Indian Journal of Science and Technology, Vol 9(46), DOI: 10.17485/ijst/2016/v9i46/86623, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Adaptive Embedding Approach in Color Image Carrier for Covert Communication

Haider Ismael Shahadi[1], Ahmed Toman Thahab[1] and Manaf Mohammed Ali[2]

[1]Electrical and electronic engineering department, university of Kerbala, 56001, Karbala, Iraq; haider_almayaly@yahoo.com, toeahmed@gmail.com
[2]English education department, University of Karbala, 56001, Karbala, Iraq; manafgq77@yahoo.com

Abstract

Steganography plays a vital role in the field of covert communication. This paper proposes a novel embedding scheme which embeds secret data adaptively. The proposed scheme employs integer to integer Lifting Wavelet Transforms (LWT) and pixel strength to specify suitable locations for data embedding. The integer LWT eliminates distortions, which is produced because of rounding process in the convolutional wavelet transforms. The performance of the proposed scheme is addressed using image quality metrics based on Peak Signal To Noise Ratio (PSNR) versus embedding ratio. Moreover, Bit Error Rate (BER) is utilized to assess robustness of the scheme. The experimental results show that the proposed is superior over several embedding techniques such as embedding based convolutional wavelet transforms and Lest Significant Bits (LSBs). The range of PSNR is gained between 51.52 and 22.15dB for range of embedding rate between 5% and 35%. Furthermore, the technique results error free for retrieving of secret data. In addition to the above features, the proposed technique increases security level of embedded data due to adaptive embedding process that increases randomly of embedding locations. The proposed scheme can be used in several important applications such as bank tag for authentication, military communications. Also, it can be implemented easily as a hardware chip and combine with covert imaging systems.

Keywords: Adaptive Embedding, Covert Communication, Lifting Wavelet Transform, Steganography, Security.

1. Introduction

Digital steganography is a technique known to conceal secret data inside a digital media with intent to be undetectable[1, 2, 3]. It is widely used nowadays in information security technologies. The technique has become essentially important over the last decade together with extensively spreading of internet[4, 5]. Unlike cryptography, that changes secret message to be ambiguous to hackers unless they have a decryption key, steganography hides the reality of message existents[6, 7].

The vast majority of image steganography techniques explore the maximum amount of redundancy in cover image in order to embed the secret data inside the cover image[8, 9]. Message data ought to be visually imperceptible and should not cause any noticeable alteration in the original cover image[10, 11, 12]. Imperceptibility means that the output cover after embedding the secret data, which is called "stego", should be highly correlated to the original cover media. In addition to imperceptibility, quality, security and capacity are also essential factors in assessing the performance of an image steganography algorithm[13, 14]. A superior algorithm accumulates the above factors to produce a robust steganography technique. The essential role of image steganography has imposed its shadow on researchers and numerous papers have been published in this evolving field. One of the types of steganography is key based algorithm which uses a key to embed data.

*Author for correspondence

Authors in[15] used a technique to enhance the existing least significant bit (LSB) method for increasing security of the embedded secret data. The technique is based on using a secret key encryption that encrypts the position of the secret data being embedded and data is embedded according to the key. Although a maximum peak signal to noise ratio (PSNR) of 53.7869 dB is attained but embedding capacity is not debated in the paper which is considered as an essential factor since quality alters with capacity.

Other techniques were used utilizing source coding methods. The authors in[16] have used Huffman encoding which is performed on the secret data and embed in the cover image using LSB method. Although the technique achieved a PSNR of 57.43, however, the major drawbacks are that the Huffman table and size of bit stream must be known to the receiver as well the Huffman encoding requires long processing time to encode the secret data. The capacity of the technique used in 16 is 25% of the cover image size. According to the researches[17, 18, 19] the direct LSB method has fragile security level and limited capacity; therefore, it has been enhanced over the years. In[17], the authors had been proposed an enhancement for direct LSB-substitution which possesses an increase in security level. A Ron Code (RC4) algorithm was utilized to achieve the randomization in hiding secret data bits in the cover image instead in hiding the bits in sequential manner. The main disadvantage in the former method is that the algorithm is complex and requires a significant processing time.

