Steganography using Coefficient Replacement and Adaptive Scaling based on DTCWT

N Sathisha *nsathisha@gmail.com*
Department of ECE,
Govt. S K S J Technological Institute,
Bangalore, India.

K Suresh Babu *ksb1559@gmail.com*
Department of ECE,
University Visvesvaraya College of Engineering,
Bangalore, India.

K B Raja *raja_kb@yahoo.com*
Department of ECE,
University Visvesvaraya College of Engineering,
Bangalore, India.

K R Venugopal *venugopalkr@gmail.com*
Principal,
University Visvesvaraya College of Engineering,
Bangalore, India.

Abstract

Steganography is an authenticated technique for maintaining secrecy of embedded data. Steganography provides hardness of detecting the hidden data and has a potential capacity to hide the existence of confidential data. In this paper, we propose a novel steganography using coefficient replacement and adaptive scaling based on Dual Tree Complex Wavelet Transform (DTCWT) technique. The DTCWT and LWT 2 is applied on cover image and payload respectively to convert spatial domain into transform domain. The HH sub band coefficients of cover image are replaced by the LL sub band coefficients of payload to generate intermediate stego object and the adaptive scaling factor is used to scale down intermediate stego object coefficient values to generate final stego object. The adaptive scaling factor is determined based on entropy of cover image. The security and the capacity of the proposed method are high compared to the existing algorithms.

Keywords: Steganography, DTCWT, LWT, Stego Image, Cover Image, Adaptive Scaling, Entropy.

1. INTRODUCTION

Enormous growth of high speed computer networks and internet communication leads to increase in demand of data security systems. The various data hiding techniques for providing security to the confidential information are cryptography, watermarking and steganography. Cryptography scrambles the data to prevent the attacker from understanding the contents. Watermarking is to hide signal into host signal for marking the host signal to be one's legal property. Steganography is the technique of embedding confidential information in a carrier medium the carrier medium can be images, audio, video and text files. Digital images are the most commonly used carrier media used for steganography. The Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) format and Portable Network Graphics (PNG)

formats are the most popular image file formats being used for images shared on internet. Steganographic techniques which are used to modify image files for hiding information includes spatial domain technique, transform domain technique, spread spectrum technique, adaptive technique, statistical methods and distortion techniques. In spatial domain technique, the secret messages are embedded directly. The most common and simplest steganography method is the Least Significant Bit (LSB) insertion method. In the LSB technique the LSB bits of the cover image pixels are replaced by the secret information message bits which are permuted before embedding. A basic classification of spatial domain steganographic algorithms are (i) non filtering algorithm (ii) randomised algorithms and (iii) filtering algorithms. In transform domain technique the cover image is converted into transform domain by applying transformation such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT) etc., and then embedding of confidential information into these transformed coefficients of the cover image. The wavelet transform separates the high frequency and low frequency information on a pixel by pixel basis. DWT is preferred over DCT because image in low frequency at various levels can offer high resolution. The DWT is decomposed into Approximation band (LL), vertical band (LH), horizontal band (HL) and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients which contains the insignificant part and edge details of the spatial domain image. DWT will allow independent processing without significant perceptible interaction between them and hence making the process imperceptibility with more effective. Applications of steganography are in digital copy right protection, digital media content surveillance, content authentication and covert communication involving industries like e-pressing, e-government, e-business etc.,

Contributions: In this paper steganography using coefficient replacement and adaptive scaling based on DTCWT technique is proposed. The DTCWT and LWT are applied on cover and payload images respectively. The HH coefficients of DTCWT are replaced completely by LL coefficients of LWT to generate intermediate stego object. The coefficient of intermediate stego object is scaled down by scaling factors based on the entropy of cover image to generate final stego object. The stego image is obtained by using IDTCWT on final stego object.

2. RELATED WORK

Rigdas and Themrichon Tuithung [1] proposed a Huffman encoding steganography. The Huffman encoding is applied on secret image and each bit of Huffman code of secret image is embedded into the cover image altering the LSB of each cover image pixel. Najeena and Imran [2] presented a steganographic and cryptographic technique based on chaotic encryption with adaptive pixel pair matching. The scrambled data is embedded into the cover media based on pixel pair matching technique. The cover pixel pairs are changed randomly by using keys to increase the security level of the system. Ran-zan wang and Yeh-shun chen [3] presented a steganography technique based on two way block matching procedure. The block matching procedure search for the highest similarity block from a series of blocks generated from the cover image and embeds the secret information in imperceptible areas of the cover image. The hop embedded scheme is used which resulted in high quality of stego image and extracted secret image. This method exhibits high payload embedding. Vojtech holub and Jessica fridrich [4] developed an adaptive steganographic distortion function a bank of directional high pass filters is employed to obtain the directional residuals. The impact of embedding on the every directional residual is measured. The embedding is done on smooth areas along edges and noisy areas. Baolong Guo et al., [5] proposed robust image watermarking schemes based on the mean quantization using DTCWT. The energy map of the original image is first composed from the six high frequency sub bands of DTCWT and the watermark is embedded into the high energy pixels. The two schemes embed the watermark into the high frequency and low frequency DTCWT coefficients by quantizing.

Ajit danti and Manjula [6] proposed an image steganography using DWT and hybrid wavelet transform. The cover and secret images are normalized and the wavelet coefficients are obtained

by applying DWT. The wavelet coefficients of both the cover and secret images are fused into single image. Jani Anbarasi and kannan [7] have developed a secure steganographic system for secret color image sharing with reversible characteristics. The secret color image pixels are transformed into M-ary notational system. Reversible polynomial function is generated using (t-1) digits of secret color image pixels and the secret shares are generated using reversible polynomial function and the participant's numerical key. The secret image and cover image are embedded together to construct stego image. Reversible image sharing process is used for reconstructing secret image and cover image. Secret is obtained by Lagrange's formula generated from sufficient secret shares. Quantization process is applied to improve quality of cover image. Sathya et al., [8] discussed the various techniques for data hiding in audio signal, video signal, text and JPEG images. The pros and cons of the available techniques are analysed and proposes a technique based on T-codes. T-codes are used for encoding of original message and entropy encoding of compressed stego image. After this SB technique is used for embedding process. T-codes are considered because of its self synchronizing property which increases robustness of the technique. Zawawi et al., [9] discusses the operation of active warden and how it is the main hindrance for steganography information retrieval. Active wardens are attackers of steganography which aims to destroy the possible hidden information within the carrier. If the objective of the attacker is is to disrupt the communication of hidden information then active approach will be the preferred method compared to time consuming passive steganalysis methods. Yang et al., [10] proposed an improved method of image sharing with steganography for providing authentication to prevent cheating. Manipulation of the stego images are prevented by using Hash function with secret keys. The authentication is provided by hashing 4 pixel blocks, block ID and image ID. The quality of both stego image and secret image are improved by a new arrangement of seventeen bits in the four pixel square block. Chiang- Lung Liu and Shiang-Rong Liao [11] have developed a high performance steganographic scheme for JPEG using complementary embedding strategy to avoid detections of several statistical attacks in spatial domain. Here instead of flipping the LSBs of the DCT coefficients, the secret bits are embedded in the cover image by subtracting one or adding one to the non zero DCT coefficient and hence cannot be detected by both Chi square and Extended Chi square attacks. Manjunatha Reddy and Raja [12] have proposed high capacity and security steganography using DWT technique. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength alpha and beta. The cover and payload are preprocessed to reduce pixel range ensuring accurate recovery of payload at destination.

