Image Steganography using Non Embedding and Average Technique in Transform Domain

N Sathisha, K Suresh Babu, K B Raja, K R Venugopal

Abstract— The steganography is an art and science of hiding information into a given media to ensure the security of information over the communication channel. In this paper we propose a Image Steganography using Average Technique in Transform Domain (ISATT). The Lifting Wavelet Transform (LWT) is applied on both cover image and payload. The Diagonal band (CD) of cover image and Approximation band (PA) of payload are segmented into N x N blocks. The N x N matrix of PA is divided by N x N matrix of CD to generate resultant matrix based on Non Embedding Threshold Value (NETV) fixed by key. The average value of N x N resultant matrix is calculated and used to divide PA to generate modified CD. The average value of each N x N block are scale downed by key and embedded into corresponding N x N block of horizontal band (CH) of cover image. The inverse LWT is applied on stego object to derive stego image1. The Peak Signal to Noise Ratio (PSNR) is computed between cover image and stego image1 for different NETV values till maximum PSNR is obtained and the corresponding stego image is considered as final stego image. The capacity and PSNR values are high in the case of proposed algorithm compared to existing algorithms since non embedding and average technique is used in transform domain.

Index Terms— Steganography, Stego image, Payload, Cover Image, Non LSB, LWT.

1 INTRODUCTION

Online banking transaction and resource sharing on the internet communication certainly requires security. Development of security for communication is evolved from long back. The secrecy of confidential information was maintained by writing information on pieces of paper using invisible ink so that the paper appears to be a blank piece of paper for ordinary people. The authorized recipient extracts the confidential information by dipping the paper into the liquids such as urine, milk, vinegar etc., the rapid developments in the digital technology leads to the evolution of security techniques among those cryptography, watermarking and steganography are the most important method. 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. Steganography is the art and science of hiding secret information by embedding messages within other. In Greek steganography means “covered writing” in modern steganography the confidential information is embedded into digital multimedia files and also at the network packet level. The digital multimedia files may be text, audio, video or images. Images are most widely used because an image consists of more redundant information and human visual system can’t detect the variation in luminance of color vectors at higher frequency ends of the visual spectrum. Image steganography is the method of hiding data into cover image and generates a stego image this stego image is sent to the other party trough communication channel where the opponent does not know that this stego image consists of confidential information at the receiving end the confidential information is extracted with or without stego key.

The common image steganography techniques are (i) Least Significant Bit (LSB) 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), Dual Tree Complex Wavelet Transform (DTCWT) etc., and confidential information.

The important requirements of steganography are (i) Invisibility: - the strength of steganography lies in its ability to be unnoticed by the human eye, (ii) Payload capacity: - the maximum amount of secret information can be embedded into cover image. (iii) Robustness against statistical attacks: - how much the stego image is intact if it pass through transformation such as scaling, filtering, cropping and addition of noises. (iv) Computational complexity: - how much it is computationally expensive during embedding and extracting of a hidden message.

Steganalysis [1] is the reverse process of steganography. The aim of steganalysis process is to break steganography systems. The steganography process starts with a set of suspected information streams. Then the set is reduced with the help of advanced statistical methods. The three main types of steganalysis are (i) visual detection steganalysis:- a set of stego images are compared with original cover images and note the visible difference. (ii) Statistical detection steganalysis:- are powerful and successful because they reveal the smallest alterations in an images. This attack is further classified as passive and active attacks. Passive attack deal with identifying the presence or absence of a covert message or the embedding algorithm used etc. whereas the active attacks is to estimate the embedded message length or the locations of the hidden message or the secret key used in embedding. (iii) structural attacks are based on fact that format of the data files often changes as data to be hidden are embedded, on identifying these characteristic structure changes can detect the existence of image. Applications of steganography are confidential
communication and secret data storing, copyright protection of electronic products, Bank Transactions, Healthcare information, Internet security, Authentication and Information assurance etc.

**Motivation:** Due to increasing demand for privacy and security, a need of 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 non embedding steganography using average technique in transform domain is proposed. The new concept of average value of matrix obtained using division of PA by CD is used to generate stego image. The quality of stego image is improved by using different values of NETV.

**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 described in section 3. Section 4 discusses the algorithm used for embedding and extraction. In section 5 Performance analysis is discussed and conclusion future work is discussed in section 6.