Increasing embedded data capacity in the chosen cover media (eg. image) based on spatial domain lead to modification noticeability in the cover media. As a result, the steganography approach is failed. In order to increase embedding capacity without compromise imperceptibility, other domains can be used such frequency and wavelet domains[20]. In these domains, the designer of the embedding algorithm can specify the frequency or bands that unnoticeable after embedding of secret data based on Human Visual System (HVS)[21]. However, wavelet domain is more suitable for image steganography than conventional frequency domains (eg. Fourier and discrete cosine transforms). This is because that wavelet transform provide high resolution for spatial domain in low frequencies and low resolution for spatial domain in high frequencies and vice versa for frequency domain[22]. This type of dividing the resolution of spatial and frequency domains gives more facility to find unnoticeable bands for data embedding.

Recently, several researches have been based on discrete wavelet transform (DWT) because it's above mentioned features. In[23], the authors have proposed to embed data in the DWT coefficients. The method implies conducting a Haar DWT on the secret and cover image and embed the secret data in the DWT coefficients of the cover image. The method increases security of the hidden data since, the algorithm finds the most similar match between the smooth cover block and smooth message block, therefore; the resultant stego image correlates the original cover. The research does not mention any information about the stego image quality which should be correlated with the original cover image. Moreover, the method is complicated since it is computationally expensive. In[24], the authors have proposed a steganography using DWT. The cover image and secret image is modified after applying the DWT transform. The approximation band and horizontal band of the cover image and the approximation band of the secret image are partitioned to 4x4 blocks. Each 4*4 block of the approximation band secret image is searched in the partition block of the approximation cover image, a block with minimum error is considered as a best match. The secret key is the address of the best match. The error value is then searched in the partitioned horizontal band using the root mean squared error; the least value is stored in the cover image horizontal band. A second address key is also presented.

Although this method is considered as a secure method but it is computation expensive since the secret and cover image is partitioned and a block search algorithm is conducted twice per block to find the best match. The composition and decomposition of the DWT produces floats that can falsify the positions of the keys, therefore; the secret image could be corrupted. The quality of the PSNR of the stego image is in the range of 29.64dB-23.38dB for various cover and secret images. Some steganography algorithms utilize encryption to the secret message to increase security. The authors in[25] have proposed a steganography method using encryption and DWT. The DWT is applied on the cover image; a threshold calculation is applied to determine the redundancy in the cover image. The message is partitioned and converted to one dimension bit stream and encrypted using RC4 algorithm. Before embedding, DWT is also applied to the encrypted bit stream message. The embedding process implies replacing DWT coefficients of the encrypted message in the previously specified DWT of the cover image. Since it uses redundancy determination in a pixel level and uses encryption to increase security, expensive

computational is a major drawback of the proposed method, therefore; it requires hard ware resources such as processor speed and memory.

All the above methods that are based on convolution DWT have common critical drawbacks as well as their own individual disadvantages. These drawbacks are related to the recovered hidden data, where, all the above methods are considered lossy methods, and require extensive computation. The losing parts of hidden data because data type conversion from integer spatial domain of image into floating point in wavelet domain and verse versa, impose to rounding and truncated processes in the pixels values that carried the hidden information. As a result, errors will be happened in the recovered messages[24, 25].

In order to obtain fully recovered messages and low computational cost, this paper employs integer mode of lifted wavelet transform (LWT) in the proposed image steganography. The integer-LWT has several advantages over convolutional DWT in addition to lossless and low complexity such as require fewer resources to be implemented, it does not require an auxiliary memory to execute the inverse transform, and less memory size is needed to store its integer coefficients compared to the conventional DWT[24]. The proposed method in this paper takes in its consideration the strength of the LWT coefficient to embed data in its least significant bits (LSBs) adaptively. This technique utilizes LWT coefficient or not, and specify its number of embedding bit capacity based on its energy. The method gains two important features by using this adaptive embedding technique. Firstly, maintain the stego image quality by error reduction between cover coefficient and stego coefficient, and secondly, because of random embedding based on the cover coefficient strength, the security level of the embedded messages will be increased.

