Image Steganography Based on Mantissa Replacement using LWT

N Sathisha[1], K Suresh Babu[2], K B Raja[2], K R Venugopal[3]

[1]*Department of ECE, Govt. S K S J Technological Institute, Bangalore, India.*
[2]*Department of ECE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India.*
[3]*Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India.*

***Abstract*—Steganography is an art and science of hiding confidential information into a cover media to ensure the security of information over the communication channel. The concept of replacing mantissa part of cover image by the generated mantissa part of payload is proposed for higher capacity and security. The Lifting wavelet Transform (LWT) is applied on both cover image and payload of sizes a *a and 3a * 2a respectively. The mantissa values of Vertical band (CV), Horizontal band (CH) and Diagonal band (CD) of cover image are removed to convert into real values. The approximation band of payload is considered and the odd column element values and even column element values are divided by 300 and 30000 respectively to generate only mantissa part of payload. The modified odd and even column vector pairs are added element by element to form one resultant vector. The column vector elements of cover image and resultant column vector elements of payload are added to generate stego object, column vector elements corresponding to vertical, horizontal and diagonal elements. The inverse LWT is applied to generate stego image.**

***Index Terms* - Steganography, LWT, Stego image, Payload, Mantissa.**

I. INTRODUCTION

The rapid growth in modern communication like wireless networks and the internet requires security to protect data, resources and to guarantee the authenticity from network based attacks. The important methods employed to protect the confidential information are cryptography, digital water marking and steganography. Cryptography is a method of protecting confidential information by scrambling and mapping pieces of data into cipher text with a key. Digital water marking is the process of embedding information (watermark) into digital multimedia contents such that the information can later be extracted to ascertain the authenticity of the object. Steganography is a word originated from Greek which literally means *covered or hidden writing*. Steganography is an art and science of hiding confidential information into a cover media to ensure the security of information over the communication channel. The cover objects are digital files like Images, video clips, text, music, sound and other digital mediums. The text steganography is the most difficult technique due to lack of redundant information in a text file compared to an image or a sound file. Digital images are of more concern for steganography because images contain more redundant information. Many types of images have been used as cover media like Bitmap File Format (BMP), Joint Photographic Experts Group (JPEG) and Graphics Interchange Format (GIF) images, JPEG is the common image format for internet and local usage, since it provides large compression ratio and maintains high image quality.

The basic block diagram of image steganography is shown in Fig1. The secret information is embedded into the cover image using an embedding algorithm. Embedding algorithm is a steganographic technique that will embed the secret image into the cover image such that intruder is unable to detect the confidential information. The embedding algorithm will generate stego image. Stego image is same as the cover image containing secret image inside it. This stego image is communicated over the channel. At the receiver end an extraction algorithm is used to extract the secret image from the stego image.

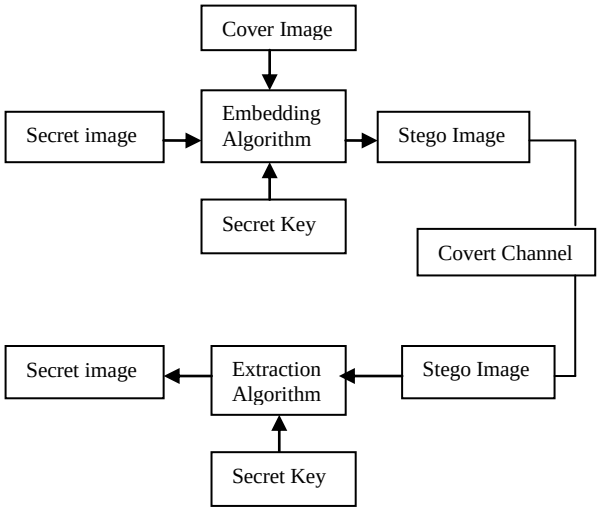


Fig 1. Block diagram of image steganography

The steganography is categorized into (i) Spatial domain based steganography includes the LSB replacement and Bit Plane Complexity Steganography (BPCS). The LSB technique is the most significant example of spatial domain embedding wherein the LSBs of the cover image is substituted by the MSBs of the payload. The BPCS steganography hides secret data by means of block replacing. Each image plane is segmented into the same size pixel-blocks (a typical size of 8*8) which are classified into

ISSN: 2278 – 1323

informative and noise like blocks. The noise like blocks is then replaced with the secret blocks. Palette based steganography is generally used for the color images which are represented in the color luminance model like Y Cb Cr. Images transformed into the palette based color representation can be widely used over the internet which involves hiding the stego message into the palettes or indices of cover image. (ii) Transform domain steganography: in which secret information is embedded in the transform coefficients. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) 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) Document based steganography embeds data in document files by adding tabs of spaces to text or doc files. (iv) File structure based steganography embeds secret data in the redundant bits of cover file. The method is immune to visual attack and the statistical detection. (v) Steganography based on video compression encoding and (vi) Spread spectrum techniques.

