British Journal of Applied Science & Technology
14(4): 1-12, 2016, Article no.BJAST.23942
ISSN: 2231-0843, NLM ID: 101664541

SCIENCEDOMAIN *international*
www.sciencedomain.org

Image Steganography Scheme Using Parent Child Relationship in Wavelet Domain

Geeta Kasana[1*], Satvinder Singh Bhatia[2] and Kulbir Singh[3]

[1]Department of Computer Science and Engineering, Thapar University, Patiala, India.
[2]School of Mathematics, Thapar University, Patiala, India.
[3]Department of Electronics and Communication Engineering, Thapar University, Patiala, India.

Authors' contributions

This work was carried out in collaboration between all authors. Author GK designed and implemented the research proposal. Authors SSB and KS supervised the research work. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2016/23942
Editor(s):
(1) Samir Kumar Bandyopadhyay, Department of Computer Science and Engineering, University of Calcutta, India.
Reviewers:
(1) Stepan Bilan, State Economy and Technology University of Transport, Kiev, Ukraine.
(2) Xiaoqiang Zhang, China University of Mining and Technology, China.
Complete Peer review History: http://sciencedomain.org/review-history/13240

Original Research Article

Received 29th December 2015
Accepted 22nd January 2016
Published 9th February 2016

ABSTRACT

In this paper, a steganography scheme for digital images by using Integer Wavelet Transform (*IWT*) is proposed. This scheme is based on the qualified significant wavelet tree (*QSWT*). In this scheme, the secret data bits are embedded into largest and smallest wavelet child coefficients of a parent wavelet coefficient of a cover image. Embedding of secret data bits are performed in selected wavelet subbands only so that the embedding capacity and Peak Signal to Noise Ratio (*PSNR*) can be achieved maximum as *PSNR* value decreases with the increase of embedding capacity. Visual quality of stego images produced by the proposed scheme is acceptable by human visual system as *PSNR* between cover and stego images is above 40 *dB* and extracted secret image is exactly the same as original secret image.

Keywords: Discrete wavelet transform; steganography; peak signal to noise ratio; integer wavelet transform; qualified significant wavelet tree.

[*]Corresponding author: E-mail: gkasana@thapar.edu;

1. INTRODUCTION

Security of digital data has become very important issue in this era of Internet. Two types of approaches are used to protect digital data from being captured during transmission on a public network. One is the cryptography in which the digital data is encoded into unreadable form by using encryption prior to transmission on a public network. On the receiver side, encoded data is decoded using secret keys. Another approach is the steganography which provides data security by hiding the information in a cover media so that even the existence of hidden information is not known to an intruder. The cover medium may be any digital medium such as an image, audio, or video. Digital images are widely used as carriers of secret information because of the high redundancy present in them. In image steganography applications, the image used for hiding a secret data is referred as the cover image and an image carrying hidden secret information is referred as a stego image. The hidden information may be of any type such as image, audio, video or text. The main challenge in steganography applications is that the secret information should be embedded in such a way that stego image does not deviate much from the original image, visually and statistically [1-3].

Image steganography can be performed in both spatial as well as transform domain. In spatial domain technique, the secret data is embedded by modifying pixel intensities of a cover image where as in the transform domain, cover image is first transformed in the frequency domain, then the transform domain coefficients are altered to embed the secret data and finally inverse transform is applied to obtain the stego image. Transform domain steganography techniques has high computational complexity, more robust and provides better imperceptibility than spatial domain techniques because when a stego image is inversely transformed, the embedded secret data is distributed irregularly over the image, making the attacker difficult to read or modify the embedded data. Many image steganography techniques have been proposed in the literature [4-18]. Shejul and Kulkarni [13] used the skin tone region of images to hide the secret data to propose a steganography technique. This skin tone detection is performed using Hue, Saturation and Value color space. Embedding capacity of their technique is 0.7% of the cover image size. Wavelet based non LSB steganography is proposed by Reddy and Raja [14] by using the blocks of the cover image. Each of the blocks is decomposed into wavelet domain by using *DWT/IWT*. Their main observation is that *PSNR* values between cover and stego images are higher in case of *IWT*. After going through the literature survey, it has been observed that no image steganographic scheme for wavelet domain exists using which the original extracted image can be recovered, without any loss, from its stego image. So there is the need to have a steganogrpahic scheme for wavelet domain.

This paper is organized into following sections. Section 2 contains an overview of *IWT*. The algorithms used for embedding, extracting process and evaluation parameters are described in Section 3. Experimental results and steganalysis tests are illustrated in Section 4 and conclusion in Section 5.

2. INTEGER WAVELET TRANSFORM

IWT is the invertible wavelet transform that maps integers to integers and have important applications in lossless coding [14]. *IWT* has the important property that *IWT* coefficients have the same dynamic range as the original data. This makes easier the implementation considerations regarding the size of variables to be used and the range to provide for in the coding algorithm. *IWT* is not only computationally faster and more memory-efficient but also more suitable in lossless data-compression applications. When an image is transformed using *IWT*, it is decomposed into four subbands as low low (*LL*) subband, low high (*LH*) subband, high low (*HL*) subband and high high (*HH*) subband. Again *IWT* can be applied on *LL* subband to generate further four subbands at next level. This decomposition continues till the required level of wavelet decomposition is achieved.