The rest of the paper organized as follows: Section two explain in details the hiding phase of the proposed method. Section three presents the recovery phase of the proposed method. Section four gives the results of some tests for the proposed steganography algorithm and comparison with the related algorithms. Finally, section five concludes the entire paper.

2. The Proposed Embedding Approach

In this section we describe our image steganography algorithm for hiding and recovering of secret data. As mentioned in the previous section, wavelet domain has specific features which make it best choice for steganography algorithms that achieve high embedding rates. In convolutional wavelet steganography such as[24, 25], the wavelet converts 8-bits unsigned integer pixels into non-integer coefficients. Therefore, those approaches scale the obtained coefficients and then convert them to a binary data. As a result, the retrieved hidden messages are not identical to the original ones. In order to solve this problem, we employ a lifting scheme to produce integer to integer wavelets. Integer to integer means the wavelet coefficients are also integer with same resolution of pixels (8-bits). So, there is no requiring to scale and rounding the coefficients. The errors in the recovered messages arise in non-spatial domains steganography because rounding and out of range errors. When an image transform to another domain, then change the pixels and back to spatial domain, the resulting pixels is not necessarily integer. Moreover, it is not in the range which the original pixels were. For example, if the bit resolution of image is8-bit/pixel, each pixel has a value within range of 0-255. But the produced pixel from transformation process can be any value such as 300. The values of out range require truncating to save in file or transmitted over a channel with the same original resolution before transformation (eg. 300 truncate to 255, 8-bits/pixel). Therefore, some information that is hidden in the LSBs' is lost.

Since we use integer to integer wavelets, we solve the errors due to non-integer values. With the aim of cancel out of range errors, we have not inserted equal data in all coefficients. As an alternative, our technique selects the number of LSBs adaptively to replace with secret data. The technique takes in consideration two important factors the color and strength of the coefficient cover. Essentially, the human eyes are more sensitive to green and red than blue color. This fact employs in the proposed technique to embed more bits in blue color than red and green. Furthermore, the technique inserts more bits in bigger coefficient of pixels and fewer bits in smaller coefficients of pixels for the same color coefficients. This adaptive insertion is achieved by calculating the number of bits that are used for embedding in each coefficient according to the following formulas:

$$2^p < coef < 2^{p+1} \quad (1)$$

$$n = p - nbh \quad (2)$$

Where n is the number of bits to hold data in coefficient, p is the biggest power of 2 that is smaller than the coefficient

value coef, and nbh is number of bitsto be hold, which are used to reduce error between cover and stego coefficients. Therefore, with different values of nbh, different embedding rates and qualities can be attained. The nbh values enable the control by embedding rate for each color layer. The details of hiding and recovering phases of the proposed steganography method are explained in the following subsections.

2.1 Hiding of Secret Message

The proposed technique embeds secret data in a cover image after LWT process. The stages of the proposed hiding algorithm are explained in the block diagram of Figure 1.

Pre-embedding: The term conducts a broad range of operations. First of all, the color image that is a cover is segmented into a three layers of color planes R, G and B. Each layer of 2-dimension plane is converted to a one dimension vector. Since there are three planes, a three of a one dimension vectors are conveyed to the second stage. The entered pixel vectors to the remainder system stages arranges as B-pixel vector in the first, then R-pixel vector, and finally, G-pixel vector. This arrangement for pixels vectors gives a priority to embed data in the blue layer, then in the red layer and finally in the green layer. We employ in this arrangement the human vision system which is more sensitive to green and less sensitive to blue than red by around twice and half respectively.