The most important requirements for steganography are (i) good visual/statistical imperceptibility of the payload which is essential for security of hidden communication. (ii) Payload capacity: means the maximum number of bits that can be hidden with an acceptable resultant stego image quality and (iii) Robustness: is the ability of stego image to retain its contents from attacks. Steganography is employed in various applications like copy right control of materials, enhancing robustness of image search engines and smart identity cards, video-audio synchronization, protection of intellectual property, exchange of highly confidential data in a covert manner and bank transactions.

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 new concept of replacing cover image mantissa parts of detailed bands of LWT by payload mantissa parts of manipulated approximation band of LWT is used to generate stego image.

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 are discussed in section IV. In section V performance analysis is discussed and conclusions & future work is discussed in section VI.

II. RELATED WORK

Olioulislam et al., [1] developed a steganographic technique to hide data in bitmap image using the concept of LSB verification method. The method uses three colours of image pixels to define the embedding position of secret bit into the fourth colour. Vikas et al., [2] proposed a Least Significant Bit (LSB) steganography method using midpoint circle approach. The midpoint circle approach is used to hide message. The method overcomes the disadvantages of regular LSB system resulting in difficult to detect the secret information and improves the security level. Hayat et al., [3] proposed a steganography method for hiding patient's confidential information. Pixel Value Differencing (PVD) is used to identify contrast regions in the image and a hamming code that embeds three secret message bits into four bits of the cover image. The embedding is performed using the region of noninterest. Shalu and Monika Mathur [4] proposed a method to hide scrambled secret image into cover image using fractional Fourier transform with wavelet coefficients. Arnold transform is applied on cover image with key to maintain high security followed by DWT to the cover image and secret image. The cover image and secret image is added using a technique called alpha bending. Scrambled secret image is generated using IDWT. Lakshmi et al., [5] proposed a comparison of LSB based and histogram shifting based reversible data hiding based on grayscale division. In LSB substitution data hiding method the secret information is embedded in the LSB of the cover image. In Histogram shifting method the pixel value of the cover image is either increased or decreased by one to carry one bit of secret data.

Yinan Wang [6] proposed a steganographic algorithm for preserving the histogram of the cover images in the stego images and minimizing visual distortions. The gray scale images are partitioned into small segments based on the intensity value and the same intensity secret images are embedded into the cover image. Randomization is employed to ensure the preservation of the histogram of cover images. Prabhakarn et al., [7] proposed a steganography method based on DWT and IWT. The secret image is embedded into cover image using fusion process. Various combinations of DWT and IWT are applied on both images to improve the stego quality. DWT and IWT domain steganography is more secure with secret key and certain robustness. Juan [8] developed a method for secret key steganography using image to embed message with unaltered pixel information. The transmitted stego key is modified which maps the information in the unaltered cover image. The original message is reconstructed by the receiver using the seeds of pseudo random generators, included in the stego-key. Sunny dagar [9] developed a image steganography using two secret keys to randomize the bit hiding process. Use of two secret keys enhances the security of secret information. Secret information bits are placed at the random positions of the pixels. The random positions are calculated based on two secret keys. The hidden information is highly randomized so it is difficult for attacker to retrieve the secret information from stego image. Bingwenfeng et al., [10] proposed a binary image steganographic scheme to minimize the embedding distortion on the texture. The steganographic scheme generates the cover vector by dividing the scrambled image into super pixels and syndrome trellis code is employed to minimize the embedding distortion. The complement, rotation and mirroring-invariant local texture patterns are extracted from the binary image. The changes in complement, rotation and mirroring-invariant local texture patterns distortion show a strong relationship with the detectability of the embedding distortion. The flipping distortion measurement is set with the weighted sum of complement, rotation and mirroring-invariant local texture patterns changes, where the weight is empirically assigned according to the discrimination power of the complement, rotation and mirroring-invariant local texture patterns histogram.

ISSN: 2278 – 1323

OuldMedeni and MamounSouidi [11] proposed a steganographic method in spatial domain for gray scale images based on four pixel differencing and LSB substitution. The secret information is hidden into each pixel by the k^{th} bit LSB substitution method, where k is decided by the number of 1's in the most part of pixel. Rui Song Ye et al., [12] proposed a technique of hiding a digital image using matrix decomposition. The quality of the stego image enhanced with low extra computational complexity. Moazzam Hossian et al., [13] proposed variable rate embedding technique using three different steganographic methods for gray scale images. Four diagonal and eight neighbourhood methods utilize a pixel's dependency on its neighbourhood and psycho visual redundancy to evaluate the smooth areas and edged areas in the image. Three bits of secret information bits are embedded in smooth areas whereas variable rate bits are embedded in edged areas. Radu-loan Ciobanu et al., [14] implemented steganography and cryptography over network protocols. The protocols for data hiding are ICMP and UDP. The security is increased by compression and encryption techniques. The two developed scenarios are, first method describes about hiding data in the image files and second method is less conspicuous and it can be integrated based on TCP connection.