After transforming an image by using *IWT*, it is represented using tree because of the sub sampling that is performed in the transform. A wavelet coefficient in a low subband has four descendants in the next higher subband, as shown in Fig. 1(a). Each of these descendants also has four descendants in the next higher subband, as shown in Fig. 1(b).

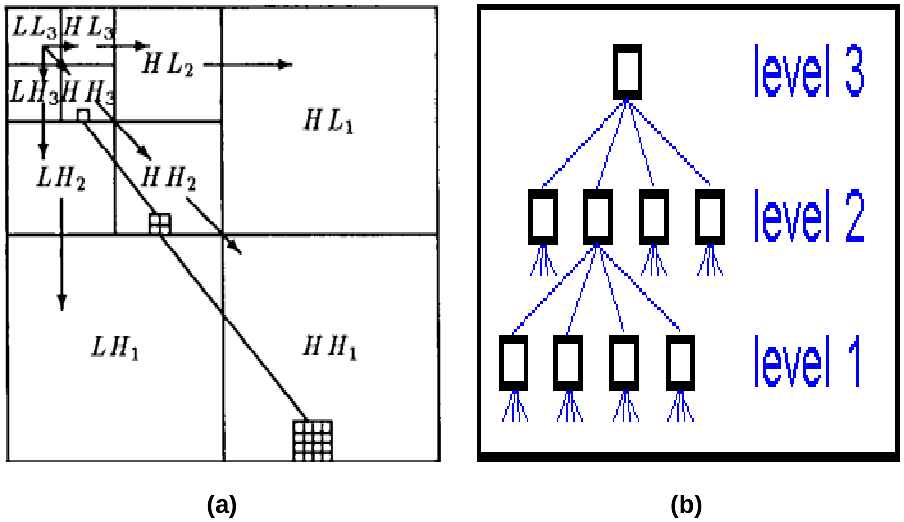


Fig. 1. (a) Parent child relationship of wavelet coefficients of image subbands. (b) Relationship between the levels of the wavelet decomposed image

3. PROPOSED STEGANOGRAPHY SCHEME

In this section, proposed steganography scheme is discussed. Secret data bits are embedded into largest and smallest child coefficients of a parent wavelet coefficient in a subband of cover image. Embedding is performed in selected subbands so that the capacity and PSNR can be achieved maximum as both capacity and PSNR are contradicting characteristics. The detail of the embedding and the extracting algorithm are given in following subsections.

3.1 Embedding Method

To embed the secret data *Se* into the cover image steps are as follows and also shown in Fig. 2.

Step 1. Decompose the cover image using *IWT* to obtain wavelet subbands b_i. Repeat Step 2 and Step 3 for all wavelet coefficients of selected subbands untill all secret bits *Se* are embedded into wavelet coefficients of a cover image.

Step 2. Find the largest child *l_child* from the children of each parent wavelet coefficient of a subband b_i and embed the secret data pixel using the following:

$$l\_child = \begin{cases} l\_child + 1 \ \ (if \ \ Se = 1 \, and \ l\_child \ is \ even) \ or \ (if \ \ Se = 0 \ and \ l\_child \ is \ odd) \\ l\_child \qquad otherwise \end{cases}$$

Step 3. Find the smallest child s*_child* from the children of each parent wavelet coefficient, and embed the secret data pixel using the following:

$$s\_child = \begin{cases} s\_child - 1 \ \ (if \ \ Se = 1 \, and \ s\_child \ is \ even) \ or \ (if \ \ Se = 0 \ and \ s\_child \ is \ odd) \\ s\_child \qquad otherwise \end{cases}$$

Step 4. Apply Inverse *IWT* to get the stego image.

