.

REFERENCES

1. Guangjie Liu, Yuewei Dai, and Zhiquan Wang, "Breaking Predictive-Coding-Based Steganography and Modification for Enhanced Security," International Journal of Computer Science and Network Security, pp.144-149, vol.6, no.3B, March 2006.
2. Yuan-Hui Yu, Chin-Chen Chang and Iuon-Chang Lin, "A new steganographic method for color and grayscale image hiding", Elsevier journal Computer Vision and Image Understanding 107, pp-183–194, 2007.
3. Shashikala Channalli and andAjay Jadhav, "Steganography An Art of Hiding Data," Journal of Computer science and Engineering, pp.137-141, vol.1 (3), 2009.
4. K. Munivara Prasad, V.Jyothsna, S.H.K. Raju and S.Indraneel, " High Secure Image Steganography in BCBS Using DCT and Fractal Compression," International Journal of Computer Science and Network Security, pp.162-170, vol.10 no.4, April 2010.
5. Weiqi Luo; Fangjun Huang; Jiwu Huang "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE transactions on Information Forensics and Security, vol.5, issue.2, pp.201-214, June 2010.
6. Der-Chyuan Lou, Nan-I Wu, Chung-Ming Wang, Zong-Han Lin and Chwei-Shyong Tsai, "A novel adaptive steganography based on local complexity and human vision sensitivity", The Journal of Systems and Software 83 (Elsevier), pp. 1236–1248, 2010.
7. A. A. Zaidan, B. B. Zaidan, Y. Alaa Taqa, M. Kanar Sami, Gazi Mahabubul Alam and A. Hamid Jalab, " Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem", International Journal of the Physical Sciences, vol. 5(11), pp. 1776-1786, September 2010.
8. Pei-Yu Lin and Chi-Shiang Chan, "Invertible secret image sharing with steganography", Elsevier Pattern Recognition Letters 31, pp.1887–1893, 2010.
9. Marghny Mohamed, Fadwa A-Afari 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.
10. Lokeswara Reddy, A. Subramanyam and P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats," International journal of Advanced Networking and Applications, pp.868-872, vol.2 (5), 2011.
11. Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, International Journal of Computer Science and Security, pp.561-570, vol. 4, issue. 6, 2011.
12. Chia-Chun Wu, Shang-Juh Kao and Min-Shiang Hwang, "A high quality image sharing with steganography and adaptive authentication scheme" The Journal of Systems and Software 84(Elsevier), pp.2196-2207,2011.
13. Yuting Su,ChengqianZhang N and ChuntianZhang," A video steganalytic algorithm against motion-vector-based steganography", Elsevier Signal Processing 91, pp. 1901–1909, 2011.
14. Zhili Chen, Liusheng Huang, Haibo Miao, Wei Yang and Peng Meng, "Steganalysis against substitution-based linguistic steganography based on context clusters", Elsevier Computers and Electrical Engineering 37, pp.1071-1081, 2011.
15. J K Mandal and madhumita Sengupta, "Authentication/ Secret Message Transformation through Wavelet Transform based Subband Image Coding (WTSIC)" International Symposium on Electronic System Design, pp. 225 – 229, 2010.

AUTHORS PROFILE

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 ursuing 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 86 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.