Haar LWT: A lifted wavelet transform is applied to the pixel vectors. The operation will produce two bands of frequency contents for each vector, a low frequency content, which is known as "Smooth coefficients (A)" and obtained by process named "Update", and a high frequency content, which is known as "Detail coefficients (d)" and obtained by process named prediction[26]. The filter used in the decomposition is Haar filter because its symmetry that gives lossless transformation. The lifted wavelet transform localizes the low and high frequency contents and produces integer coefficients; therefore it does not require rounding of float numbers. Furthermore, the process is very fast compared to convolutional DWT. This is because the LWT splits the input pixels into odd and even according to its position in the input vector and then process them without decimation outputs by two as in the convolutional DWT. Formulas (3, 4, and 5) show the LWT steps (splitting, prediction and update).

$$\text{Splitting: } Sj\,(e),\ Sj\,(O) \tag{3}$$

$$\text{Prediction: } dj\text{-}1 = Sj\,(0) - \text{floor}\,(P\,\{Sj\,(e)\}) \tag{4}$$

$$\text{Update: } Aj\text{-}1 = Sj\,(e) + \text{floor}\,(U\,\{Sj\,(o)\}) \tag{5}$$

Where, S is an input vector of pixels, (S(e)) and (S(o)) are even and odd pixels respectively, P and U are the prediction and update functions that have formula depend on the wavelet filter (eg. Haar, Daubechies), and floor (z) is a function that finds the largest integer less than or equal to z. This rounding function is used in integer to integer type of lifting scheme and it is not required in floating type.

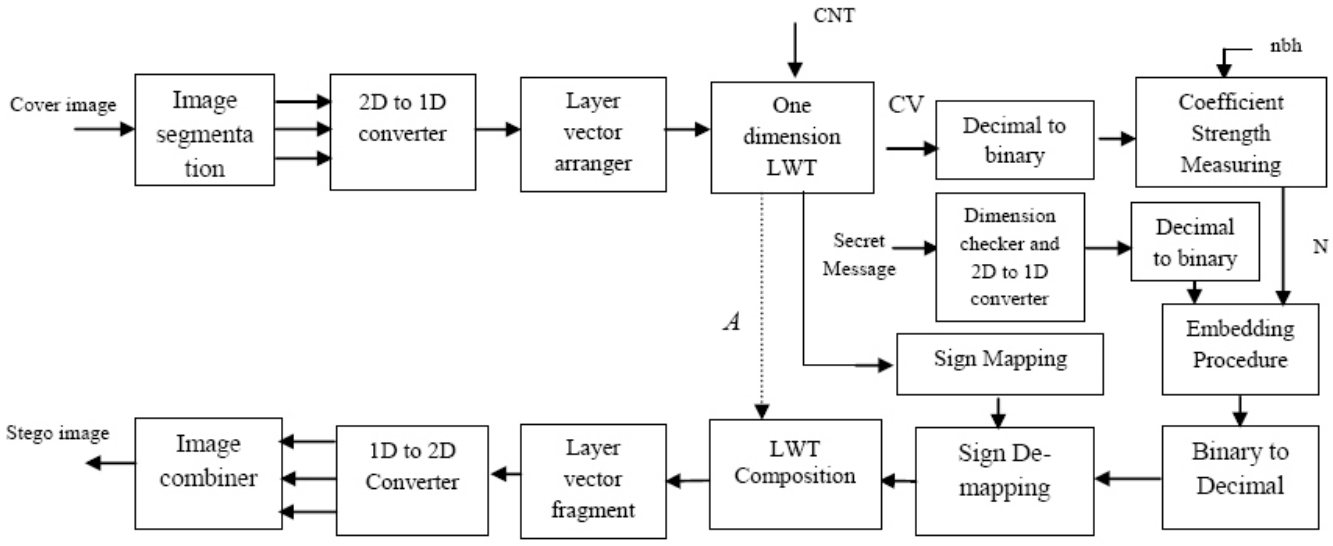

Figure. 1 Block diagram of the proposed hiding algorithm

According to control action applied (CNT as shown in Figure 1) which is considered as a key, the embedding procedure is conducted either merely in detail band or in the combined smooth and detail bands, therefore; the output of operation (CV) is:

$$\text{If CNT} = 1 \text{ then } CV = [d]$$

$$\text{Else } CV = [d] \cup [A]$$

Where: CV is the output vector in the LWT domain.

d: are the LWT detail coefficients.