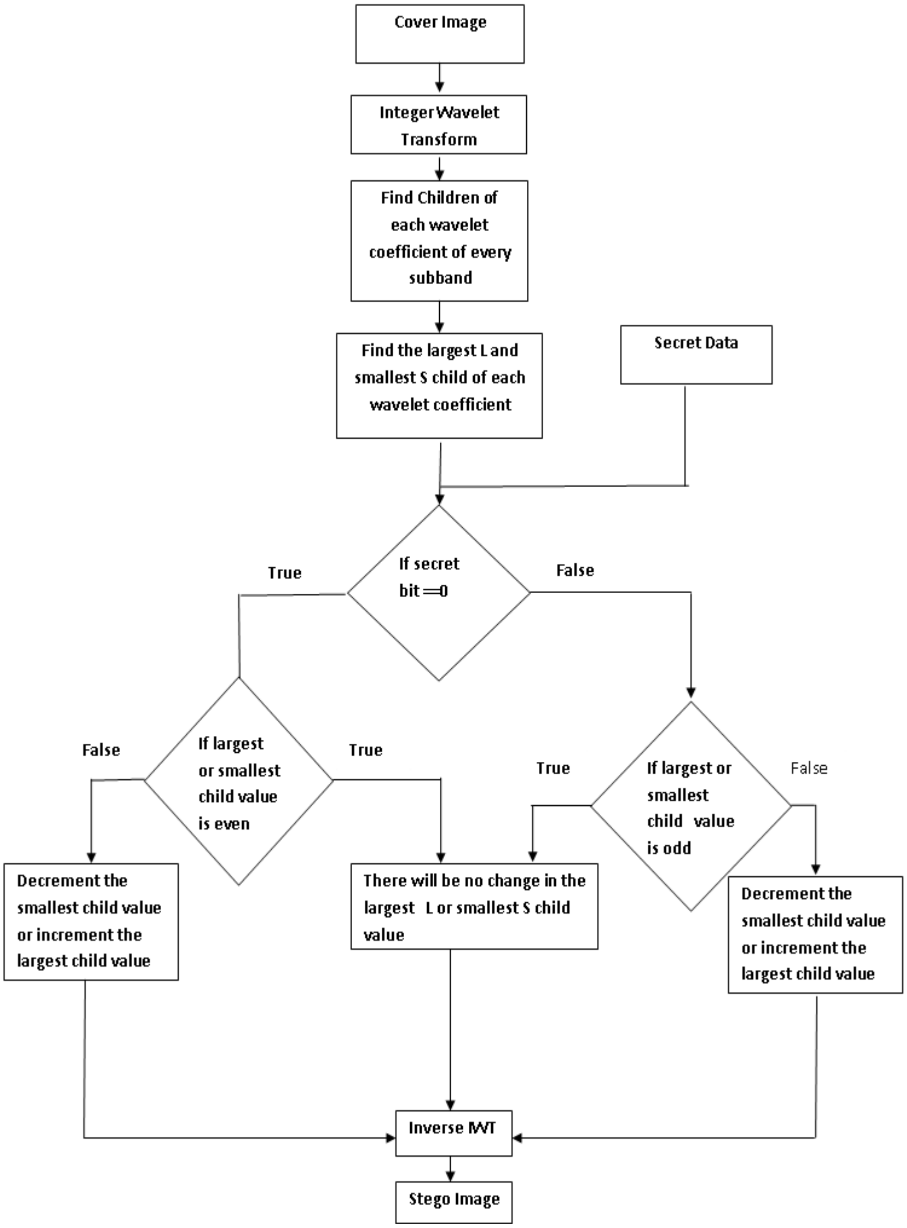

Cover Image
Integer Wavelet Transform
Find Children of each wavelet coefficient of every subband
Find the largest L and smallest S child of each wavelet coefficient
Secret Data
If secret bit==0
True
False
If largest or smallest child value is even
False
True
If largest or smallest child value is odd
True
False
Decrement the smallest child value or increment the largest child value
There will be no change in the largest L or smallest S child value
Decrement the smallest child value or increment the largest child value
Inverse IWT
Stego Image

Fig. 2. Embedding steps used in proposed scheme

3.2 Extracting Method

To extract the secret data from the stego image, steps are depicted in Fig. 3 and are as follows:

Step 1. Decompose the stego image using *IWT* to obtain wavelet subbands b_i. Repeat Step 2 and Step 3 for all wavelet coefficients of selected subbands and till all secret bits *Se* are extracted from wavelet coefficients of a stego image.

Step 2. Find the largest child *l_child* from the children of each parent wavelet coefficient of a subband b_i and extract the secret data pixel using the following:

$$Se = \begin{cases} 1 & if\ l\_child\, is\ odd \\ 0 & otherwise \end{cases}$$

Step 3. Find the smallest child *s_child* from the children of each wavelet coefficient of a subband b_i and extract the secret data pixel using the following:

$$Se = \begin{cases} 1 & if\ \ s\_child\, is\, odd \\ 0 & otherwise \end{cases}$$

Proposed scheme is explained with an example. A decomposed cover image is shown in Fig. 4.

Middle level subbands are selected to embed secret data bits instead of low level subbands as most of the image energy is stored in the low level subbands as embedding in low level subbands will cause more distortion which will further affect quality of stego image.

Consider a parent wavelet coefficients in third level subband at position(1, 65) and its four children will be at ((1, 129), (1, 130), (2, 129), (2, 130)) having the pixel values 119,-3,-8,-5. Similarly for next parent wavelet coefficient at position (1, 66) and its four children will be at position ((1,131), (1,132), (2,131) and (2,132)) having pixel values -4,-2,-8,-5 as shown in the Fig. 4. Suppose the secret data bits are “1110”.

To embed, check whether the secret data bit is zero or one. If it is one and child wavelet coefficient is odd then no modification is done otherwise modify it to make odd by adding or subtracting one. If it is zero and child wavelet coefficient is even then no modification is done in cover wavelet coefficient otherwise modify it to make even by adding or subtracting one.

Consider parent wavelet coefficient at position (1, 65) and its four children coefficients as shown in Fig. 5(a). First secret data bit is “1” and largest child wavelet coefficient is 119 *i.e.* odd (119mod 2) ≠ 0, there will be no change. Cover and stego child wavelet coefficients will be similar, as shown in Fig. 5(b).

Next sceret bit is ”1” and smallest child wavelet coefficients is -8, *i.e.* even (8 mod 2)=0. To make wavelet coefficient as odd, subtract secret bit “1” from the cover wavelet coefficient and stego pixel will be -9 as shown in Fig. 5(b).