## 2 RELATED WORK

Mehdi Hussain and M Hussain [2] proposed an algorithm to embed the data around the edge boundary of cover image. The cover edge computation is done by sobel or canny edge detector. The stego image is utilized for segmentation process. The technique shows high PSNR with low data capacity. Changcheng Li et al., [3] proposed LSB information hiding algorithm based on Lifting Wavelet Transform Technique (LWT). The pre-processing of secret information is done by LWT. The secret information replaces the random noise using the lowest plane embedding secret information to avoid noise and attacks. Hui-yu hang and shih-hsu chang [4] presented a lossless data hiding method based on quantized coefficients. The subbands obtained after DWT are quantized to generate quantization factors. The secret information is embedded into the successive zero coefficients of the medium - high frequency components of cover image. The algorithm shows high embedding capacity and acceptable stego image quality. Yizhen chen et al., [5] proposed an adaptive steganography algorithm based on block sensitivity vectors using human visual system features. The images is divided into 8 X 8 blocks and analyze the mean, variance and entropy value of gray scale image for each block then sensitivity vectors are calculated. The embedding scheme is decided dynamically based on sensitivity vectors.

Mohammad Iaved khorsavi and Samaeh ghandali [6] presented a steganography based on secret sharing method. The cover image is transformed into frequency domain using IWT. The secret image is divided into shares using cryptography and these shares are embedded into coefficients of cover image. Reconstruction of the secret image is done by extracting the shares and rebuilt the extracted shares to generate original secret image. Mehdi Hussain and Mureed Hussain [7] proposed a data embedding method based on pixel intensity. The originality of secret message is modified by applying XOR operation an all bytes with the 8 bit secret key. The modified secret message is hidden into the cover intensity pixels of cover image. S K Mutt and Sushil Kumar [8] presented a image steganography based on slantlet transform and T – codes. The message is encoded using the T codes and the cover image is decomposed into four sub bands HH, HL, LH and LL using slantlet transforms. The encoded message is embedded in high frequency components of cover image.

Hossein Miar Naimi and Bagher Ramazannia [9] presented a steganographic method using Run Length Code (RLC) and Modular arithmetic. The cover image is segmented into blocks of pairs of successive pixels. The run values 0 and 1 are rearranged and run count is obtained. The run counts are embedded in two pixel blocks of cover image which limits the local destruction. Embedding process uses the modular arithmetic. Sara ershadi nasab and Hassan agheinia [10] proposed a method of hiding messages in digital images using integer to integer wavelet transform. The image is divided into subbands of 8 X 8 blocks and constructs bit planes of each block. The capacity of each block is calculated. If the capacity is one the LSB 1/3 used and if capacity is more than one the rounding method for embedding of secret information into digital images is used. Elzbieta zielinska and Krzysztof sozczyiorski [11] developed a steganographic coding scheme using direct sequence spreading technique for IEEE 802.15.4 the embedding of additional content into IEEE 802.15.4 data symbols which ensures a high steganographic data rate by maintaining good performance characteristics. Shivakumar et al., [12] proposed a discrete and integer wavelet transform technique for robust steganography. The cover image is segmented into 4X4 blocks. DWT is applied on each block to obtain 2X2 blocks. The vertical band of 2X2 is considered and IWT is applied to obtain 1X1 block. The DWT and IWT are applied to payload. The payload is is embedded into coefficients of cover image using LSB replacement method. Ahmed A Abdelwahab and lobna A Hassaan [13] developed an image data hiding technique based on DWT. The cover image and secret image is decomposed into four sub images using linear phase two channel integer filter bank. Each sub images are partitioned into 4x4 pixels. The best matched block which has minimum error is searched using the root mean square error method and secret image block is embedded. Cover image by best matched block of minimum error which is searched root mean squared error.