A: are the LWT smooth coefficients.

It is observed in the else condition that CV embeds in the detail band before the smooth since the detail contains the high frequency contents that have less information than low frequency contents. Subsequently, the embedded data is being less effect on the stego image quality than if it is embedded in low frequency band. .

Sign Map: LWT vector output will possess positive and negative sign coefficients which ought to be saved in a one dimension matrix. The sign map will utilized later to re-possess each coefficient its sign before LWT reconstruction. The sign-less CV vector is converted to the binary system whereas each coefficient is converted to its eight bit binary value system.

Coefficient Strength Measurement: The strength of coefficient can be obtained according to inequality Eq. (1). Where, p in Eq. (1) represents the highest order bit in the coefficient, which contains binary bits. The value of number bit hold to hide data (nbh) for blue vector is entered by the user of the algorithm. The other nbh values for red and green vector are computed automatically by multiplying the entered value by two to control on the stego-image quality and embedding rate. Basically, increasing the value of nbh increases the image quality and decreases the embedding rate and vise-versa. The embedding rate or number of embedding bits (n) of each coefficient is given by Eq. (2). According to Eq. (2), some of coefficients have n values equal to zeros or negatives. These coefficients are not used for data embedding in our proposed algorithm to maintain the stego image quality.

Embedding Procedure: As shown in the block diagram of Figure 1, secret image is converted into a one dimension vector, and then into a binary stream. The bits of binary stream are embedded sequentially in the LSBs of CV coefficients that have positive n values. The number of the used LSBs in data embedding for each coefficient equals to its positive n value.

Again, utilizing this kind of technique gains the algorithm adaptive data embedding to lift security level by random embedding and decrease errors that are resulted from substitution, while the conventional least significant bit algorithm embeds the secret data directly regardless the measurement of the strength of cover code word. Subsequently, two critical drawbacks are resulted, the detecting of the embedded data is very simple to an attacker and qualities of stego pixels that have low strength are affected. An example illustrates a comparison between conventional LSB and the proposed algorithms:

Assume a cover pixels are [88, 0, and 32] and message is [127]. So we have:

Cover pixel codes = [01011000, 00000000, 00100000], Message stream= [1111111]

Firstly, we will embed data by using Conventional LSBs substitution; we need insert 3 bits/pixel for the first two pixels and one bit/pixel for the last one. Therefore, the stego pixels as follows:

Stego pixels = $[01011111, 00000111, 00100001]_2$ or stego pixels = $[95, 7, 33]_{10}$.

The mean square error (MSE) in stego pixel after data embedding can be calculated according to Eq. (6) 27 as follows:

$$\text{MSE} = \frac{1}{\text{N}} \sum_{\text{i}=1}^{\text{N}} (\hat{\text{S}} - \text{S})^2 \quad (6)$$

Where, and S are the stego and cover pixels. N is the total number of pixels. Essentially, the image quality is inverse proportional to the value of MSE. So, for above example, $\text{MSE} = 1/3\ [(95-88)^2 + (7-0)^2 + (33-32)^2] = 33$.

Also, we can evaluate the quality of the stego pixels by using peak signal to noise ratio (PSNR) assessment in decibel (dB) as shown in Eq. (7) 27, 28, 29.The image quality increases with incising of the value of PSNR.

$$\textbf{PSNR} = \mathbf{10} \log_{\mathbf{10}} \left(\frac{\mathbf{255}}{\mathbf{MSE}} \right)^{\mathbf{2}} \quad (7)$$

For the above example PSNR = 17.7605 dB

Now, let us use the proposed embedding techniques:

Assume nbh = 2, then pi = [7, 0, 6], and ni = pi – nbh = [5, -2, 4]. So, based on ni values, the second pixel does not utilized for embedding data, while we can embed 5 and 4 bits in first and last pixels respectively. Because of the message data is only 7 bits, our technique will insert 5

bits in the first pixel and twos bits in the third one. So the stego pixels are as shown below:

Stego pixels = $[01011111, 00000000, 00100011]_2$ or stego pixels = $[95, 0, 33]_{10}$.