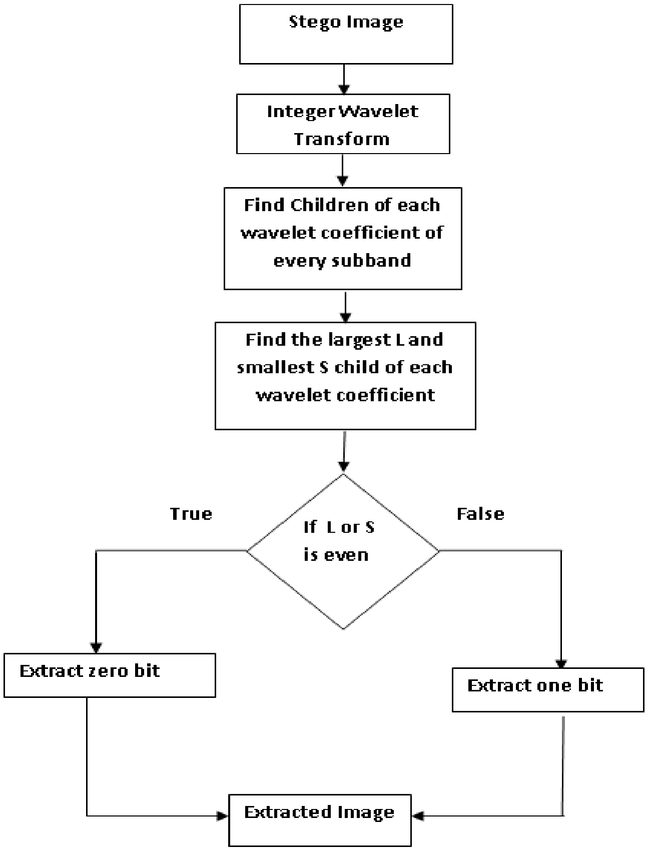

Stego Image
Integer Wavelet Transform
Find Children of each wavelet coefficient of every subband
Find the largest L and smallest S child of each wavelet coefficient
If L or S is even
True
False
Extract zero bit
Extract one bit
Extracted Image

Fig. 3. Extracting steps used in proposed scheme

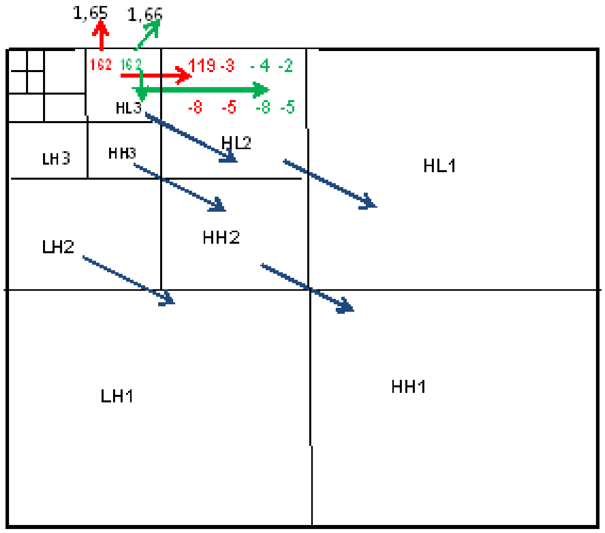
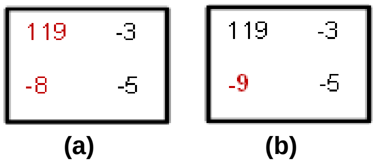


Fig. 4. Parent child relationship of wavelet coefficients of image subbands



119	-3
-8	-5

(a)

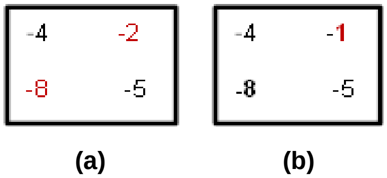
119	-3
-9	-5

(b)

Fig. 5. Children of first parent at position (1,65) (a) cover) (b)Stego

Similarly consider next parent wavelet coefficient at (1,66) and their children coefficients as shown in Fig. 4 in green color and below Fig. 6(a). Find the largest and smallest wavelet child coefficient. The largest child coefficent of this parent wavelet coefficient is -2. Next secret data bit is ”1” and child wavelet coefficient is even so it needs to make it odd by adding “1”. So largest wavelet coefficient will be largest.

Next secret bit is ”0” and smallest wavelet child coefficient is -8, as both secret bit and cover wavelet coefficient are even, no need to make any modification into the cover wavelet coefficient. Therfore stego pixel will similar to the cover wavelet coeffient as shown in Fig. 6(b).



-4	-2
-8	-5

(a)

-4	-1
-8	-5

(b)

Fig. 6. Children of second parent at position (1,66) (a) cover (b) Stego

In this way, the secret data bits are embedded into children wavelet coefficents of the cover image.

For extraction process, decompose the stego image by uisng IWT. Consider the stego children of respective parents.

In example, parent at (1,65) position and their four children coefficients as shown in Fig. 5(b) Find out the largest child *i.e.* 119, which is odd, so extracted secret bit will be “1”. Find out the smallest child *i.e.* -9, it is again odd, therefore next extracted bit is “1”. So from these children, extracted bits are 11.

Consider the next parent at (1,66) position and their four children coefficients as shown in Fig. 6(b). Find out the largest child *i.e.* -1, it is odd, so extracted bit will be “1”. Find out the smallest child for same parent *i.e.* -8, it is even, therefore next extracted bit is “0”. So from these children extracted bits are 10. So finally secret bits ”1110” are extracted.