ShivaKumar et al., [13] have developed hybrid domain in LSB steganography technique which is an integration of both spatial and transform domain techniques. The cover image and payload is divided into two cells and cell I is transformed to frequency domain using DCT/DWT/FFT while maintaining components of cell II in spatial domain itself. Next, the MSB pixels of payload cell I and cell II are embedded into corresponding cell I and cell II of cover image. Youngran Park et al., [14] proposed a method for integrity verification of secret information in image steganography. The secret information is hidden into spatial domain of digital image and the embedded secret information is randomly permuted to achieve confidentiality. Integrity of secret information is verified using DCT coefficients. Xinpeng Zhang and ShouZhang Wang [15] have suggested an improvement for PVD steganography technique to reduce its vulnerability for histogram analysis there by providing enhanced security. The method preserves the advantage of low visual distortion of the PVD. This introduces a pseudo-random dithering to the division of ranges of PVDs. The Histogram based steganalysis is defeated while preserving embedding capacity and high invisibility of original PVD. Chin-Chan Chang and Hsian-Wen Tseng [16] have proposed a steganographic method which provides larger embedding capacity and minimizes the distortion of stego image. The method exploits the correlation between neighboring pixels to estimate the degree of smoothness or contrast of pixels and the pixel in the edge area has more data than those in the non edge areas. Two sided, three sided and four sided match methods are used for embedding. Manjunatha Reddy and Raja [17] proposed a wavelet based non LSB steganography technique in which the cover image is segmented into 4*4 cells and DWT/IWT is applied to each cell. The 2*2 cell of HH band of DWT/IWT are considered and manipulated with payload bit pairs using identity matrix to generate stego image and the key is used to extract payload bit pairs at

the destination. The algorithm cannot be detected by steganalysis techniques such as Chi-square and pair of values techniques.

Shiva Kumar et al., [18] proposed a bit length replacement steganography based on DCT coefficients where the cover image is segmented into smaller matrix of size 8*8 blocks and converted into DCT domain by applying 2D-DCT to each block. The MSB bits of payload are embedded into each DCT coefficients of cover image based on the coherent length 'L' which is determined by the DCT coefficient values. K.B. Shiva Kumar et al., [19] proposed a steganographic technique based on payload transformation which is a non LSB and non transform domain technique. The cover image is segmented into 2*2 matrices then the matrix for payload embedding process is obtained based on the threshold value fixed by adjacent pixel intensity differences. The transformation matrix is obtained by considering the identity matrix and the payload bit pair. The stego image matrices of size 2*2 are derived from the 2*2 cover image matrices and the transformation matrix. Key is generated with first bit payload matrix at sending end and this is used to extract the payload from stego image.

Manjunatha Reddy and Raja [20] developed wavelet based secure steganography with scrambled payload. It is a hybrid domain technique. Daubechies Lifting Wavelet Transform (LWT) is applied on the cover image whose XD band is decomposed into upper and lower bands for payload embedding. The payload is segmented into four blocks and Haar 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. Then, bit reversal is applied on each coefficient of payload blocks to scramble payload and cube root is applied on these scrambled values to scale down the number of coefficient bits. The payload is embedded into XD band of cover image to obtain stego image. Arnab Kumar Maji et al., [21] proposed a steganographic scheme using Sudoku puzzle. An 18 x 18 Sudoku reference matrix is used for message embedding and 8 x 8 Sudoku is embedded into the cover image to detect whether cover image is modified or not. The secret information is embedded inside the cover image using 18 x 18 Sudoku reference matrix. In the proposed work an 18 x 18 Sudoku reference matrix is used instead of 256 x 256 or 27 x 27 reference matrix. Rashedul islam et al., [22] proposed a steganography technique to hide large data in bit map image using filtering based algorithm. The secret message is converted into cipher text using AES cryptography and the cipher text is embedded into the cover image. The method uses the concept of status checking for insertion and retrieval of message. Chi Yuan Lin et al., [23] presented a steganographic system for Vector Quantization (VQ) code books using section based informed embedding. The Fuzzy Competitive Learning Network (FCLN) clustering technology generate optimal code book for VQ. The VQ code book of secret image information is embedded into the cover image by a section based informed embedding scheme.

3. PROPOSED MODEL

In this section definitions of evaluation parameters and block diagram of proposed model are discussed.

3.1 Definitions

I *Mean Square Error (MSE):* It is defined as the square of error between two images 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 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.

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

$$PSNR = 20\log_{10}(255/\ MSE)\ dB \qquad (2)$$

III *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. The percentage of Hiding Capacity is given in Equation 3.

$$\text{Hiding Capacity} = (P_{ij} / C_{ij}) * 100 \qquad (3)$$

Where, Pij is the payload image dimensions,

Cij is the cover image dimensions.

3.2 Proposed Embedding Model

In the proposed method, the concept of Dual Tree Complex Wavelet Transform is used to transform the cover image into low and high frequency sub bands. The payload is transformed into frequency domain using lifting wavelet transformation. The approximation band coefficients of payload are embedded into coefficients of high frequency sub bands of cover image to generate stego image based on the entropy of cover image and scaling factor. The block diagram of the proposed embedding model is as shown in Figure 1.