Gopalan K [15] proposed a method for hiding information in the frequency domain of an audio or image cover medium, which can be further extended to video frames by exploiting the human imperceptibility of auditory and visual system to minute changes in the spectrum. To achieve this different pairs of frequencies for each frame is used. Pedro N. Safier et al., [16] made an attempt to analyze the possibility of sending stego object using a digital communication channel. The secret message is added as noise to the cover image. The performance of a steganographic channel in terms of bit error rate, detect ability, stego payload limits and impact of binary capacity is analyzed. Chao Wang et al., [17] proposed a content adaptive steganographic scheme. The specific selection of cover image pixel and neighboring pixel is done to embed the secret information. The redundant pixels are identical and embedded in order to improve the conventional LSB method. MichiharuNiimi et al., [18] have shown a method to apply BPCS steganography to palette based images which consists of palettes storing color vector information and an index image whose pixel value corresponds to the index in the palettes using color quantization. Almohammad and Ghinea [19] investigated the relationship between PSNR and subjective quality of stego image. The commonly used performance parameter PSNR cannot be reliably used since it has poor correlation with mean opinion score. Hence PSNR alone cannot be used to express stego quality. Marwaha P and Marwaha P [20] proposed a technique for encrypting data that combines the features of steganography, cryptography along with multimedia data hiding. Data embedding into images changes its color frequencies in a predictable way. The concept of cryptography is proposed where the data will be encrypted into a cipher and cipher will be hidden into a multimedia image file in encrypted format.

Weiming Zhang et al., [21] proposed the N page construction for wet paper coding using which a family of wet paper codes can be generated. N page construction is a generalization of the paper folding method and an equivalent version of wet zzw construction. Tao Zhang et al., [22] proposed a technique to resistant the analysis of histogram. The improved BPCS steganography takes different measures to deal with bit plane accordingly. BPCS steganography carries on different processing's to different bit planes, with setting high threshold value at the high bit plane and low threshold value at the low bit plane. The algorithm also provides good visual imperceptibility and data embedding capacity along with the capability of resisting the analysis of whole complexity algorithm. Wang Yan and Ling-di Ping [23] proposed a steganography algorithm based on spatial domain to hide a large amount of information into color BMP image. It utilizes the arrangement of the secret data to compensate distortion, which is called fixed LSB substitution methods. The algorithm can reach the high capacity with good image quality. Ling Xi et al., [24] proposed an algorithm based on complementary modification to eliminate the influence of Histogram of LSB matching steganography and intensify the capability of statistical analysis resistance. The modification amplitude and the number of modified pixels are same thus this algorithm keeps the good visual invisibility and high embedding capacity of LSB matching.

Kumar and Newman [25] discussed different types of Steganalysis attempts and proposed a JPEG steganography that provides high embedding capacity with zero-deviant histogram restoration. The algorithm uses stop points in its header structure that allows it to restore the algorithm completely, making its detection impossible by any first order steganalysis. Ching-Sheng Hsu and Shu-Fen Tu [26] proposed a technique that can be used to embed the secret information in the LSB bits of the cover image and to overcome the issues of security. To construct an LSB substitution matrix Ant colony Algorithm is applied. The algorithm constructs the LSB substitution matrix within little iteration even though the search space is large. Shang-Kuan Chen and Ran-Zan Wang [27] proposed a High payload image hiding scheme using best block matching approach. The method divides the image into multiple non-overlapping blocks. For each block a K-way block matching procedure is designed to search for the most similar block from 'K' sets of 2^n candidate blocks. K base modulus operation is applied which enlarges the searching space of an n-bit index to $kX2^n$ candidate blocks, which reduces the quantity of the data should be recorded, hence increases the quality of the embedding results.

Shahzad Alam et al., [28] proposed a secret key based random LSB substitution for hiding confidential information. The capacity is improved by using canny edge detection based pixel dependency. The canny edge detection assists in generating a better quality stego image. Cherukuri Balakrishna et al., [29] proposed a Single Digit Sum (SDS) based image steganography scheme. The SDS is obtained by adding the digits of a given number. The SDS is used in image steganography to reduce embedding noise. A 3 bit message string is embedded in a pixel such that the SDS of the changed pixel value in the stego image equals the decimal equivalent of the 3 bit message string. Sumedha Sirsikar and JagniliSalunkee, [30] proposed a data hiding at method that combines the features of Hamming, Optimal Pixel Adjustment Procedure (OPAP). Zig – Zag modified and adaptive technique. Comparison of all the methods show that adaptive data hiding method gives the better results. Linjie Guo et al., [31] presented a JPEG steganographic scheme using syndrome trellis coding and uniform embedding strategy. A uniform embedding distribution function for both

ISSN: 2278 – 1323

non side informed and side informed JPEG steganography to incorporate the uniform embedding.

III. MODEL

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

A. Definitions

In this section definition of evaluation parameters has been discussed.

(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. It 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 the image.

X_{ij} : The value of the pixel intensity in the cover image/original payload.

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

2) Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e. it measures the percentage of the stegano data to the image percentage. PSNR is calculated using Equation 2.

$$PSNR = 10\log_{10}(255^2/\ MSE)\ dB \qquad (2)$$

3) 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 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).

$$Capacity = (P_{ij} / C_{ij}) \qquad (3)$$

Where, Pij is the payload image dimensions,

Cij is the cover image dimensions.