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

In this section, empirical results show the satisfactory performance of proposed steganography scheme in terms of its effectiveness (imperceptibility) and feasibility. The proposed scheme is implemented in MATLAB software. Cover images are decomposed upto 5 levels using *IWT*. Original secret image is shown in Fig. 7(a) and cover images considered in this work are uncompressed 512×512 gray images like Lena, Barbara, Baboon, Truck, Pepper, Airplane, Boat, Sailboat, and Zelda *etc*. few of them are are shown in Figs. 8(a) to (d). All of these images are taken from the standard image database which is used by the researchers working in the domain of image and computer vision [19].

4.1 Experimental Results

A steganography scheme is often measured in terms of visual quality of the stego images through the *PSNR*. *PSNR* is used to measure the distortion between the cover and stego image. A large *PSNR* value means that the stego image is almost similar to the cover image. *PSNR* is defined by the expression

$$PSNR = 10log_{10}\frac{255^2}{MSE}$$

where *MSE* is the mean square error and is defined as

$$MSE = \sum_{m=1}^{h}\sum_{n=1}^{w}\frac{\left(Y(m,n) - X(m,n)\right)^2}{h \times w}$$

where $Y(m,n)$ is the pixel of marked image and $X(m,n)$ is the pixel of cover image, h and w is the height and width of the images, respectively.

For steganalysis and also to show imperceptibility, mean and standard deviation i.e. first and second order moments are used.

First Order Moment:

$$M1 = \frac{\sum_{i=1}^{i=n} X_i}{n}$$

Second order Moment:

$$M2 = \sqrt{\frac{1}{n-1}\sum_{i=1}^{i=n}(X_i - \bar{X})}$$

where *n* is the total number of pixels in image or subband and X_i is the image pixel and $\bar{X}$ is the mean of the image or of a subband.

The visual quality of stego images is the most important property in case of steganography system so that it does not create the suspicious to the attackers. A large *PSNR* value means that the stego image is almost similar to the cover image. Table 1 shows the *PSNR₁ i.e. PSNR* between cover and stego images where as *PSNR₂* is *PSNR* between original and extracted secret image.

Table 1. *PSNR₁* and *PSNR₂* of different images after embedding 122760 bits of secret image

Image	*PSNR₁(dB)*	*PSNR₂ (dB)*
Lena	43.2831	Inf
Boat	43.4416	Inf
Pepper	43.3185	Inf
Airplane	42.5327	Inf
Barbara	42.9660	Inf
Tank	42.4401	Inf
Zelda	40.7365	Inf
Truck	43.3209	Inf
Sailboat	43.2045	Inf

PSNR₁ is calculated between cover and stego images after embedding secret image size $248 \text{ X } 495$. *PSNR* in proposed scheme is above 40 *dB* which is higher than the standard measurement of 30 *dB*. This means that the secret image which is embedded in the cover image is imperceptible to human vision. The extracted secret image, shown in Fig. 7(b), is similar to original secret image and *PSNR* between original secret image and extracted secret image is infinity, as shown in Table 1, *SIM* and correlation is also one. Fig. 8 shows that there is no much visual difference between cover and stego images.

(a) (b)

Fig. 7. Secret images (a) original (b) extracted

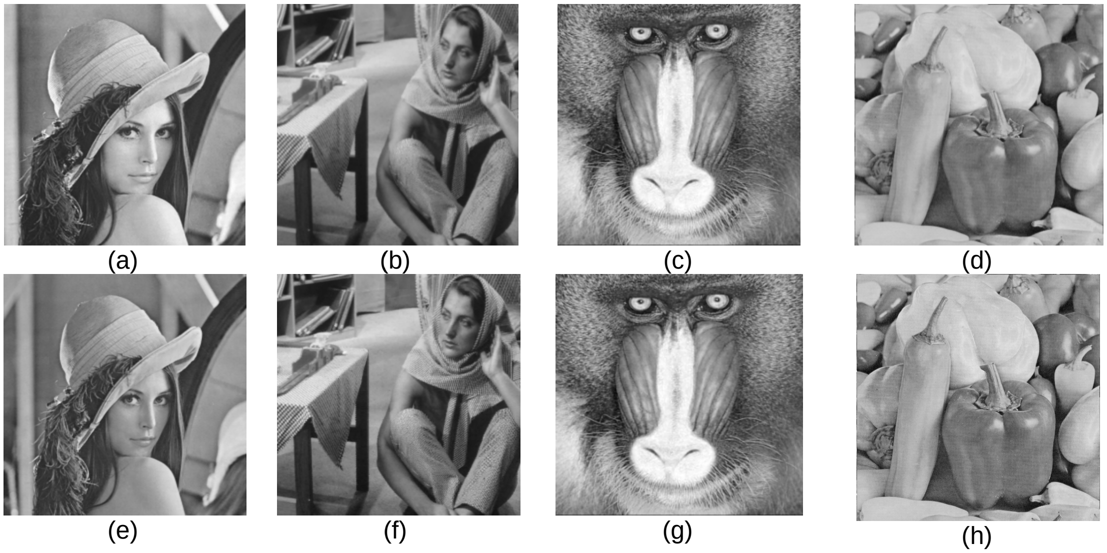


Fig. 8. (a) to (d) cover images of Lena, Barbara, Baboon and Pepper. (e) to (h) Stego images of Lena, Barbara, Baboon and Pepper