According to Eq.s (6 and 7), MSE = 19.3333 and PSNR = 22.4047 dB. This is mean the proposed embedding technique have quality better than the conventional LSB by about three times for the above example. However, this is not the only enhancing for the stego image quality in the proposed algorithm. The other important part is the enhancing that is provided by the LWT decomposition that is explained in the former subsection.

Sign Remapping: After converting the one dimension vector to decimal values, the signs of the stego coefficients are retained to their values. According to its position, each value has its original sign.

LWT Decomposition: Depending on the CNT value, the signed stego coefficients that are resulted from merely detail or detail and smooth after embedding data. If the embedding was merely detail embedding then smooth coefficients will be directly input to the LWT composition. The signed values of the stego coefficients are then composed back to the one dimension spatial domain with the precise dimensions of the original cover.

Vector and Image Combiner: The resulted vectors from the LWT-decomposition represent three color planes. The vectors are converted into individually two dimension planes and collected back to a three dimension color plane which is known as "stego image" which conceals the secret data.

3. Recovery of Secret Messages

Mainly it is the inverse operation which is in Figure 1. In order to retrieve the secret image, the same stego keys (nbh and CNT) are required. Figure 2 shows the block diagram of the recovery algorithm.

Most of the blocks are previously explained in section (2). As shown in Figure 2, stego image, secret keys (nbh and CNT) ought to be input to the algorithm. Depending on the CNT, smooth band would skip to LWT composition or it may be included to the recovery procedure.

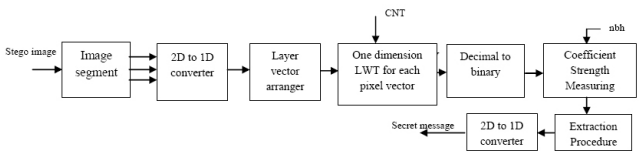

Figure 2. Block diagram of the proposed image recovery

The coefficient strength measuring block will designate the first one bit, with the existence of the key nbh, n is determined according to Equation (2). Then, the stream bits of the secret message are extracted from each positive coefficient according its n value. Subsequently, the resulted bit stream is converted to decimal and the produced vector is converted to its original secret data (eg. image and text). In the proposed method, an exact secret image is attained from the recovery algorithm without any lose in the information.

4. Results and Discussions

This section presents some experimental results of the proposed and related approaches. We choose two related approaches to compare with the proposed embossing approach. The first is the conventional LSB, which embeds secret data in the LSBs of the image pixels starting from first least significant bit such as in15. The second related approach embeds data in the LSB-coefficients of the convolution based DWT such as in25.

In order to compare the proposed and selected related approaches, all methods are implemented by Matlab programming. The main goal of steganography for applications of covert communications is to verify high embedding rate without causing any noticeable difference compare to cover image before embedding process. Moreover, in the receiver or message recovery side, the vital issue is the errors in the retrieved messages. Therefore, we are listed in the following subsections the two most important tests by measuring the quality of the stego image versus embedding capacity and robustness against distortion.

Admittedly, PSNR is the most popular formula to indicate quality of stego images. Equation (7) gives the formula of the PSNR. Besides PSNR, the corresponding embedding rate should be computed. Basically, an embedding rate is computed by dividing the number of embedding bits to the number of cover image bits and multiplying by 100 to get in percentage (%).

Correspondingly, robustness against distortion is computed by finding a Bit Error Rate (BER) of the retrieved secret messages. The BER is easily computed comparing retrieved and original message bits, then, the number of error bits is counted and divided over the entire number of the message bits, and finally, the result is multiplied by 100%. The BER can indicate accurately the distortion in the secret message either causing by embedding algorithm, i.e. lossy stego methods, or causing by transfer channel and data compression.