B. Embedding model

In the proposed method, the new concept of embedding payload into the mantissa part of cover image by converting payload into mantissa part. The flow chart of the proposed embedding model is as shown in Fig. 2.

(i) Cover image: The cover image is of equal (a, a) size and format is considered to test the performance analysis. The cover image is resized to a square matrix dimensions for embedding payload for better performance.

(ii) Payload: The secret image to be transmitted is embedded into cover image to generate a stego image. The payload image is resized to dimension of (3a, 2a). The payload may be of any format.

(iii) Lifted Wavelet Transform 2 (LWT2) [32]: The main feature of the lifting scheme is that all constructions are derived in the spatial domain. It does not require complex mathematical calculations that are required in traditional methods. Lifting scheme is simplest and efficient algorithm to calculate wavelet transforms. It does not depend on Fourier transforms.

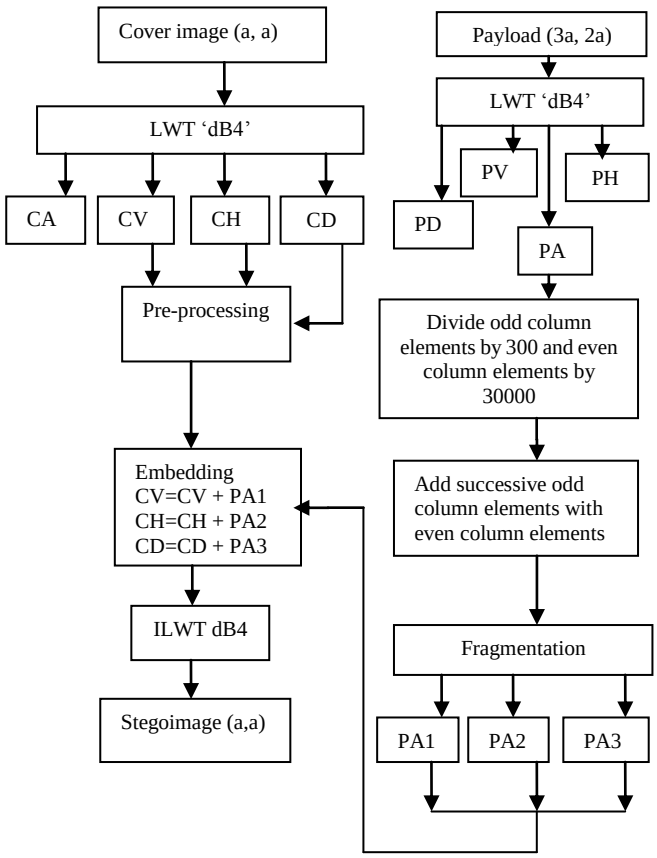


Fig. 2. Embedding flow chart of proposed algorithm

Lifting scheme is used to generate second-generation wavelets, which are not necessarily translation and dilation of one particular function. The lifting scheme of wavelet transform has the following advantages over conventional wavelet transform technique. (i) It allows a faster implementation of the wavelet transform. It requires half number of computations as compare to traditional convolution based discrete wavelet transform. This is very attractive for real time low power applications. (ii) The lifting scheme allows a fully in-place calculation of the wavelet transform. In other words, no auxiliary memory is needed and the original signal can be replaced with its wavelet transform. (iii) Lifting scheme allows us to implement reversible integer wavelet transforms. In conventional scheme it involves floating point operations, which introduces rounding errors due to floating point arithmetic.

Constructing wavelets using lifting scheme consists of (i) Split phase (ii) Predict phase (iii) update phase as shown in Fig 3.

The first step in the lifting scheme is to separate the original sequence (X) into two sub sequences containing odd indexed samples and even indexed samples. This sub sampling is called as lazy wavelet transform

$X_o : d_i \leftarrow X_{2i+1}$

$X_e : s_i \leftarrow X_{2i}$

ISSN: 2278 – 1323

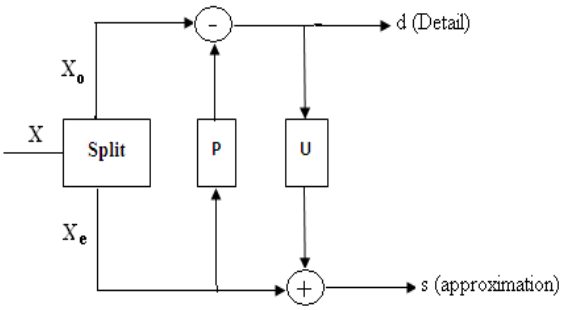


Fig.3. Lifting scheme implementation

The prediction phase is also called dual lifting (P). This is performed on the two sequences Xo and Xe which are highly correlated. Hence, the predictor P can be used to predict one set from the other. In this step the odd sample are predicted using the neighbouring even indexed samples and the prediction error is recorded replacing the original sample value, thus providing in- place calculations.

$$d_i \leftarrow d_i - P\langle S_A \rangle$$

Where, $A = \left(i - \left[{}^{N}/_{2}\right] + 1, \ldots\ldots\ldots\ldots\ldots\ldots i + \left[{}^{N}/_{2}\right]\right)$

N = number of vanishing moments in d. this sets the smoothness of the P function.