Table 2. *PSNR* (in *dB*) at different capacities embedded into different images

Capacity(bits)	Lena	Boat	Pepper	Truck
2500	58.4798	59.7382	57.7440	59.0564
10000	52.8599	53.3748	52.3966	53.3078
22500	49.3930	50.3339	48.9264	49.6652
40000	46.5356	47.0448	46.4593	46.5273
50625	45.4781	45.959	45.7441	45.7118
61009	44.8642	45.9590	44.9432	44.7082
85209	44.1514	45.2090	44.2483	44.0307
98800	43.7232	45.2991	43.9005	43.6549
111150	43.4929	44.6805	43.6140	43.4316
122760	43.2831	43.4416	43.3185	43.3209

Table 2 shows that when embedding capacity increases, *PSNR* between stego and cover image decreases. After embedding 2,500 bits in the cover image, maximum *PSNR* between cover and stego image is 59.7832 *dB.* As capacity increases to 1, 22,760 bits, *PSNR* is 43.4416 *dB i.e.* above 30 *dB* [13] which shows that the imperceptibility is maintained by the proposed scheme.

If an image contains extra data information, obvious its statistical properties get change and that can decreases its imperceptibility. So only *PSNR* is not sufficient to show that the stego image is imperceptible, one can analyze it by comparing and observe the differences between the statistical properties of cover and stego images that maintained its texture and imperceptibility. In the proposed scheme, three statistical properties- histogram, first and second order moments and entropy that characterize the texture of an image are used.

4.2 Histogram Analysis

Histogram of a wavelet subbands reflects the statistical distribution of wavelet coefficients in the subband. The visually quality and imperceptibility can be analyzed using histograms shown in Fig. 9. It is observed that there are no significant changes in the stego image histogram of Lena when compared to the histogram of the cover image Lena. There are no noticeable changes of higher significance are found in the analysis. Even when compared the histogram of individual bands of cover image to stego image there were no noticeable changes. Thus this makes the proposed method more secure and robust against susceptible attacks. The basic point of this though is not to see just the histograms are similar to our eyes, but to see how the stego image preserves the statistics of the cover image. The attack is based on how the coefficients behave after embedding. By seeing histograms of stego images, one can say that they have maintained the same symmetry to the cover image. Hence, on the basis of histogram, one can say imperceptibility is maintained by the proposed scheme.

4.3 First and Second Order Moment

First and second order moments *i.e.* mean and standard deviation of different cover and stego images are calculated and their differences are observed. The absolute difference between cover and stego image is very little as shown in Table 3. After analyzing the results from Table 3, one can observe there is little difference in the first and second order moments of cover and stego image which does not attract the attacker to get suspicious about the hidden data.

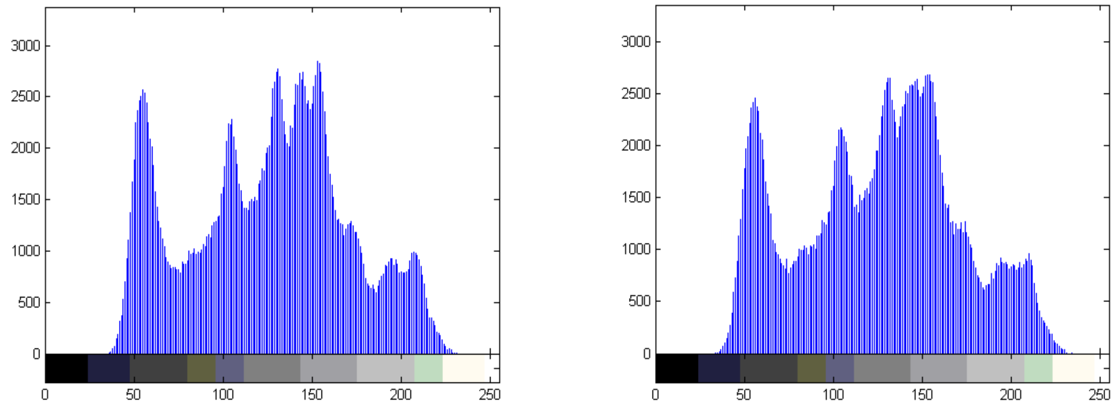
4.4 Entropy Analysis

It is the measurement of randomness that can be used to characterize the texture of an image. Entropy of an image is defined as:

$$-\sum_{i=1}^{n} a_i \log(\Pr(a_i))$$

where a_i, *i*= 1, 2, …, *n*, is the value of *i*th gray level of image, *n* is the total number of different gray levels in the image and $Pr(a_i)$ is the probability of gray level a_i of the image.

Entropy of the cover images and stego images are calculated and their differences are shown in Table 4.