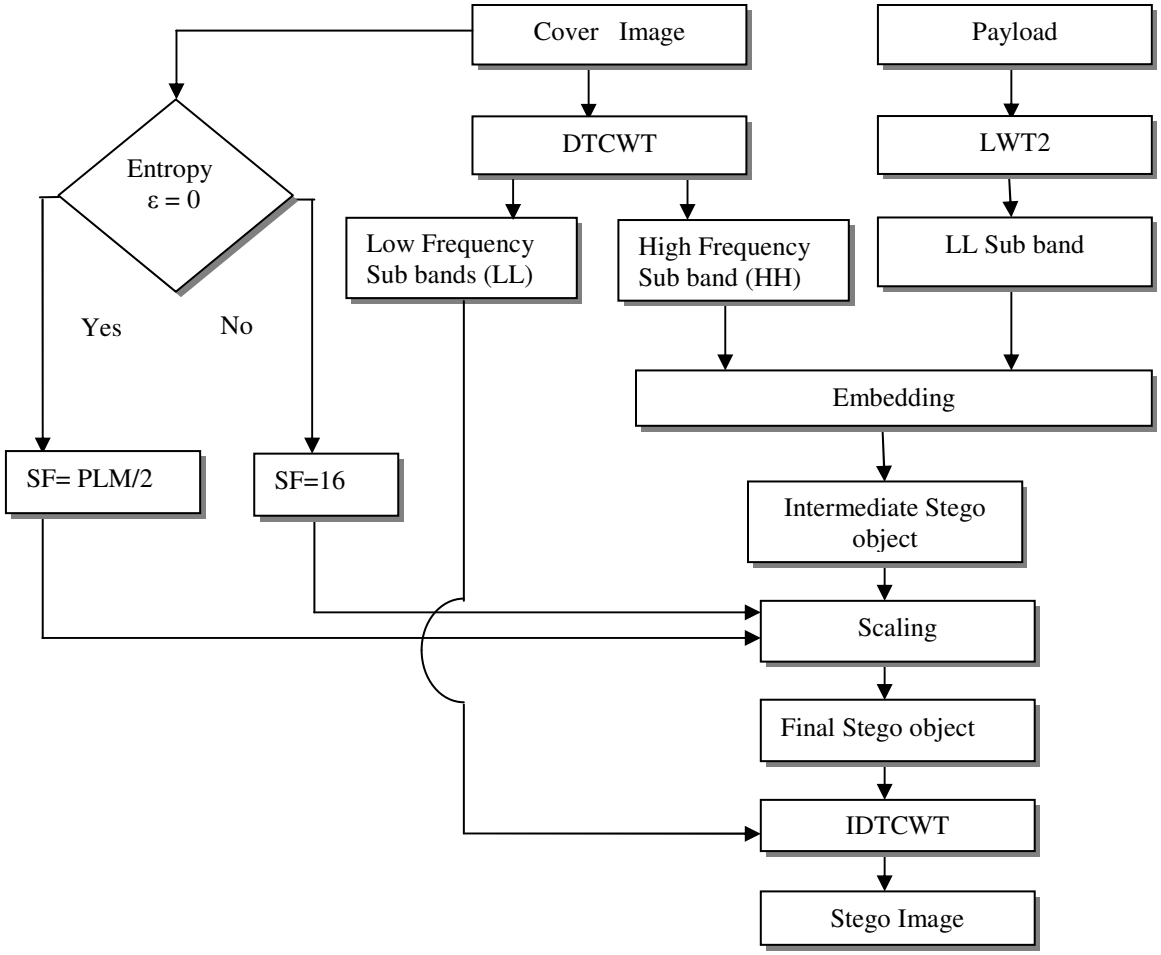


FIGURE 1: Embedding Model of Proposed Algorithm.

3.2.1 Cover image (CI): The cover image of any size and format is considered to test the performance analysis. The cover image is resized to a square matrix dimensions to embed payload for better performance.

3.2.2 Payload: The secret image to be transmitted is embedded into cover image to generate a stego image. The payload may be of any format and of size less than or equal to cover image.

3.2.3 Lifted Wavelet Transform 2 [24]: 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.

Constructing wavelets using lifting scheme consists of (i) Split phase (ii) Predict phase (iii) update phase as shown in Figure 2

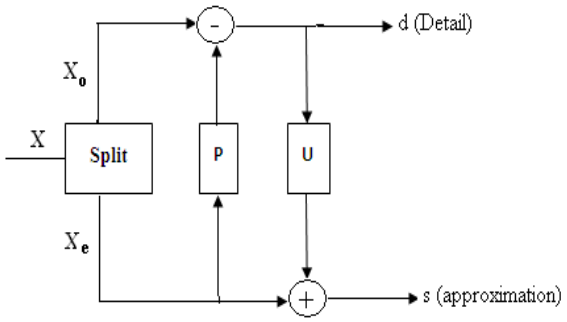


FIGURE 2: Lifting Scheme Implementation.

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

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

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

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.

$$d_i \leftarrow d_i - P(S_A)$$

Where, $A = (i - [N/2] + 1, \ldots\ldots\ldots\ldots\ldots\ldots i + [N/2])$

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

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

The U operator preserves the first $\hat{N}$ 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 LWT 2 is applied on resized Payload to transform from spatial domain to wavelet domain bands such as Approximation band (LL), Horizontal band (LH), Vertical band (HL) and Diagonal band (HH). The LL band has significant information hence coefficients of LL band is embedded into high frequency sub bands of cover image.

3.2.4 Dual Tree Complex Wavelet Transform [25]: A recent enhancement to DWT with additional, directionality properties. It is an effective approach for implementing an analytic wavelet transform. This is nearly shift invariant and directionally selective in two and higher dimensions this is achieved with a redundancy factor of only 2^d for d-dimensional signals, which is comparatively lower than the undecimated DWT. The idea behind dual tree approach is that it employs two real DWT in its structure. The first DWT gives the real part of the transform and second part gives the imaginary part. The two real wavelet transforms use two different sets of filters, with each satisfying the perfect reconstruction conditions. The two sets of filters are jointly designed so that the overall transform is approximately analytic. The analysis Filter banks used in DTCWT are shown in Figure 3.

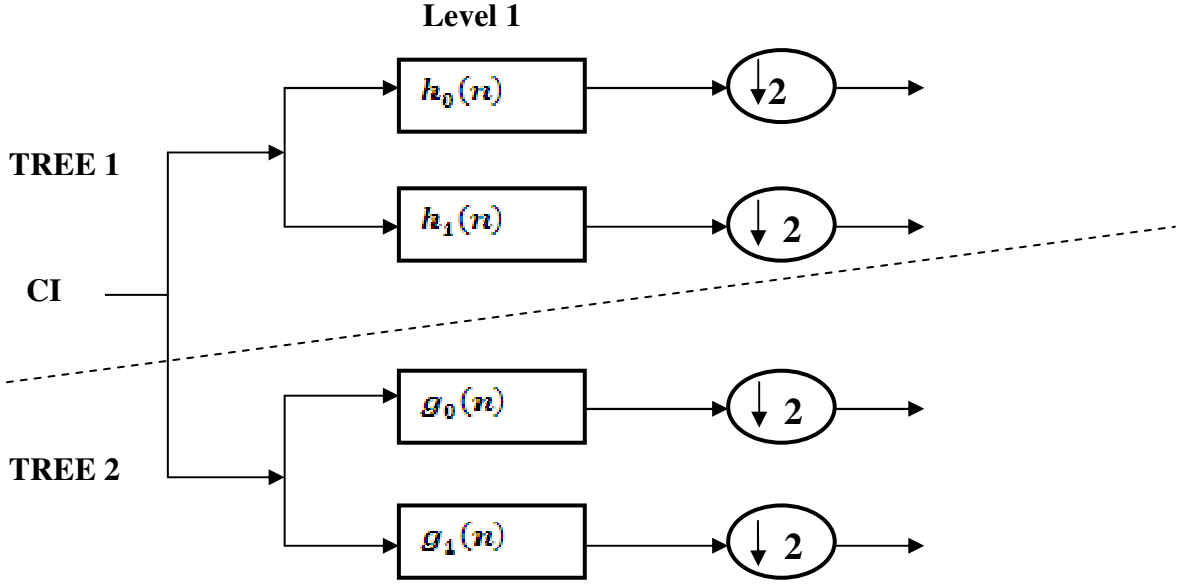


FIGURE 3: Analysis filter bank structure of DTCWT.

Let $h_0(n)$, $h_1(n)$ denote the low-pass and high-pass filter pair for the upper filter bank that is filter bank of tree 1, and let $g_0(n)$, $g_1(n)$ denote the low-pass and high-pass filter pair for the lower Filter Bank that is filter bank of tree 2. The two real wavelets associated with each of the two real wavelet transforms are denoted as $\psi_h(t)$ and $\psi_g(t)$. In addition to satisfying the perfect reconstruction conditions, the filters are designed so that the complex wavelet shown in Equation 4 is approximately analytic.

$$\psi(t) = \psi_h(t) + j\,\psi_g(t) \quad (4)$$

Equivalently, they are designed so that $\psi_g(t)$ is approximately the Hilbert transform of $\psi_h(t)$ as shown in Equation 5.

$$\psi_g(t) \approx \mathcal{H}\{\psi_h(t)\} \quad (5)$$

The implementation of the DTCWT does not require complex arithmetic because filters are themselves real. DTCWT is not a critically sampled transform; it is two times expansive in 1-D because the total output data rate is exactly twice the input data rate. The dual tree CWT is also easy to implement because there is no data flow between the two real DWTs, the transform is naturally parallelized for efficient implementation however, the dual tree CWT requires the design of new filters. Primarily, it requires a pair of filter sets chosen so that the corresponding wavelets form an approximate Hilbert transform pair. Existing filters for wavelet transforms should not be used to implement both the trees of the dual tree CWT. If the dual tree wavelet transform is implemented with filters not satisfying this requirement, then the transform will not provide the full advantages of analytic wavelets.