Update phase is the second lifting step also called as primal lifting (U). Here the even samples are replaced with smoothed values using update operator (U) on previously computed details. The U operator is designed to maintain the correct running average of the original sequence, to avoid aliasing.

$S_i \leftarrow S_i + U(d_B)$

Where, $B = \left(i - \left\lfloor {}^{\widehat{N}}/_{L} \right\rfloor, \ldots\ldots\ldots\ldots i + \left\lceil {}^{\widehat{N}}/_{L} \right\rceil - 1\right)$

$\widehat{N}$is the number of real vanishing moments

The U operator preserves the first $\widehat{N}$ moments in the S sequence, The lazy wavelet is lifted to a transform with required properties by applying dual and primal lifting pair of operations one or more times. Finally, the output streams are normalized using the normalizing factor K.

$d_i \leftarrow d_i - {}^{1}/_{k}\, s_i \leftarrow s_i * k$

The output from the S channel after the dual lifting step provides a low pass filtered version of the input, where as the output from the d channel after the dual lifting steps provide the high pass filtered version of the input. The inverse transform is obtained by reversing the order and sign of the operations performed in the forward transform.The dB4 LWT is applied on resized cover image to transform from spatial domain to wavelet domain bands such as CA, CH, CV and CD. The CA band has significant information hence CA band is not used for embedding. The CH, CV and CD sub bands are detailed bands and has high frequency components with insignificant information of cover image hence used for embedding. The LWT-dB4 is applied on payload and consider only approximation band PA since it has significant information of payload.

(iv) Pre processing: The mantissa part of the detailed bands CH, CV and CD are removed and only real part is retained.

(v) Embedding: The Approximation band (PA) of payload is considered and the odd column vector values are divided by 300 to obtain the result in mantissa part of first two digits say 0.xx and the even column vector values are divided by 30,000 to obtain the result in mantissa part of third and fourth digits say 0.00xx. The resultant matrix is considered and the successive odd column elements are added with even column elements to reduce the column size of payload. The reduced matrix is further decomposed into 3 blocks PA1, PA2 and PA3 of equal row size called fragmentation. The decomposed blocks PA1, PA2 and PA3 are of same size as that of XV, XH and XD bands of cover image.

The element value of PA1 is added to the XV block, the element value of PA2 is added to the XH block and the element value of PA3 is added to the XD block. The inverse LWT is applied to generate stego image.

C. Extraction model

In this section the proposed extraction model has been discussed and is shown in Fig 4.

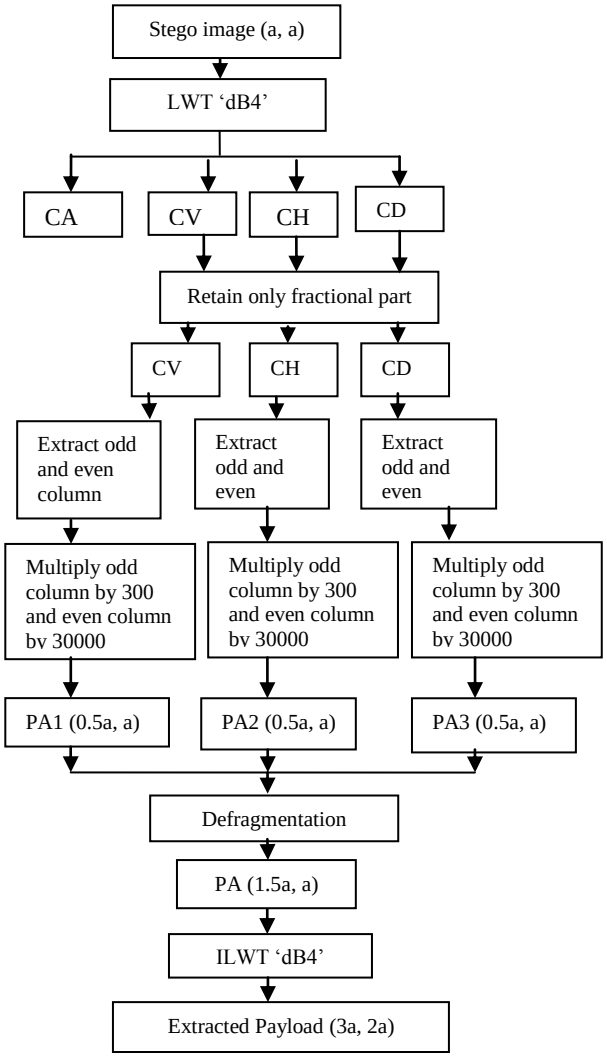


Fig. 4. Extraction flow chart of proposed algorithm

The LWT is applied on stego image to generate Approximation, Vertical, Horizontal and Diagonal bands. The Vertical, Horizontal and diagonal bands are considered and fractional part is retained. The three bands are expanded by generating odd column and even column by choosing two values after mantissa for odd column and last 3rd and 4th values after mantissa. Multiply odd column elements by 300 and even column elements by 30000 to generate 3 different blocks called PA1, PA2 and PA3 of equal row size. The PA1,

ISSN: 2278 – 1323

PA2 and PA3 are considered and ILWT is applied to generate payload.