The experimental results of the proposed and the two related approaches are explained in the following subsections.

4.1 Stego Image Quality Versus Embedding Rate

In this section, the quality of the stego image, in terms of PSNR using Eq.(6), is assessed with various embedding ratio's. In order to test the superiority of our proposed method, results are compared with the conventional LSB method and convolutional DWT method. Two cover images, children and nature, with dimensions of 275*183and 259*174 respectively, are used in the experiments as shown in Tables 1 and 2. From the tables, it is clearly at low embedding rates in range of (5-10)%, the PSNR for the conventional LSB method is higher than both convolution based DWT and the proposed methods. However, all methods satisfy excellent stego image quality in terms of PSNR where PSNR greater

Table 1. Stego image quality versus embedding rate for children cover image

Embedding Ratio	Stego image and its quality in terms of PSNR					
	Conventional LSB method		Convolution based DWT method		The proposed method	
	PSNR	Stego image	PSNR	Stego image	PSNR	Stego image
5%	59.67		49.07		51.52	
10%	47,66		44,68		46,39	
15%	41.63		39.32		42.61	
20%	33.71		34.57		35.71	
25%	29.28		29.74		30.92	
30%	22.21		25.49		27.82	
35%	17.03		21.80		22.15	

Table 2. Stego image quality versus embedding rate for nature cover image

Embedding Ratio	Stego image and its quality in terms of PSNR					
	Conventional LSB method		Convolution based DWT method		The proposed method	
	PSNR	Stego image	PSNR	Stego image	PSNR	Stego image
5%	53.37		48.86		50.15	
10%	44,18		44,09		45,19	
15%	39.58		39.92		41.01	
20%	31.16		32.38		35.44	
25%	25.68		26.97		28.44	
30%	20.92		22.81		24.17	
35%	15.53		19.99		20.05	

than 40 dB. Also, the tables show that at high embedding rates, the PSNR in the conventional LSB and DWT methods compared to the proposed method decrease with an average drop of approximately 7dB per 5% increase in embedding ratio. In conventional LSB method visual errors accumulate in each cover pixel during embedding since LSB procedure embeds secret bits regardless of the strength of the cover bit stream. As for the convolution DWT method the rounding of detail cover coefficients before embedding produced visual error in addition to the embedding. Since the proposed method utilizes LWT and embeds the secret data after measuring the strength of detail cover coefficient, the PSNR is increased with an average of 5dB per 5% increase in embedding ratio, therefore; the proposed method shows better performance than other methods.

4.2 Robustness against Distortion

This section presents some test results of the robustness of the proposed hiding approach against distortion. Generally, there are two types of distortion; the first distortion occurs because of the information lose in the stego algorithm, while the second one occurs at the

Table 3. Shows the BER for various embedding ratio's

Embedding Ratio	BER of the extracted secret messages Vs. Channel Gaussian's Noise (CGN) in terms of CSNR								
	Conventional LSB method			Convolution based DWT method			The proposed method		
	CSNR= 150 dB	CSNR = 50 dB	CSNR = 20 dB	CSNR = 150 dB	CSNR = 50 dB	CSNR =20 dB	CSNR = 150 dB	CSNR = 50 dB	CSNR = 20 dB
5%	1.1 %	15.45 %	43.23 %	5.72 %	22.46 %	42.34 %	0 %	0.57 %	4.23 %
10%	1.7 %	18.56 %	47.15 %	9.79%	27.93 %	44.86 %	0 %	0.77 %	5.38 %
15%	2.3 %	19.91 %	48.33 %	13.43%	32.41 %	51.37 %	0 %	1.49 %	5.06 %
20%	3.48 %	19.23 %	45.82 %	16.89 %	35.16 %	53.65 %	0 %	1.84 %	5.64 %
25%	3.89 %	18.87 %	43.67 %	19.46 %	36.66 %	52.54 %	0 %	1.62 %	4.94 %
30%	4.12 %	18.13 %	42.35 %	21.32%	39.58 %	49.23 %	0 %	1.36 %	4.81 %

channel because noise or malicious attacking to the stego image such as low pass filtering and compression.