In the proposed technique a single level of DTCWT is applied to the cover image which gives 12 high frequency sub-bands and 4 low frequency sub bands, only the high frequency sub bands which forms the real part is suitable for embedding as it gives good retrieval quality of the payload without any perceptive degradation to the stego image. In the proposed technique one of high frequency sub band with negligible randomness is selected for embedding. Referring to the Figure 3 the formation of sub-bands in DTCWT can be analyzed as follows (i) The use of filters of Tree 1 alone in both the dimensions that is along rows and columns gives four sub-bands namely LL, LH, HL and HH (ii) The use of filters of Tree 1 along the rows and Tree 2 filters along the columns produces another set of four sub-bands namely LL, HL, LH and HH. (iii) In another combination the filters of Tree 2 are used along the rows and the filters of Tree1 are used along the column to produce yet another set of sub bands namely LL, HL, LH and HH. (iv) finally, the use of Filters of Tree 2 alone in both the dimensions that is along rows and columns produces another set of sub-bands LL, HL, LH and HH.

Thus, a single level of DTCWT when applied to the cover image gives totally 16 frequency sub-bands out of which 4 are LL bands and 12 high frequency sub-bands.

3.2.5 Embedding: The new concept of embedding is used in the proposed model. Here, the chosen high frequency sub band coefficient of the transformed cover image is completely replaced by the LL band coefficient of the payload image. Since coefficients of high frequency sub band of the image are replaced it does not result in the perceptive degradation of the stego image. The use of coefficient replacement method of embedding also gives good retrieval quality of the payload at the receiver end.

3.2.6 Scaling: Scaling operation at the sender end is performed by dividing all the coefficients of the intermediate stego object by a scaling factor. Since the LL sub band coefficients of payload completely replaces the high frequency sub band coefficients of the cover image, only two HH sub bands from real part of DTCWT are used for embedding to get better stego image quality and

also to get perceptively good extracted payload at the destination. The coefficients of two HH sub bands are totally replaced by LL sub band coefficients of payload to generate final stego object. scaling has to be performed to restore the regular pattern of the DTCWT coefficients so that all the high frequency coefficients will have smaller values their by giving fewer chances for suspicion. If only the band in which embedding is done is scaled then only that particular band will show a different pattern of coefficients hence all the high frequency sub bands are scaled so that all of them look almost similar thereby avoiding suspicion. The scaling also improves the security of the payload in the stego image.

3.2.7 Entropy: Entropy [26] is a statistical measure of randomness that can be used to characterize the texture of the image. An image X of size M*N can be considered as a system with 'L' pixel intensity scales. For example, a 8-bit gray image allows L = 256 gray scales from 0 to 255. The probability of i^{th} pixel is given by Equation 6.

$$P_i = \Pr(X = l) = \frac{N(l)}{MN} \quad (6)$$

Where, X = image of size M*N

l= intensity levels varies from 0 to 255 for gray scale image
N(*l*)= No. of pixels with intensity values *l*

Then the entropy of an image is given by Equation 7

$$H(X) = -\sum_{l=0}^{255} P_l \log_2 P_l = \sum_{l=0}^{255} \frac{N(l)}{MN} \log_2 \frac{MN}{N(l)} \quad (7)$$

The image entropy is a quantitative measurement of $\{P_l\}$ where l *v*aries from 0 to 255. It is equivalent to the histogram analysis, which plots the distribution of P_l and is commonly used for security analysis

3.2.8 Scaling Factor: the scaling factor is chosen based on the entropy of cover image.

Case (i): When the Entropy of Cover Image ε =0

When the entropy of cover image is zero the scaling factor is chosen to be half the mean value of payload pixel intensity**.** When this Scaling Factor is used the technique gives good PSNR along with good zero it implies that the randomness of CI is zero hence a high scaling factor can be used as shown in Equation 8

$$SF = \frac{PLN}{2} \quad (8)$$

When Scaling Factor is high the Euclidean distance between the Cover image and stego image is small that is both the images are nearly similar thus giving perceptively good retrieved payload.

Case (ii): When the Entropy of Cover Image ε ≠ 0 in this case when the cover image has randomness a different scaling factor has to be chosen as the stego image will also have randomness. The scaling factor is decided based on the observations by trial and error method where the technique is checked with different formats of image for different scaling factors. It is observed that the scaling factor is independent of the cover image format used hence the same scaling factor can be used for all the formats of cover image. From Table 1 it can be observed that choosing smaller scaling factors in the range 2-10 gives poor stego quality, lesser PSNR but good payload retrieval because the Euclidean Distance (ED) between the intermediate stego object bands before and after transmission is very large. While, Scaling Factor above 15 gives good PSNR, stego quality and retrieval quality but as scaling factor increases the perceptive quality of the retrieved payload becomes poor hence as a trade off to obtain good stego image with good PSNR and good quality of retrieved payload the scaling factor in this case is fixed at

16. Also the histogram pattern of cover image and Stego image are checked for different scaling factors and it is observed that for the scaling factor fixed there is no significant variation in the histogram pattern but smaller scaling factors show significant difference in the pattern

Table 1: Scaling Factor Selection.

Scaling Factor	PSNR(dB)	PSNR1(dB)	ED	Observations
[2-10]	Decreases <30 dB	Increases >40 dB	Higher	Stego Quality- Poor Retrieval Quality- good PSNR- Low Histogram-significant
15	37.3831	32.0704	403.563	Stego Quality – good Retrieval Quality- good PSNR- Good Histogram- insignificant
16	39.3631	36.1902	300.265	
[32 and above]	Increases >40 dB	Decreases <30 dB	Lesser	Stego Quality – good Retrieval Quality- Poor PSNR- Good Histogram-insignificant

Hence the scaling factors used for the proposed techniques are chosen based on the entropy of cover image. Scaling Factor (SF) summarized as shown in Equation 9.

$$SF = \begin{cases} \frac{PLM}{2} = Key1 & \text{if } \varepsilon = 0 \\ 16 = key2 & \text{if } \varepsilon \neq 0 \end{cases} \quad (9)$$

3.2.9 Key: the scaling factor values are used as keys which are embedded in HH sub bands to retrieve payload at the destination**.**

3.2.10 Stego object: The intermediate stego object after performing scaling operation is referred to as stego object. The stego object is the transform domain version of the stego image which will be transmitted through the channel for communication.