IV. ALGORITHM

Problem definition: the secret image is embedded into the fractional part of the detailed band of cover image. The new concept to generate stego image is used by dividing PA band of payload and fractional values are embedded into cover image.

Assumptions :(i) The cover and payload objects are gray scale images with different dimensions.

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

Table I. Embedding algorithm of proposed model

Input: Cover and Payload images.
Output: Stego image

1. Transform cover image (a, a) by lifting scheme using Daubechies 'dB4'wavelet.
2. Transform payload (3a, 2a) image by lifting scheme using Daubechies 'dB4' wavelet.
3. The insignificant bands XV, XH and XD of cover image are considered and fractional part is eliminated.
4. The significant band PA of payload is considered and divides odd column element by 300 and even column element by 30000.
5. Successive odd column elements are added with even column elements to reduce the size to (1.5a, 0.5a).
6. Split the matrix into equal 3 blocks of size (0.5a, 0.5a).
7. The first part PA1 is added with XV band of cover image. The second part PA2 is added with XH band of Cover image. The third part PA3 is added with XD band of cover image.
8. Apply inverse lifting wavelet transform to get stego image.

Table I and Table II give the payload embedding in cover image and retrieval of payload from cover image at the destination respectively.

Table II. Retrieving algorithm

Input: Stego image
Output: Payload

1. Transform stego image by lifting scheme using Daubechies 'dB4'Wavelet.
2. Consider only fractional part of Vertical, horizontal and Diagonal bands.
3. Extract odd and even column elements.
4. Multiply the odd column elements by 300 and even column elements by 30000.
5. Combine the 3 different components to generate Approximation band
6. Apply Inverse LWT to generate the payload.

V. PERFORMANCE ANALYSIS

The several images with different sizes and formats are used to test the performance of proposed algorithm. The few cover and payload images such as Lena, Peppers, Boat, Blue hills, Barbara and Mandrill are shown in Fig 4.

a) Lena

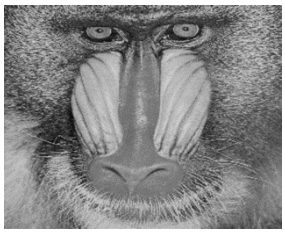
b) Peppers

c) Boat

d) Blue hills

e) Barbara

f) cameraman



g) Mandrill

Fig 4. The sample of cover and payload images.

The PSNR values between stego image and cover image and extracted payload and payload for different cover image and payload formats with different sizes are given in Table III. The PSNR value is around 57 dB between stego image and cover image and varies between 37 to 49 between extracted payload and original payload. The PSNR values between cover and stego image and hiding capacity for proposed and existing algorithms proposed by A M Nickfarjam et al., [33], J K Mandal et al., [34] and Nadeem Akhtar et al., [35] are compared in Table IV.

ISSN: 2278 – 1323

Table. III. The PSNR Values for different sizes and formats of cover image and payload images.

Cover image	Cover size	Payload	Payload size	PSNR (stego image and cover image)	PSNR (payload and extracted payload)
Lena.jpg	128X128	Peppers.png	384X256	56.46	49.92
	256X256		768X512	56.67	49.83
	440X440		1320X880	57.36	49.81
	512X512		1536X1024	57.76	49.77
Barbara.bmp	128X128	Cameraman.tif	384X256	57.12	27.79
	256X256		768X512	57.2	49.78
	440X440		1320X880	57.25	37.15
	512X512		1536X1024	57.33	49.74
Cameraman.tif	128X128	Bluehills.jpg	384X256	57.17	49.95
	256X256		768X512	57.3	49.93
	440X440		1320X880	57.67	49.91
	512X512		1536X1024	57.86	49.90
Peppers.png	128X128	Cameraman.tif	384X256	57.27	28
	256X256		768X512	57.49	49.79
	440X440		1320X880	57.89	36.51
	512X512		1536X1024	57.89	49.74
Boat.gif	128X128	Cameraman.bmp	384X256	57.13	28.16
	256X256		768X512	57.23	49.79
	440X440		1320X880	57.31	36.74
	512X512		1536X1024	57.32	49.74
Mandril.bmp	128X128	Lena.png	384X256	57.21	49.89
	256X256		768X512	57.27	49.92
	440X440		1320X880	57.31	49.93
	512X512		1536X1024	57.29	49.91
Lena.jpg	128X128	Barbara.jpg	384X256	57.34	49.92
	256X256		768X512	57.54	49.91
	440X440		1320X880	58.16	49.91
	512X512		1536X1024	58.52	49.91

It is observed that (i) The PSNR values in the proposed method are high compared to existing methods since only mantissa part of cover image is used for embedding, hence error is low. (ii) The capacity in the proposed algorithm is high compared to existing algorithms since the payload is compressed by adding modified successive column vector elements. (iii) The security to the payload is high since the hacker cannot identify the payload as the odd column elements and even column elements are divided by 300 and 30000 respectively to modify column elements and also successive column vector elements are added to convert into single column which results in payload compression. The compressed payload is embedded into detailed LWT bands of cover image.