Sunny Sachideva and amit kumar [14] proposed a steganographic method based on JPEG and a Modified Quantization Table [JMQT]. The cover image is divided into blocks of 8X8 pixels and transformation is applied to generate DCT coefficient matrix each block is quantized using modified quantization table. The encrypted two bits of secret information is embedded into selected quantized block. Entrophy is applied on each block and stego image is generated. Mazhar Tayel et al., [15] proposed a chaos steganography algorithm for hiding the confidential multimedia information. Discrete chaotic dynamic system are used to distribute the confidential image pixels randomly within the lower byte of the cover image pixels then embedded into the LSBs of original image to generate stego image. Wien Hong and Tung shou chen [16] proposed an embedding algorithm based on adaptive pixel pair match-
ing. The values of pixel pair is used as reference coordinate and search a coordinate in the neighborhood set of this pixel pair according to confidential message digit. The pixel pair is then replaced by the searched coordinate to hide the digit.

Rong – jian chen and shi – jinn Horng [17] proposed an antiforensic steganography system using multibit adaptive embedding algorithm with flexible bit locations to achieve large embedding capacity and high image quality. The multibits secret information like logo is embedded into any adjoining k bit of cover image. Septimiu Fabian Mare et al., [18] proposed a steganographic method based on High Dynamic Range (HDR) images. The secret data can be reliably embedded using smart LSB pixel mapping and select the best set of low dynamic range images that will be chosen to be joined later in the resulting HDR. This method combines the quality obtained using smart LSB pixel mapping and data rearrangement technique.

Narasimmalou and joseph [19] proposed image data hiding technique based on discrete wavelet transform. Two different hiding techniques are implemented namely (i) three level wavelet decomposition taking a single plane of the cover image for embedding and processing the image as 4x4 blocks with swapping. (ii) Single level wavelet decomposition. Prabhadak and Bhavani [20] proposed a modified secure and high capacity based steganography method of hiding a large size secret image into a small size cover image. Arnold transformation is performed to scramble the secret image. DWT is applied followed by alpha blending operation. Banoci et al., [21] presented a steganographic method for embedding of secret data in still gray scale JPEG image. The embedding is performed in DCT domain in JPEG file. The method uses modulo operator to achieve characteristics of blind steganography system. The secret message is encrypted by advanced encryption standard Ciphering. Nadeem Akhtar et al., [22] implemented a LSB based image steganography. The bit inversion is applied on stegoimage which is obtained by LSB technique. The steganography quality is improved using bit inversion technique, particular pattern of some bits of the cover image pixels are inverted to reduce the number of cover image pixel modification. The bit patterns for which LSB’s has been inverted is stored within the stego image. Nadeem Akhtar et al., [23] presented a data hiding based on a module – based substitution method. Modulus and shifting operations with compression logic is used for hiding secret data. Secret data may be text, image or audio file.

IndradiP Banerjee et al., [24] proposed a frequency domain image steganography in 4 bit pixel factor mapping method using DCT coefficients. DCT coefficient value for embedding the secret data is selected using pixel selection algorithm. Gabriel Bugar et al., [25] designed a steganography method that uses the properties of Harr transformer coefficients. The secret message is compressed before embedding into cover image to improve capacity. The blind steganography methods do not require an original image in the process of extraction.

Bin Li et al., [26] proposed the process of cost assignment in spatial image steganography. The two phases are (i) determining a priority profile and (ii) specifying a cost value distribution. The cost value distribution determines the change rate of cover elements, when the cost values are specified to follow a uniform distribution, the change rate has a linear relation with the payload, which is a rate property for content – adaptive steganography. Kodovsky and Fridrich [27] presented a paper on how the detectability of embedding changes is affected when the cover image is down sampled prior to embedding. The down scaled images are used for steganography, since down sampling changes the strength and character of dependencies among adjacent image pixels. It also affects steganalysis. The lower image resolution decreases the strength of pixel dependencies due to more rapid changes in the image content. Depending on the image down sampling algorithm the strength of pixel dependencies may increase due to interpolation (averaging). Kuo Chen Wu and Chung –Ming Wang [28] proposed a steganography method using a reversible texture synthesis. The source texture image embeds secret messages into cover image through the process of texture synthesis. A texture synthesis process resamples a smaller texture image, which synthesizes a new texture image with a similar loca; appearance and an arbitrary size.

3 PROPOSED MODEL

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

3.1 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.

\[
MSE = \frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2
\]  

Where:

- \(X_{ij}\): The value of the pixel in the cover image.
- \(\bar{X}_{ij}\): The value of the pixel in the stego image.
- \(N\): Size of Image.