3.2.11 Inverse Dual Tree Complex Wavelet Transform (IDTCWT): The inverse of the DTCWT is as simple as the forward transform. To invert the transform, the real part and the imaginary part are each inverted, the inverse of each of the two real DWTs are used, to obtain two real signals. These two real signals are then averaged to obtain the final output. The original signal can also be obtained from either real part or imaginary part alone however, such inverse DTCWTs do not capture all the advantages an analytic wavelet transform offers. IDCTWT is applied on the stego object to generate Stego Image (SI).

3.3 Proposed Extraction Model

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

DTCWT is applied on the stego image to extract the high frequency sub bands where the LL sub band of payload embedded in the embedding module. The entropy of stego image is calculated. The scaling factor is fixed at PLM/2 if entropy of stego image is zero else scaling factor is fixed at 16. The coefficients of HH sub band are scaled by multiplying appropriate scaling factors based on entropy of stego image to obtain payload coefficients in wavelet domain. The ILWT2 is applied on payload coefficients to obtain the payload in spatial domain.

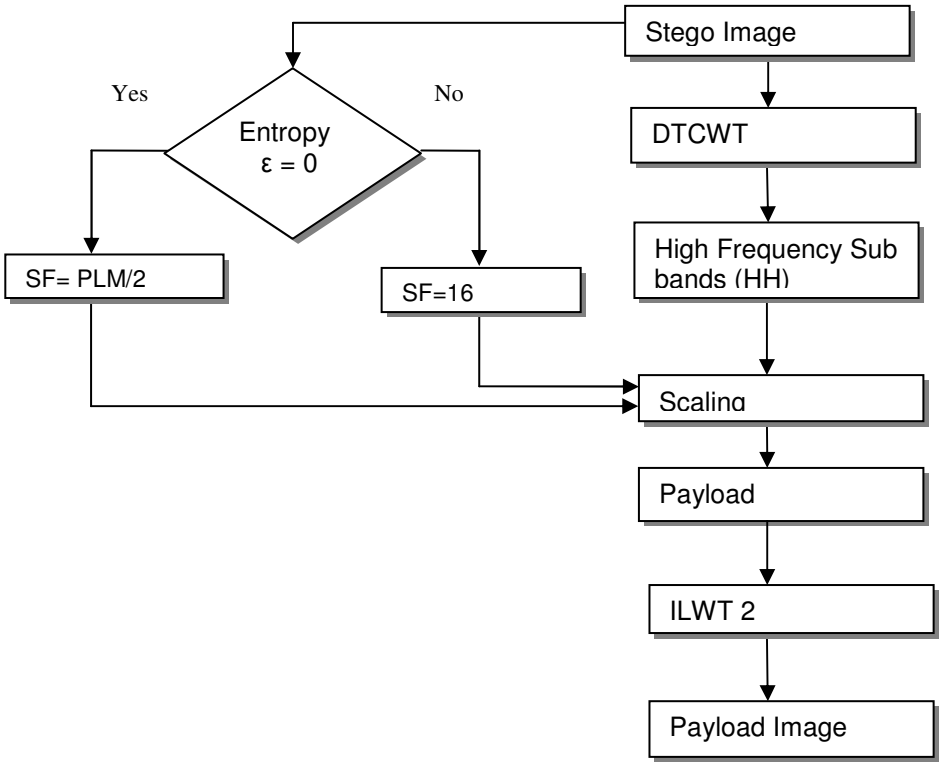


FIGURE 4: Block Diagram of the proposed retrieval model.

4. ALGORITHM

Problem definition: The secret image is embedded into cover image in transform domain using DTCWT technique. In the proposed approach, the new concept to generate stego image is used by replacing the high frequency sub band coefficients of cover image by the approximation band coefficients of the payload.

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 2: Embedding Algorithm of Proposed Model.

Input: Cover image, payload,
Output: Stego image

1. Cover image and Payload image of different formats and sizes are considered
2. Resize CI to $2^m x 2^m$ to apply DTCWT, where m is an integer.
3. Apply one Level DTCWT on the CI
4. Apply one level LWT2 on Payload image
5. The high frequency sub band coefficients of cover image are replaced by LL sub band coefficients of payload in embedding block to generate a stego object.
6. Entropy of cover image is calculated
7. The scaling factor of PLM/2 is fixed if entropy is zero else scaling factor is fixed at 16.
8. The coefficients of intermediate stego object are divided by the appropriate values of scaling factor.
9. The final stego object is generated by scaled intermediate stego object and low frequency sub bands of cover image.
10. Stego image in spatial domain is obtained by applying IDTCWT on the final stego object.

The algorithm of embedding model is discussed in Table 2. The DTCWT and LWT2 are applied on cover image and payload image respectively. The high frequency coefficients of cover image are replaced by LL sub band coefficients of payload. The retrieving algorithm is described in Table 3 to extract payload from stego image by adapting reverse process of embedding.

TABLE 3: Retrieving Algorithm.

Input: Stego image Output: Payload 1. Apply single level DTCWT on the stego image to obtain higher frequency HH sub bands. 2. Entropy of Stego image is computed to fix scaling factor. 3. Scaling factor is PLM/2 if entropy is zero otherwise scaling factor is 16. 4. The high frequency sub band coefficients of DTCWT are multiplied by appropriate scaling factor values to generate payload coefficients. 5. The ILWT2 is applied on payload coefficients to generate payload image in spatial domain.

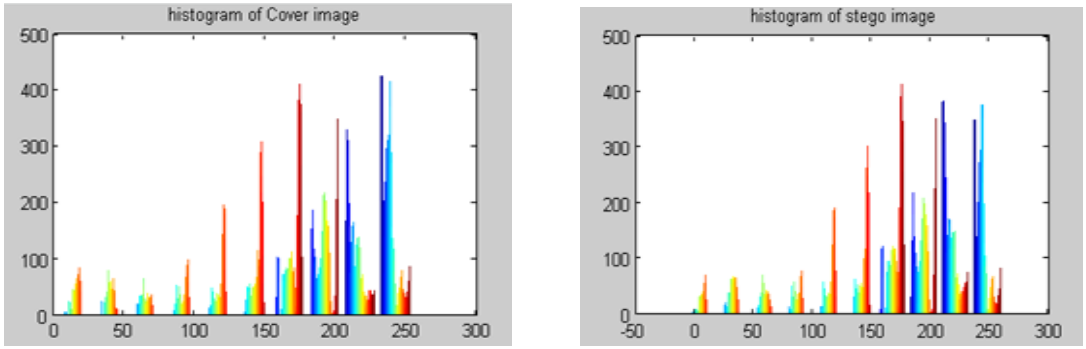
5. PERFORMANCE ANALYSIS

(i) Histogram Comparison: The payload image Lena.Jpg of size 512 x 512 is embedded into the cover image mandril.Jpg of size 512 x 512 to generate stego image is shown in the Figure 5 using proposed steganographic algorithm.

(a) Cover image (b) Payload (c) *Stego Image* (d) *Retrieved payload*

FIGURE 5: (a) CI: Mandril (512*512) (b) PL: Lena (512*512) (c) Stego Image (512*512) (d) Retrieved payload (512*512).

The histograms of cover image and stego image are shown in Figure 6 the patterns of cover image and stego image histograms are almost same which indicates the statistical properties of stego image are not varied compare to original cover image



a) Cover image b) Stego image

FIGURE 6: (a) Histogram of CI (b) Histogram of SI.

(ii) Performance Parameters of Proposed Algorithm for different image formats and hiding capacity

The different cover and payload images used to test performance of the proposed algorithm are shown in Figure 7.