Table.IV The comparison of PSNR values and capacity.

Technique	PSNR	Capacity (bpp)
A M Nickfarjam et al., [33]	47.03	0.25
J K Mandal et al., [34]	40.09	0.342
Nadeem Akhtar et al., [35]	41.79	0.25
Proposed	**57.89**	**6**

VI. CONCLUSION

Steganography is an authenticated technique for maintaining secrecy of embedded data. In the proposed method the mantissa part of cover image is replaced by modified mantissa part of payload to improve capacity and PSNR values. The LWT is applied on cover image and payload to generate four sub bands. The approximation band of payload is considered and the coefficient values of odd and even columns are modified by dividing with values 300 and 30000 respectively to generate mantissa values. The mantissa values of vertical, horizontal and diagonal sub bands of cover image are replaced by modified mantissa values of payload to generate stego object. The inverse LWT is used to generate stego image. It is observed that the performance of the proposed algorithm is better compared to the existing algorithms. In future the stego image may be compressed and try to extract payload to test robustness.

ISSN: 2278 – 1323

REFERENCES

[1] Md. OlioulIslam, Md. SazzadHossain, Md. Sayed Hassan Siddique and Durjoy Kumar Saha, "Improving the Non-filtering Steganographic Algorithm using LSB Verification Method," *International Conference on Electrical Engineering and Information & Communication Technology*, pp. 1 – 6, 2014.

[2] VikasVerma, Poonam Rishma and Chawla, "An Enhanced Least Significant Bit Steganography Method using Midpoint Circle Approach," *International Conference on Communications and Signal Processing*, pp.105-108,2014.

[3] Hayat Al-Dmour, AhmedAl-Aniand Hung Nguyen, "An Efficient Steganography Method for Hiding Patient Confidential Information," *IEEE International conference on Engineering in Medicine and Biology Society*, pp. 222 – 225, 2014.

[4] ShaluGarg and Monika Mathur, "Chaotic Map Based Steganography of GrayScale Images in Wavelet Domain,"*International Conference on Signal Processing and Integrated Networks*, pp. 689 – 694, 2014.

[5] Shri Lakshmi Pravalika, C SheebaJoice and Alex Noel Joseph Raj, "Comparison of LSB Based and HS Based Reversible Data Hiding Techniques," *Second International Conference on Devices, Circuits and Systems*, pp. 1 – 4, 2014.

[6] Yinan Wang, Weirong Chen, Yue Li, Wei Wang and Chang Tsun Li, "HPS: Histogram Preserving Steganography in Spatial Domain," *International Workshop on Biometrics and Forensics*, pp. 1 – 4, 2014.

[7] Prabakaran G,Bhavani R, S Sankaran, "Dual Wavelet Transform in Color Image Steganography Method," *International Conference on Electronics and Communication Systems*, pp. 1 -6, 2014.

[8] Juan M Gutierrez-Cardenas,"Secret Key Steganography with Message Obfuscation by Pseudo-random Number Generators," *Thirty Eighth International Computer Software and Applications Conference Workshops*,pp. 164 – 168, 2014.

[9] Sunny Dagar, "Highly Randomized Image Steganography using Secret Keys," *IEEE International Conference on Recent Advances and Innovations in Engineering*, pp. 1- 5, 2014.

[10] Bingwen Feng, Wei Lu and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture,"*IEEE Transactions on Information Forensics and Security*,pp. 243-255, 2014.

[11] M B Ould Medeni and El Mamoun Souidi, "A Novel Steganographic method for Gray-level Images with Four-Pixel Differencing and LSB Substitution," *International Conference on Multimedia Computing and Systems*, pp. 1 – 4, 2011.

[12] Ruisong Ye, "A Novel Digital Image Hiding Scheme Based on Matrix Decomposition," *International Forum on Information Technology and Applications*, pp. 147-150, 2009.

[13] Moazzam Hossain, Sadia Al Haque and FarhanaSharmin, "Variable rate Steganography in Gray scale Digital Images using Neighborhood Pixel Information," *IEEE International Conference on Computers and Information Technology*, pp 267-272, 2009.

[14] Radu-IoanCiobanu, Mihai-OvidiuTirsa,RalucaLupu, Sonia Stan, MugurelionutAndreica, "SCONeP: Steganography and Cryptography Approach for UDP and ICMP," *Tenth Roedunet International Conference*, pp 1-6, 2011.

[15] KaliappanGopalan, "A Unified Audio and Image Steganography by Spectrum Modification," *IEEE International Conference on Industrial Technology*, pp. 1 – 5, 2009.