(a)

(b)

Fig. 9. Histogram of (a) cover image Lena and (b) Steo image Lena

Table 3. Absolute difference of first and second order moments between stego and cover images

Image	**Mean of cover image$(\mu 1)$**	**Mean of stego image $(\mu 2)$**	**Absolute difference $(\mu 1 - \mu 2)$**	**Standard deviation of cover image$(\sigma 1)$**	**Standard deviation of stego image $(\sigma 2)$**	**Absolute difference $(\sigma 1 - \sigma 2)$**
Lena	125.1605	125.5552	0.3947	11.8995	11.8578	0.0416
Boat	129.7080	130.2064	0.4985	9.0416	9.0228	0.0188
Pepper	149.8213	150.2377	0.4164	8.3655	8.3873	0.0217
Airplane	177.5769	178.0323	0.4553	6.8019	6.7882	0.0137
Barbara	113.8497	114.3328	0.4830	8.3985	8.3828	0.0157
Tank	132.3847	132.8710	0.4863	9.7859	9.7737	0.0121
Zelda	91.1696	91.5374	0.3677	8.7820	8.8195	0.0375
Truck	107.1140	107.5301	0.4161	4.4469	4.4717	0.0248
Sailboat	31.0070	131.4647	0.4577	9.2365	9.2738	0.0372

Table 4. Absolute difference of entropy between cover and stego images

Image	Entropy of cover image(ec)	Entropy of stego image $(\boldsymbol{es})$	Absolute difference $(\mathbf{ec} - \mathbf{es})$
Lena	7.3479	7.3645	0.0166
Boat	7.1914	7.2255	0.0341
Pepper	7.3388	7.3456	0.0068
Airplane	6.7178	6.7527	0.0350
Barbara	7.5927	7.6032	0.0106
Tank	5.4957	6.4197	0.9239
Zelda	7.2668	7.2795	0.0127
Truck	6.0274	6.5966	0.5692
Sailboat	7.3124	7.3277	0.0153

From this table, one can observe that entropy of stego images is almost same to the cover images. So on the basis of entropy test, one can say stego image maintained its texture near about to the cover image *i.e.* presence of secret data image is not detectable and imperceptibility is maintained.

From the entire above statistical test performances one can conclude that stego images preserved the statistic properties of cover image *i.e.* scheme avoids the detector to get suspicious about the presence of hidden secret data.

Proposed scheme is compared with existing wavelet based steganography schemes and this comparison is shown in Table 5. For this comparison, maximum data, which can be embedded by an existing scheme, is embedded into a cover image and same amount of data is embedded into corresponding cover image using proposed scheme and then *PSNR* between cover and stego images are calculated. From this comparison, one can conclude that proposed scheme provides higher capacity and better image quality, as *PSNR* between stego and cover images provided by proposed scheme is higher than *PSNR* provided by existing schemes. Maximum PSNR gain is more than 14.52 *dB* at same capacity percentage. *PSNR* of [20] is higher than proposed scheme, but maximum embedding capacity of their technique is 5.60 percentages which is less than maximum embedding capacity (6.20%) of the proposed scheme.

5. STEGANALYSIS

Steganalysis is the concept used to determine whether a medium carries some hidden information or not. Steganalysis serves a way to evaluate the security performance of steganography techniques. One can say a good steganography scheme should be imperceptible not only to human vision systems, but also to computer analysis.

Table 5. Comparison of *PSNR* at different capacities with existing schemes

Scheme	Maximum capacity (in %)	Maximum PSNR
(Shejul et al. 2011) [13]	0.70	64.92
(Reddy et al. 2011) [14]	1.50	38.21
Proposed	6.25	43.95
	1.50	47.9050
	0.70	51.3315

The wavelet transform is known for its competence of multi-resolution decomposition and coefficients de-correlation. The characteristics/feature extracted from one high frequency subband is un- correlated to that extracted other high frequency subband at the same level. Therefore, features from different subbands can form an M-D (Multi-Dimensional) feature vector with different dimensions most likely to un-correlated to each other. After considering this point the M-D feature vector can be suitable to represent the image for steganalysis. Therefore, the statistical moments of the wavelet characteristic function are good candidates of features for steganalysis.

Considering M-D feature Vector are Mean and Standard Deviation. In the proposed scheme, a five level wavelet transform is performed to the image used for hiding secret data. Each band has two features, totally 32 features which form a 32-D vector for steganalysis for each image. Tables 6 and 7 show the derived data for steganalysis for pepper and boat, if one observed there is minor differences, that shows it's quite difficult for the detector to detect something is hidden inside the image, because imperceptibility is very good.

Table 6. 32-D feature vectors of cover and stego image of Pepper

Bands	Mean of cover image $(\mu1)$	Mean of stego image $(\mu2)$	Absolute difference $(\mu1-\ \mu2)$	Standard deviation of cover image$(\sigma1)$	Standard deviation of stego image $(\sigma2)$	Absolute difference $(\sigma1-\sigma2)$
LL5	5.6094	5.6094	0	13.6036	13.6036	0
HL5	-0.6172	-0.6172	0	1.3679	1.3679	0
LH5	8.1289	8.1289	0	20.7568	20.7568	0
HH5	0.5430	0.5430	0	1.5559	1.5559	0
HL4	-0.7275	-0.7275	0	4.9774	4.9774	0
LH4	2.4482	2.4482	0	16.1259	16.1259	0
HH4	-1.6709	-1.6709	0	5.6647	5.6647	0
HL3	0.0361	0.0361	0	4.6587	4.6587	0
LH3	0.3103	0.3103	0	5.0021	5.0021	0
HH3	0.9858	0.9858	0	7.2066	7.2066	0
HL2	0.0527	0.0506	0.0001	5.2973	5.2776	0.0197
LH2	0.3609	0.3630	0.0021	6.2716	6.2689	0.0027
HH2	0.2148	0.2118	0.0030	4.6656	4.6530	0.0126
HL1	0.1053	0.1070	0.0017	4.4282	4.4116	0.0166
LH1	0.3506	0.3487	0.0019	5.1598	5.1623	0.0025
HH1	0.2320	0.2335	0.0015	4.2544	4.2538	0.0006