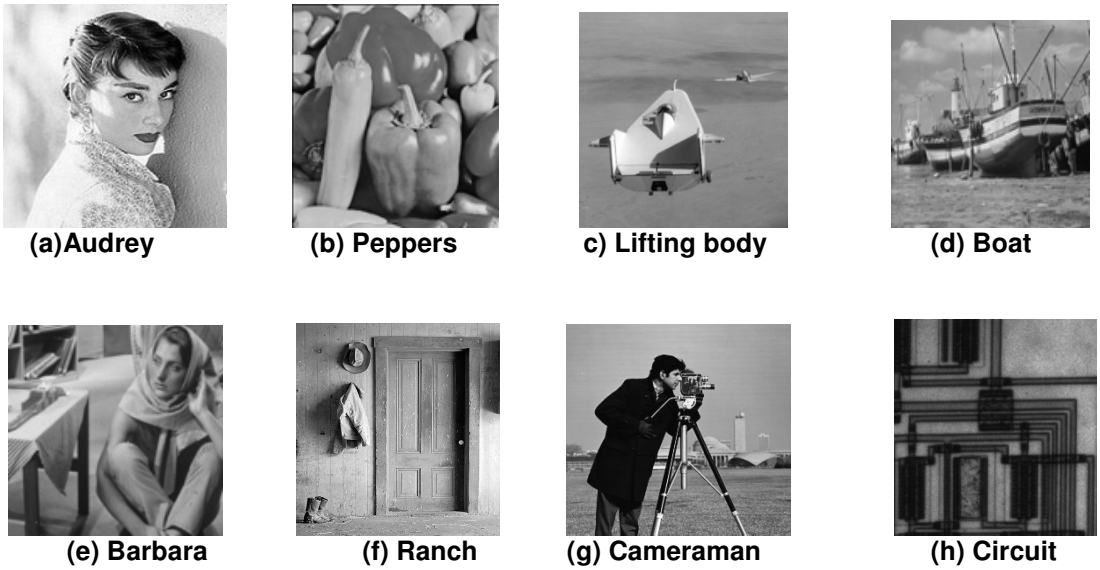


FIGURE 7: Images used as cover and payload with different formats

TABLE 4: Performance Parameters for Different Image Formats With 100% Hiding Capacity.

Cover image (512*512)	Payload (512*512)	(PSNR(CI& SI))	(PSNR(PL&EPL))	Entropy (CI)	Entropy (SI)
Mandril.jpg	lena.tif	42.9421	36.9712	0	0
	audrey.Jpg	42.9096	37.2117	0	0
	ranch.bmp	42.9505	35.3612	0	0
	liftingbody.Png	43.0296	37.4578	0	0
Audrey.jpg	lena.tif	41.5943	42.2837	0.0058	0.0014
	barbara.jpg	41.6521	38.7104	0.0058	0.00051
	ranch.bmp	41.77	37.2746	0.0058	0
	liftingbody.png	41.724	35.2302	0.0058	0.000518
circuit.tif	lena.tif	39.8503	36.9188	0	0
	barbara.jpg	39.8570	30.8117	0	0
	ranch.bmp	39.8472	35.3104	0	0
	liftingbody.png	39.8809	37.3862	0	0
Mandril.tif	lena.tif	32.3845	29.5074	0.000074	0.00072
	barbara.Jpg	32.4569	29.5074	0.000074	0.00317
	ranch.bmp	32.2646	27.3367	0.000074	0.00074
	liftingbody.png	32.1867	27.2270	0.000074	0.0420
Liftingbody.png	lena.tif	36.7624	37.7115	0.0014	0.0036
	barbara.jpg	35.4529	29.7459	0.0014	0.0018
	pirate.bmp	35.8598	31.4215	0.0014	0.000518
	mandril.png	35.08596	27.5279	0.0014	0.0051

The cover and payload images are converted into transform domain and the payload is embedded into the cover to derive the stego image. The payload is retrieved from stego image using reverse embedding process at the destination. The performance parameters such as PSNR between cover image and stego image PSNR (CI& SI), PSNR between payload & Extracted payload (PSNR (PL&EPL)), entropy of cover image (CI) and entropy of stego image (SI) with hundred percent hiding capacity are tabulated in Table 4. The PSNR between cover and stego image is almost constant irrespective of payload image formats. The value of PSNR between the cover and stego image depends on the cover image format and also entropy of cover image. The PSNR between cover and stego image is little high when the entropy is zero compare to entropy of non zero value, since scaling factor is high in the case of entropy zero compared to lower scaling factor for non zero entropy value. The values of PSNR are high in the case of JPG image format of the cover image compare to Tiff, PNG and Bmp formats of cover image.

The performance parameters such as PSNR between cover image and stego image PSNR (CI& SI), PSNR between payload & Extracted payload PSNR (PL&EPL), entropy of cover image (CI) and entropy of stego image (SI) with seventy five percent hiding capacity are tabulated in Table 5

TABLE 5: Performance Parameters for Different Image Formats With 75% Hiding Capacity.

Cover image (512*512)	**Payload (512*384)**	**PSNR (CI& SI)**	**PSNR(PL&EPL)**	**Entropy (CI)**	**Entropy (SI)**
Mandril.jpg	lena.tif	43.2743	37.1437	0	0
	audrey.Jpg	43.1747	42.3191	0	0
	ranch.bmp	43.3095	35.4160	0	0
	liftingbody.Png	43.3713	37.4115	0	0
Audrey.jpg	lena.tif	41.9756	36.9878	0.0058	0.0042
	barbara.jpg	41.8893	42.3596	0.0058	0.0020
	ranch.bmp	41.9995	35.2554	0.0058	0.0094
	liftingbody.png	42.0413	37.1860	0.0058	0.0034
circuit.tif	lena.tif	40.0347	30.7472	0	0
	barbara.jpg	40.0230	36.8722	0	0
	ranch.bmp	40.0276	35.3737	0	0
	liftingbody.png	40.0523	37.3488	0	0
Mandril.tif	lena.tif	32.7592	33.2747	0.000074	0.0365
	barbara.Jpg	33.2413	37.3500	0.000074	0.0848
	ranch.bmp	33.7029	30.8545	0.000074	0.0235
	liftingbody.png	32.5427	30.2076	0.000074	0.0081
Liftingbody .png	lena.tif	36.0756	30.7044	0.0014	0.0034
	barbara.jpg	37.1842	37.6696	0.0014	0.0049
	pirate.bmp	35.7648	30.5444	0.0014	0.00096
	peppers.png	36.4326	31.4281	0.0014	0.00034

The performance parameters such as PSNR between cover image and stego image PSNR (CI& SI), PSNR between payload & Extracted payload PSNR (PL&EPL), entropy of cover image (CI) and entropy of stego image (SI) with fifty percent hiding capacity are tabulated in Table 6 The performance parameters such as PSNR between cover image and stego image PSNR (CI& SI), PSNR between payload & Extracted payload PSNR (PL&EPL), entropy of cover image (CI) and entropy of stego image (SI) with twenty five percent hiding capacity are tabulated in Table 7

TABLE 6: Performance Parameters for Different Image Formats With 50% Hiding Capacity.