[16] Pedro N Safier, Iras S Moskowitz and Paul Cotae, "On the Baseband Communication Performance of Physical Layer Steganography," *Forty fifth Annual Conference on Information Sciences and Systems*, pp. 1 – 6, 2011

[17] Chao Wang, Xiaolong Li, Bin Yang, Xiaoqing Lu and Chengcheng Liu, "A Content-Adaptive Approach for Reducing Embedding Impact in Steganography," *IEEE International Conference on Acoustics Speech and Signal Processing*, pp. 1762 – 1765, 2010

[18] Michiharu Niimi, Hideki Noda, Eiji Kawaguchi and Richard O Eason, "High Capacity and Secure Digital Steganography to Palette-Based Images*," International Conference on Image Processing*. pp. 917 – 920, 2002.

[19] Adel Almohammad and Gheorghita Ghinea, "Stego Image Quality and the Reliability of PSNR," *Second International Conference on Image Processing Theory Tools and Applications*, pp.215 – 220, 2010.

[20] Piyush Marwaha and Paresh Marwaha, "Visual Cryptographic Steganography in Images," *International Conference on Computing Communication and Networking Technologies*, pp. 1 – 6, 2010.

[21] Weiming Zhang, Jiufen Liu, Xin Wang and Nenghai Yu, "Generalization and Analysis of the Paper Folding Method for Steganography," *IEEE Transactions on Information Forensics and Security*, pp. 694 – 704, 2010.

[22] Tao Zhang, Zhaohui Li and Peipei Shi, "Statistical Analysis against Improved BPCS Steganography," *Second International Conference on Advanced Computer Control*, pp. 237-240, 2010.

[23] Wang Yan and Ling-di Ping, "A New Steganography Algorithm Based on Spatial Domain," *Second International Symposium on Information Science and Engineering*, pp. 171 – 176, 2009

[24] Ling Xi, Xijian Ping and Tao Zhang, "Improved LSB Matching Steganography Resisting Histogram Attacks," *Third IEEE International Conference on Computer Science and Information Technology*, pp. 203 – 206, 2010.

[25] Mahendra Kumar and Richard Newman, "J3: High Payload Histogram Neutral JPEG Steganography," *Eighth Annual International Conference on Privacy Security and Trust*, pp. 46 – 53, 2010.

[26] Ching-Sheng Hsu and Shu-Fen Tu, "Finding Optimal LSB Substitution Using Ant Colony Optimization Algorithm," *Second International Conference on Communication Software and Networks*, pp. 293 – 297, 2010.

[27] Shang-Kuan Chen and Ran-Zan Wang, "High-Payload Image Hiding Scheme Using k-Way Block Matching," *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 70-73, 2010.

[28] ShahzadAlam, VipinKumar, Waseem A Siddiqui, and MusheerAhmad, "Key Dependent Image Steganography using Edge Detection," *Fourth International Conference on Advanced Computing & Communication Technologies*, pp. 85 – 88, 2014

[29] Cherukuri Balakrishna, velluru Naveen Chandra and RajarshiPal, "Image Steganography using Single Digit Sum with Varying Base," *IEEE International Conference on Electronics, Computing and Communication Technologies*, pp. 1-5, 2014.

[30] SumedhaSirsikar and JagniliSalunkee**,** "Analysis of Data Hiding using Digital Image Signal Processing," *International Conference on Electronic Systems, Signal Processing and Computing Technologies*, pp. 134 – 139. 2014.

[31] LinjieGuo, Jiangqun Ni and Yun Qing Shi, "Uniform Embedding for Efficient JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, Vol. 9, Issue: 5, pp. 814 – 825, 2014.

[32] W Sweldens, "The Lifting Scheme: A Construction of Second Generation Wavelets," *SIAM Journal in Math. Analysis*, Vol. 29, issue. 2, pp.511 – 546, 1998.

[33] A M Nickfarjam and Z Azimifar, "Image Steganography based on Pixel Ranking Swarm Optimization," *Sixteenth International Symposium on Artificial Intelligence and Signal Processing.* pp. 360 – 363. 2012.

[34] J K Mandal and Madhumita Sengupta, "Steganographic Technique based on Minimum Deviation of Fidelity," *Second International Conference on Emerging Applications of Information Technology*. pp. 298 – 301, 2011.

[35] Nadeem Akhatar, Ambreenbano and Faraz Islam, "An Improved Module based Substitution Steganography Method," *Fourth International Conference on Communication Systems and Network Technologies*, pp. 695 – 698. 2014.

N Sathisha received the BE degree in Electronics and Communication Engineering from Bangalore University and the M. Tech degree in Digital Communication and Networking from Visvesvaraya Technological University Belgaum. He is pursuing Ph.D. in Computer Science and Engineering of Bangalore University under the guidance of Dr. K Suresh Babu, Associate Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering. He is currently an Assistant Professor, Dept. of Electronics and Communication Engineering, Govt. SKSJ Technological Institute, Bangalore. He has over 11 research publications in refereed International Journals and Conference Proceedings. His research interests include Computer and information security, computer networks, Image processing and Communication Engineering. He is a life member of Indian Society for Technical Education, New Delhi. He is a life member of Institute of Electronics and Telecommunication Engineers, New Delhi

ISSN: 2278 – 1323

K Suresh Babu is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME 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 25 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, Signal Processing,

K B Raja is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME 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 126 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, computer networks.

K R Venugopal is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Master's degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 275 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.

ISSN: 2278 – 1323