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

\[
PSNR = 10\log_{10} \left(\frac{255^2}{MSE}\right) \text{ dB}
\]  

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).

\[
Capacity = \frac{P_{ij}}{C_{ij}} \text{ (3)}
\]  

Where, \(P_{ij}\) is the payload image dimensions, \(C_{ij}\) is the cover image dimensions.
Fig.1. Embedding flow chart of proposed algorithm

1. **Cover Image**
2. **LWT 2 - dB4**
3. **PA**
4. **Decompose into N x N Blocks**
5. **Decompose absolute values into N x N Blocks**
6. **Divide each element of PA block of payload by corresponding element of CD block**
7. **Each resultant element value < NETV.**
   - **Yes**
   - **No**
8. **Increment value of element of CD band**
9. **Scale down avg value by key & embed the value in each block of CH band**
10. **Increment pointer of CD and PA elements in each block**
11. **End of elements of PA and CD block**
    - **Yes**
    - **No**
12. **Average (avg) value of resultant N*N block is calculated**
13. **Divide elements of each PA block by the corresponding average value**
14. **Last block of CD and PA**
    - **Yes**
    - **No**
15. **Modified CD**
16. **Stego object**
17. **Inverse LWT2-dB4**
18. **Stego Image 1**
19. **Calculate PSNR**
20. **Is PSNR > PSNRmax, (Initially PSNRmax=0)**
    - **Yes**
    - **No**
21. **PSNRmax=PSNR**
22. **Is NETV value < 1.999 * key**
    - **Yes**
    - **No**
23. **Repeat the process by incrementing NETV value**
24. **Stego image (a,a)**
3.2 Proposed Embedding Model

In the proposed method, the new concept of average value of matrix obtained by division of payload matrix by cover image matrix in transform domain is used to generate stego object. The flow chart of the proposed embedding model is as shown in Figure 1. Cover image: The cover image is of any 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.

Payload: The secret image to be transmitted is embedded into cover image to generate a stego image. The payload image is resized to dimension equal to cover image. The payload may be of any format.

Lifted Wavelet Transform 2 (LWT2) [29]: 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. 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. While in case of lifting scheme perfect reconstruction is possible for loss-less compression. It is easier to store and process integer numbers compared to floating point numbers.

Fig. 2. Lifting scheme implementation

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

\[ X_o \rightarrow d_i \leftarrow X_{2i+1} \]
\[ X_e \rightarrow s_i \leftarrow X_{2i} \]

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 neighboring even indexed samples and the prediction error is recorded replacing the original sample value, thus providing in-place calculations.

\[ d_i \leftarrow d_i - P(s_d) \]
Where, \( A = (i - \lfloor N/2 \rfloor + 1, \ldots \ldots \ldots, i + \lfloor N/2 \rfloor) \)

\( N = \) 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, \( B = (i - \lceil N/L \rceil, \ldots \ldots, i + \lceil N/L \rceil - 1) \)

The S operator preserves the first \( N \) 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.

\[ d_i \leftarrow d_i - 1/k \]

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.

Embedding: The payload in transform domain is replaced in transform domain cover image to generate stego image using new concept called Non Embedding Steganographic Technique in Transform domain. NETV is used to generate stego image with better PSNR given in Equation 4.

\[ \text{NETV} = 0.1 \text{ to } 1.999 \times \text{key} \quad (4) \]
Key = 5 to 100.

The approximation band PA of payload is considered and divided into smaller blocks of N x N size. The CD and CH sub bands of cover image are considered and divided into smaller blocks of N x N size. The N x N blocks of PA is divided ele-
ment by element by corresponding N x N blocks of CD band. The resultant values of each element is compared with initial values of NETV, if value is greater than NETV, then increment element value of CD and continue till quotient is less than NETV. The average value of resultant N x N block is computed and this process is repeated for complete payload and cover images. The N x N blocks of PA are divided by corresponding average values to convert into modified CD band of cover image. The average values of each N x N blocks are scaled down to one bit by key value and embedded into corresponding N x N blocks of CH band. The intermediate stego object is obtained by combining CA, CV, CH and modified CD bands. The inverse LWT is applied on stego object to generate stego image1.