Cover image (512*512)	**Payload (512*256)**	**PSNR(CI& SI)**	**(PSNR(PL&EPL))**	**Entropy (CI)**	**Entropy (SI)**
Mandril.jpg	lena.tif	43.6027	42.1814	0	0
	audrey.Jpg	43.6764	37.0397	0	0
	ranch.bmp	43.7017	35.5876	0	0
	liftingbody.Png	43.7466	37.3530	0	0
Audrey.jpg	lena.tif	42.2057	36.9101	0.0058	0.0071
	barbara.jpg	42.2649	42.0915	0.0058	0.00097
	ranch.bmp	42.2865	35.4492	0.0058	0.0030
	liftingbody.png	42.3165	371642	0.0058	0.0062
circuit.tif	lena.tif	40.2101	36.7554	0	0
	barbara.jpg	40.2019	37.0028	0	0
	ranch.bmp	40.2115	35.5477	0	0
	liftingbody.png	40.2292	37.3008	0	0
Mandril.tif	lena.tif	33.4252	35.4106	0.000074	0.0308
	barbara.Jpg	33.0838	37.0545	0.000074	0.0950
	ranch.bmp	32.9752	30.4197	0.000074	0.0149
	liftingbody.png	33.9277	30.4724	0.000074	0.0018
Liftingbody.png	lena.tif	37.6512	30.6509	0.0014	0.0022
	barbara.jpg	36.8103	37.5773	0.0014	0.0044
	pirate.bmp	36.5643	30.6171	0.0014	0.0014
	mandril.png	37.0894	31.4623	0.0014	0.0021
Ranch.bmp	lena.tif	36.1504	30.4790	0.0005	0.0102
	barbara.jpg	38.2569	37.2016	0.0005	0.0067
	pirate.bmp	36.1139	32.8101	0.0005	0.0171
	liftingbody.png	36.0994	31.2288	0.0005	0.0054

The performance parameters PSNR (CI & SI) and varies between PSNR (PL & EPL) are tabulated in Table 8 for different percentage capacities with cover and payload images having JPG formats. The values of PSNR (CI & SI) are almost constant for percentage hiding capacities between 25 and 100. The variations of PSNR (CI & SI) and percentage hiding capacity are plotted in the Figure 8 as the percentage hiding capacity increases from 25 to 100, the values of

PSNR (CI & SI) varies between 44.43 and 43. 91 ie., the PSNR values are almost constant with capacity.

TABLE 7: PSNR Performance Parameters for Different Image Formats With 25% Hiding Capacity.

Cover image (512*512)	Payload (256*256)	(PSNR(CI& SI))	(PSNR(PL&EPL))	Entropy (CI)	Entropy (SI)
Mandril.jpg	lena.tif	44.4238	45.7815	0	0
	audrey.Jpg	44.4274	41.6053	0	0
	ranch.bmp	44.7086	44.427	0	0
	liftingbody.Png	44.7086	53.6653	0	0
Audrey.jpg	lena.tif	42.7972	44.1040	0.0058	0.0061
	barbara.jpg	42.7962	43.501	0.0058	0.00051
	ranch.bmp	42.7992	43.0021	0.0058	0.0080
	liftingbody.png	42.8008	49.4367	0.0058	0.00047
circuit.tif	lena.tif	40.5275	52.7875	0	0
	barbara.jpg	40.5256	45.4012	0	0
	ranch.bmp	40.5260	44.3152	0	0
	liftingbody.png	40.5282	52.592	0	0
Mandril.tif	lena.tif	38.6174	36.7372	0.000074	0.0012
	barbara.Jpg	36.4341	30.25	0.000074	0.003
	ranch.bmp	37.3432	31.653	0.000074	0.0012
	liftingbody.png	38.4401	30.2705	0.000074	0.0061
Liftingbody.png	lena.tif	37.6172	31.8271	0.0014	0.0013
	barbara.jpg	37.6735	30.5944	0.0014	0.0021
	pirate.bmp	37.5189	30.6333	0.0014	0.0016
	mandril.png	37.8463	31.4820	0.0014	0.0023
Ranch.bmp	lena.tif	37.2856	33.0564	0.0005	0.0061
	barbara.jpg	38.3256	33.5432	0.0005	0.0016
	pirate.bmp	37.4265	32.1544	0.0005	0.0047
	liftingbody.png	38.2330	31.2061	0.0005	0.0062

TABLE 8: Performance Analysis of the Proposed Technique for Different Hiding Capacity.

Cover Image [Mandril.jpg]	Payload Image [Barbara.jpg]	%Capacity	PSNR (CI&SI) (dB)	PSNR(PL&EPL) (dB)
512*512	256*256	25	44.4238	45.7815
512*512	512*256	50	43.9852	37.0397
512*512	512*384	75	43.9543	37.1437
512*512	512*512	100	43.9100	36.9712

iii) Comparison of performance parameters of proposed algorithm with existing algorithms.

Table 9 shows the comparison of PSNR (CI& SI)) and percentage Hiding Capacity (HC) of proposed technique and the existing techniques. The percentage hiding capacities of the proposed algorithm is 100% with PSNR (CI & SI) varies between 35.79 and 42.94 based on cover images are compared with existing techniques presented by Hoda Motamedi and Ayyoob

Jafari [27], Tasnuva Mahajabin et. al., [28] and Ashish Soni et.al.,[29]. It is observed that the PSNR values and percentage hiding capacity values are higher in the case of proposed algorithm compare to existing algorithms for the following reasons.

(i)The percentage hiding capacity is 100% since six high frequency sub bands which form the real are used for embedding payload with good payload retrieval quality at the destination.

(ii) The scaling factor is chosen based on the entropy of the cover image. When the entropy is zero the scaling factor is high, this reduces the Euclidean distance between the high frequency sub bands of cover image and stego image, thus giving high PSNR and good retrieval payload quality.

(iii) The PSNR value does not vary significantly though the capacity is varied because of the high frequency sub bands which have negligible randomness.

(iv) when the entropy of cover image is non zero then the scaling factor is reduced from higher value and fixed at 16 to obtain better quality of retrieved payload image at the destination. The PSNR (CI&SI) is decreased since scaling factor is reduced.

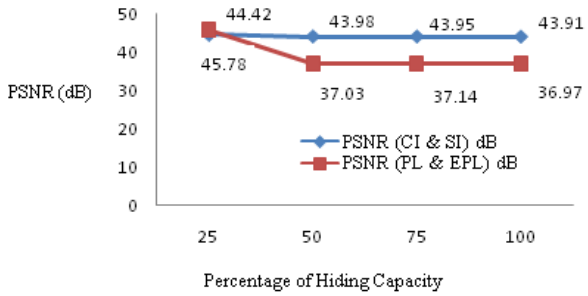


FIGURE 8: variation of PSNR and hiding capacity.

TABLE 9: Comparison of capacity and value of proposed algorithm with the existing algorithms.