Table 7. 32-D feature vectors of cover and stego image of Boat

Bands	Mean of cover image $(\mu1)$	Mean of stego image $(\mu2)$	Absolute difference $(\mu1-\ \mu2)$	Standard deviation of cover image$(\sigma1)$	Standard deviation of stego image $(\sigma2)$	Absolute difference $(\sigma1-\sigma2)$
LL5	0.6445	0.6445	0	7.3663	7.3663	0
HL5	0.0859	0.0859	0	1.6404	1.6404	0
LH5	0.5977	0.5977	0	1.4134	1.4134	0
HH5	0.4570	0.4570	0	1.7941	1.7941	0
HL4	0.1719	0.1719	0	3.8063	3.8063	0
LH4	0.7715	0.7715	0	3.7667	3.7667	0
HH4	0.7754	0.7754	0	4.1746	4.1746	0
HL3	0.6614	0.6614	0	4.4267	4.4267	0
LH3	0.3293	0.3293	0	4.6251	4.6251	0
HH3	0.1934	0.1934	0	4.8730	4.8730	0
HL2	0.2260	0.2298	0.0038	5.4829	5.4868	0.0022
LH2	0.4116	0.4119	0.0003	5.1342	5.1488	0.0146
HH2	0.0532	0.0535	0.0003	5.5378	5.5312	0.0066
HL1	-0.1190	-0.1181	0.0009	4.7700	4.7631	0.0069
LH1	0.1638	0.1638	0	4.9404	4.9337	0.0067
HH1	0.1373	0.1395	0.0022	4.6940	4.6869	0.0071

6. CONCLUSION

In this paper, a novel scheme is proposed to embed secret image data into the cover image by finding largest and smallest children of each parent wavelet coefficients. Maximum *PSNR* gain is more than 9.6950 *dB* at same capacity and its embedding capacity is 4.3% and 5.1% higher than Reddy et al. [14] and Shejual et al. [13] respectively. Also, no extra information or overhead is required to extract the hidden secret data, and extracted secret image is similar to original secret image as *PSNR* between them is infinity and correlation is one for all the images considered in this work.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital watermarking and steganography, Morgan Kauffman; 2007.

2. Xuan G, Zhu J, Shi YQ, Ni Z, Su W. Distortionless data hiding based on integer wavelet transform. IEE Electronic Letters. 2002;38(25):1646-1648.
3. Tian J. Reversible data embedding using a difference expansion. IEEE Trans. on Circuits and Systems for Video Technology. 2003;13(8):890-896.
4. Wang SJ. Steganography of capacity required using modulo operator for embedding secret image. Applied Mathematics and Computation. 2005;64: 99-116.
5. Nag A, Biswas S, Sarkar D, Sarkar PP. A novel technique for image steganography based on DWT and Huffman encoding. International Journal of Computer Science and Security. 2011;4(6):561-570.
6. Chen PY, Lin HJ. A DWT based approach for image steganography. International Journal of Applied Science and Engineering. 2006;4(3):275-290.
7. Alnawok F, Ahmed B. Multi segment steganography technique. The International Arab Journal of Information Technology. 2006;5(3):253-257.
8. Abdallah HA, Hadhoud MM, Shaalan AA. An efficient SVD image steganographic approach. IEEE. 2009;257-262.
9. Safy ROEl, Zayed HH, Dessouki AEl. An adaptive steganographic technique based on integer wavelet transform. IEEE. 2009; 111-117.
10. Hossian M, Haque AL, Sharmin F. Variable rate steganography in grey scale digital images using neighborhood pixel information. The International Arab Journal of Information Technology. 2010;7(1):34-38.
11. Ataby AA, Naima FA. A modified high capacity image steganography technique based on wavelet transform. The International Arab Journal of Information Technology. 2010;7(4):358-364.
12. Bhattacharya S, Sanyal G. Data hiding in images in discreet wavelet domain using PMM. International Journal of Electrical and Computer Engineering. 2010;5(6):359-367.
13. Shejul AA, Kulkarni UL. A secure skin tone based steganography using wavelet transform. International Journal of Computer Theory and Engineering. 2011; 3(1):16-22.
14. Reddy HSM, Raja KB. Wavelet based non LSB steganography. International Journal of Advanced Networking and Applications. 2011;3(3):1203-1209.
15. Liu S, Farid H. Steganalysis using higher-order image-statistics. IEEE Transaction on Information Forensics and Security. 2006;1(1):111-119.
16. Banoci E, Bugar G, Levicky D. A novel method of image steganography in DWT domain. IEEE; 2011.
17. Bhattacharyya S, Kshitij AP, Sanyal G. A novel approach to develop a secure image based steganographic model using integer wavelet transform. IEEE International Conference on Recent Trends in Information, Telecommunication and Computing. 2010;173-178.
18. Chen WJ, Chang CC, Le THN. High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications, Elsevier. 2010;3292-3301.
19. Available:http://sipi.usc.edu/database/
20. Swain G, Lenka SK. A novel approach to RGB channel based image steganography technique. The International Arab Journal. E-Technology. 2012;2(4):181-186.

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/13240