3.3 Proposed Extraction Model

In this section the proposed extraction model has been discussed and is shown in Figure 3. The d4 wavelet transform is applied on stego image to derive four sub bands viz., CA, CV, CD and CH. The key is extracted from CV sub band. The CH and CD bands are decomposed into N x N blocks. The scale downed average value embedded in each N x N blocks of CH at sending end is extracted and multiplied by key to generate average value for each N x N block. The elements of each N x N block of CD band are multiplied by average value of corresponding N x N block of CH to generate new CD band which results in payload extraction.

4 ALGORITHM

**Problem definition:** the secret image is embedded into cover image in transform domain using non LSB technique. In the proposed approach, we use new concept to generate stego image by dividing PA band of payload by CD band of cover image with key and average values.

**TABLE I. EMBEDDING ALGORITHM OF PROPOSED MODEL**

<table>
<thead>
<tr>
<th>Step</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Transform cover image by lifting scheme using Daubechies ‘d4’ wavelet.</td>
</tr>
<tr>
<td>2.</td>
<td>Decompose CD band into N x N blocks.</td>
</tr>
<tr>
<td>3.</td>
<td>Transform payload image by lifting scheme using Daubechies ‘d4’ wavelet.</td>
</tr>
<tr>
<td>4.</td>
<td>Decompose PA band of payload into N x N blocks.</td>
</tr>
<tr>
<td>5.</td>
<td>The scale down factor value between 5 and 100 acts as key.</td>
</tr>
<tr>
<td>6.</td>
<td>Embed ‘key’ in first 4 elements of CV band of cover image.</td>
</tr>
<tr>
<td>7.</td>
<td>NETV = 0.1 to 1.999 * key for 1 bit replacement in each CH block of cover image.</td>
</tr>
<tr>
<td>8.</td>
<td>Divide elements of each PA block by corresponding elements of each CD block.</td>
</tr>
<tr>
<td>9.</td>
<td>If element value is more than NETV then increment CD element value by 0.1 and repeat 8 else go to step 10</td>
</tr>
<tr>
<td>10.</td>
<td>Compute average value of each N x N block.</td>
</tr>
<tr>
<td>11.</td>
<td>Divide elements of each PA block of payload by its corresponding average value to derive modified CD band for stego object.</td>
</tr>
<tr>
<td>12.</td>
<td>The computed average value is scaled down by key and embedded into corresponding blocks of CH.</td>
</tr>
<tr>
<td>13.</td>
<td>Repeat steps 8 to 12 for all blocks to obtain final stego object.</td>
</tr>
<tr>
<td>14.</td>
<td>Apply Inverse lifting wavelet transform to get stego image 1.</td>
</tr>
<tr>
<td>15.</td>
<td>The PSNR is calculated between cover image and stego image 1 with variable NETV values to find better PSNR value, which is considered as the final stego image.</td>
</tr>
</tbody>
</table>

The PSNR is computed between stego image 1 and cover image for different values of NETV till highest value of PSNR is obtained. The stego image with highest PSNR value is considered as final stego image.

![Fig. 3. Extraction flow chart of proposed algorithm](image-url)
Assumptions:
(i) The cover and payload objects are grayscale images with different dimensions.
(ii) The stego image is transmitted over an ideal channel.

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

<table>
<thead>
<tr>
<th>Input: Stegoimage</th>
<th>Output: Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Transform stego image by lifting scheme using Daubechies ‘dB4’ Wavelet.</td>
<td></td>
</tr>
<tr>
<td>2. Decompose CD and CH bands into N x N blocks.</td>
<td></td>
</tr>
<tr>
<td>3. Extract ‘key’ from CV band.</td>
<td></td>
</tr>
<tr>
<td>4. Extract scaled average values from each N x N blocks of CH band.</td>
<td></td>
</tr>
<tr>
<td>5. Multiply scaled average value by key to obtain a new Average value</td>
<td></td>
</tr>
<tr>
<td>6. Multiply each elements of CD of each block with new Average value to generate payload block.</td>
<td></td>
</tr>
</tbody>
</table>