Authors	Technique	Cover image	PSNR (CI & SI) (dB)	HC (%)
Hoda Motamedi and Ayyoob Jafari [27]	Wavelet transform and image denoising techniques.	Barbara	39.65	62.37
		Boat	36.34	76.87
Tasnuva Mahajabin et. al.,[28]	Pixel value differencing and LSB substitution Method	Mandril	32.67	47.93
Ashish Soni et.al.,[29]	Discrete Fractional fourier Transform.	Rice	32.46	100
Proposed	coefficient replacement and adaptive scaling steganography based on DTCWT	Barbara	41.05	100
		Boat	42.49	100
		Mandrilla	42.94	100
		Rice	35.79	100

6. CONCLUSIONS

In this paper, an algorithm for embedding DTCWT based LL sub band coefficients of secret information into HH sub band coefficients of cover image using adaptive scaling is proposed. The novel coefficient replacement technique improves the security, PSNR and 100 percent hiding capacity. The adaptive scaling and use of DTCWT transformation yields better results compared to the existing techniques. In future, the proposed technique can be used in spatial domain.

7. REFERENCES

[1] Rig Das and Themirchon Tuithung, "A Novel Steganography Method for Image Processing Based on Huffman Encoding," Third National Conference on Emerging Trends and Applications in Computer Science, pp. 14-18, March 2012.

[2] Najeena K S and B M Imran, "An Efficient Steganographic Technique based on Chaotic Maps and Adpative PPM Embedding," International Conference on Signal Processing, Image Processing & Pattern Recognition, pp. 293 – 297, 2013.

[3] Ran-Zan Wang and Yeh-Shun Chen, "High-Payload Image Steganography using Two-way block Matching," IEEE Signal Processing Letters, Vol. 13, Issue 3, pp. 161 – 164, 2006.

[4] Vojtech Holub and Jessica Fridrich, "Designing Steganographic Distortion using Directional filters," IEEE International Workshop on Information Forensics and Security, pp. 234 – 239, 2012.

[5] BaolongGuo, Leida Li, Jeng-Shyang Pan, Liu Yang and Xiaoyue Wu, "Robust Image Watermarking Using Mean Quantization in DTCWT Domain," Eighth International Conference on Intelligent Systems Design and Applications, pp. 19 – 22, 2008.

[6] Ajit Danti and G R Manjula, "Secured Data Hiding of Invariant Sized Secrete Image based on Discrete and Hybrid Wavelet Transform," IEEE International Conference on Computational Intelligence & Computing Research, pp. 1 – 6, 2012.

[7] L Jani Anbarasi and S.Kannan, "Secured Secret Color Image with Steganography," IEEE International Conference on Recent Trends in Information Technology, pp. 44 - 48, 2012.

[8] V Sathya, K Balasubramaniyam, N Murali, M RajaKumaran and Vigneswari, "Data Hiding in Audio Signal, Video Signal, Text and JPEG Images," International Conference on Advances in Engineering Science and Management, pp. 741-746, 2012.

[9] Zawawi M. N. Mahmood. R, Udzir. N, Ahmad. F and Desa J. M, "Active Warden as the Main Hindrance for Steganography Information Retrieval," IEEE Information Retrieval and Knowledge Management International Conference, pp. 277-280, 2012.

[10] Ching-Nung Yang, Tse- Shih Chen, Kun Hsuan and Chung- Chun Wang, "Improvement of Image Sharing with Steganography and Authentication," Journal of System and Software, Elsevier , Vol 80, issue 7, pp. 1070 - 1076, July 2007.

[11] Chiang- lung Liu and Shiang- Rong Liao, "High Performance JPEG Steganography Using Complementary Embedding Stratergy," Pattern Recognition, Vol. 41, issue 9, Elsevier, pp. 2945-2955, September 2008.

[12] H. S. Manjunatha Reddy and K. B. Raja, "High Capacity and Security Steganography Using Discrete Wavelet Transform," International Journal of Computer Science and Security, vol. 3, issue 6 , pp. 462-472, 2010.

[13] K B ShivaKumar, K B Raja and Sabyasachi Patnaik, "Hybrid Domain LSB Steganography," International Journal of Computer Applications, Vol 19. No.7, pp. 35 - 39, April 2011.

[14] Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi and Kingo Kobayashi, "Intergrity Verification of Secret Information in Image Steganography," The Twenty ninth Symposium on Information Theory and its Applications, pp. 1 – 4, 2006.

[15] Xinpeng Zhang and Shou Zhang Wang, "Vulnerability of Pixel Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security," Pattern Recognition Letters, vol 25, issue 3, Elsevier, pp.331-339, February 2004.

[16] Chin - Chan Chang and Hsien- Wen Tseng, "A Steganographic Method for Digital Images Using Side," Pattern Recognition Letters, vol 25, issue 12, Elsevier, pp. 1431-1437, September 2004.

[17] H S Manjunatha Reddy and K B Raja, "Wavelet Based Non LSB Steganography," International Journal of Advanced networking and applications, vol 3, issue 3 pp. 1203 – 1209, 2011.

[18] K B Shiva Kumar, K.B. Raja, R. K. Chhotray and Sabyasachi. Patnaik, "Bit Length Replacement Steganography Based on DCT Coefficients," International Journal of Engineering Science and Technology, vol. 2(8), pp. 3561-3570, 2010.

[19] K B Shiva Kumar, K B Raja, R K Chhotray and Sabyasachi Patnaik, "Steganography Based on Payload Transformation," International Journal of Computer Science Issues, vol 8, Issue 2, pp. 241-246, March 2011.

[20] H S Manjunatha Reddy and K B Raja, "Wavelet Based Secure Steganography With Scrambled Payload," International Journal of Innovative Technology and Exploring Engineering, vol. 1, issue 2, pp.121 - 129, July 2012.

[21] Arnab Kumar Maji, Rajkumar Pal and Sudipta Roy, "A Novel Steganographic Scheme using Sudoku," International Conference on Electrical Information and Communication Technology (EICT), 2013 pp. 1 – 6, 2013.

[22] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar and Md. Delowar Hossain, "An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography," Third IEEE International Conference on Informatics, Electronics and Vision, pp. 1-6, 2014.

[23] Chi Yuan Lin, Shu cing Wu and Jyuan Jie Wang, "VQ Image Compression Steganography based on Section based Informed Embedding," International Symposium on Computer, Consumer and Control, pp. 111 – 114, 2014.

[24] W Sweldens, "The Lifting Scheme: A Construction of Second Generation Wavelets," SIAM Journal in Math. Analysis, vol. 29, no. 2, pp.511 – 546, 1998.

[25] Ivan.W.Selesnick, Richard.G.Baraniuk and Nick G. Kingsbury, "The Dual-Tree Complex Wavelet Transform," Signal Processing Magazine IEEE, Vol. 22, issue 6, pp. 123-151, 2005.

[26] Yue Wu, Joseph P Noonan and SOS Agaian, "Shannon Entropy based Randomness Measurement and Test for Image Encryption," Journal of Information sciences, Elsevier, pp. 1 – 23, 2011.

[27] Hoda Motamedi and Ayyoob Jafari, "A New Image Steganography based on Denoising Methods in Wavelet Domain," Ninth International Conference on Information Security and Cryptology, pp. 18 – 25, 2012.

[28] Tasnuva Mahjabin, Syed Monowar Hossain, and Md. Shariful Haque, “A Block Based Data Hiding Method in Images using Pixel Value Differencing and LSB Substitution Method,” Fifteenth International Conference on Computers and Information Technology, pp. 168 – 172. 2012.

[29] Ashish Soni, Jitendra jain and Rakesh Roshan, “Image Steganography using Discrete Fractional Fourier Transform,” International Conference on Intelligent Systems and Signal Processing, pp. 97 – 100. 2013.