### 5 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, and Barbara are shown in Figure 4.

#### TABLE III. THE PSNR FOR DIFFERENT SEGMENTED BLOCK

<table>
<thead>
<tr>
<th>Cover Image</th>
<th>Payload</th>
<th>Size (cover image and payload)</th>
<th>% Capacity</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2x2</td>
</tr>
<tr>
<td>Blue Hills.JPG</td>
<td>Barbara PNG</td>
<td>128X128</td>
<td>100</td>
<td>50.41</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256X256</td>
<td>100</td>
<td>52.21</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512X512</td>
<td>100</td>
<td>56.16</td>
</tr>
<tr>
<td>Lena JPG</td>
<td>Lena JPG</td>
<td>128X128</td>
<td>100</td>
<td>35.41</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256X256</td>
<td>100</td>
<td>40.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512X512</td>
<td>100</td>
<td>45.20</td>
</tr>
<tr>
<td>Peppers.PNG</td>
<td>Lena.PNG</td>
<td>128X128</td>
<td>100</td>
<td>39.77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256X256</td>
<td>100</td>
<td>43.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512X512</td>
<td>100</td>
<td>55.559</td>
</tr>
<tr>
<td>Peppers.GIF</td>
<td>Boat.GIF</td>
<td>128X128</td>
<td>100</td>
<td>37.37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256X256</td>
<td>100</td>
<td>41.74</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512X512</td>
<td>100</td>
<td>45.05</td>
</tr>
</tbody>
</table>

Figure 4. The sample of cover and payload images.
The PSNR values for different segmented block sizes with different sizes and formats of cover and payload images are given in Table III. The PSNR values for segmented block sizes such as 2x2, 3x3 and 4x4 of CD of cover and PA of payload images are almost same for different sizes and formats of cover and payload images. It is observed that PSNR value varies between 34 dB to 56.56 dB based on format and size of cover and payload images. The capacity is 100% with acceptable PSNR for different size and formats of cover and payload images.

The advantage of proposed algorithm are (i) payload capacity 100%. (ii) Non embedding technique and average value of segmented matrix is used in the proposed technique, hence it is difficult to retrieve payload by eavesdropper and hence more secure to the payload. (iii) The average PSNR value is around 45 dB.

The PSNR values between cover and stego image and Hiding Capacity (HC) for proposed and existing algorithms are compared in Table IV.

**Table IV. The Comparison Of Capacity And Value Of Proposed Algorithm With The Existing Algorithms.**

<table>
<thead>
<tr>
<th>Technique</th>
<th>PSNR (dB)</th>
<th>HC (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amitava Nag et al.,[30]</td>
<td>34.17</td>
<td>25</td>
</tr>
<tr>
<td>Tataru et al.,[31]</td>
<td>42.17</td>
<td>25</td>
</tr>
<tr>
<td>Shivakumar et al.,[32]</td>
<td>39.48</td>
<td>47</td>
</tr>
<tr>
<td>Senthoooran and Ranathunga[33]</td>
<td>45.05</td>
<td>10.15</td>
</tr>
<tr>
<td><strong>Proposed (ISATT)</strong></td>
<td><strong>56.56</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

It is observed that the PSNR and percentage hiding capacity are more in the proposed algorithm compared to existing algorithms proposed by Amitava Nag et al.,[30] Tataru et al.,[31] Shivakumar et al.,[32] and Senthoooran and Ranathunga[33]. The PSNR values in the proposed algorithm has high value since averaging of matrix is used to generate stego image along with NETV instead of LSB replacements. The capacity in the algorithm is 100% since the segmented matrix blocks of both cover and payload images are used to compute average value for each segmented block to generate stego image.

**6. Conclusion and Future Work**

The secret information is transmitted through communication channels in a secured manner using steganography. In this paper non embedding steganography using average technique in transform domain is proposed. The LWT is applied on cover image and payload to generate wavelet domain sub bands. The CD and PA are segmented into smaller blocks of N x N size. The N x N of PA are divided by N x N block of CD to generate resultant N x N block based on NETV. The average values of resultant N x N matrix is computed and scale downed by key and embed into corresponding N x N blocks of CH band of cover image. The key is embedded into CV band of cover image. The N x N blocks of PA are divided by corresponding average values to generate stego CD. The inverse LWT is applied to derive stego image in spatial domain. The quality of stego image is improved by changing the values of NETV. It is observed that the capacity of proposed algorithm is hundred percent with better PSNR values compared to existing algorithms. In future the proposed technique can be verified with spatial domain.

**REFERENCES**


[14] Sunny Sachdeva and Amit Kumar, “Colour Image Steganography Based on Modified Quantization Table,” Second International Conference on Ad-