In order to test the robustness of the proposed approach against distortion, the stego images of the proposed and the two related methods are subjected to simulated Gaussian noise in terms of channel signal to noise ratio (CSNR). This is achieved by adding white Gaussian noise to the stego images, and then the noisy images are considered the received stego images in the recovery system. The recovery system retrieves the secret hiding messages and then compares the retrieved messages with the original secret messages. Based on the comparison BER of the extracted secret message is computed, where smaller BER means less error.

The table shows that the proposed method has no errors because embedding process. Furthermore, the proposed algorithm has higher immunity against noise than the other two related method. This makes our approach suitable for applications that need robust stego system against noise.

5. Conclusions

A new embedding technique for covert communication has been proposed. The technique embeds data adaptively in a color image by employing HVS sensitivity for the modification in stego images. on the technique take in consideration the strength of the cover coefficient and the human eyes sensitivity to the red, green, and blue colors, where insert bigger number of bits in the blue coefficients than green and red coefficients which have the same strength. Moreover, the proposed technique employs LWT to split frequency bands of the noticeable and unnoticeable frequencies. The utilized LWT discards the errors because rounding process that is happened in convolution based DWT. Also, it accelerates the algorithm processing. Utilizing LWT produces PSNR above 30 dB for embedding rate greater than 20% of the cover image size. The proposed method has low complexity and it is considered as a lossless steganography algorithm since exact secret data can be extracted. Furthermore, it embeds data randomly in terms of position and amount. Therefore; the proposed method is more secure than methods which insert data in known positions to the attackers. Moreover, the simplicity of technique and its ability to process any small size of bit stream makes it appropriate to be implemented as a hardware chip. This hardware can be combined with covert imaging systems, which is very useful in applications such as secret video conference and military communications.

6. References

1. Swain GS, Saroj(MITS) L. A novel approach to rgb channel based image steganography technique. International Arab J e-Techhnology. 2012; 2(4):181–6.
2. Jambhekar ND, Dhawale CA. Bit level key agreement and exchange protocol for digital image steganography. Indian Journal of Science Technology. 2015; 8(July):1–7.
3. Sheshasaayee A, Sumathy D. Text steganography in sms using similarity of glyphs in unicode characters. Indian Journal of Science Technology. 2015; 8(29).
4. Chanu YJ, Tuithung T, Manglem Singh K. A short survey on image steganography and steganalysis techniques. In: 3rd National Conference on Emerging Trends and Applications in Computer Science [Internet]. Shillong, India: IEEE; 2012 [cited 2016 Jan 16]. p. 52–5. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6203297

5. Ramalingam M, Ashidi N, Isa M. A Steganography Approach over Video Images to Improve Security. Indian Journal of Science Technology. 2015; 8(January):79–86.
6. Moon SK, Raut RD. Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security. In: Proceeding of the 2013 Seconnd International Conference on Image Processing [Internet]. Shimla, India: IEEE; 2013. p. 660–5. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6707677&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6707677
7. Kumar N, Kalpana V. A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. Indian Journal of Science Technology. 2015; 8(July):1–10.
8. Lin E, Delp E. A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99), April 25-28, 1999, Savannah, Georgia, p. 274-278. In: Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99). p. 274–8.
9. Bilal I, Kumar R. Audio Steganography using QR Decomposition and Fast Fourier Transform. Indian Journal Science of Technology. 2015;8(December).
10. Mishra M, Tiwari G, Yadav AK. Secret Communication using Public key Steganography. In: IEEE International Conference on Recent Advances and Innovations in Engineering(ICRAIE) [Internet]. Jaipur, India: IEEE; 2014. p. 9–11. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6724212&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6724212
11. Shahadi HI, Jidin R, Way WH. Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key. Indian Journal Science of Technology. 2014; 7(March):323–34.
12. Ramalingam M, Ashidi N, Isa M. Video steganography based on integer haar wavelet transforms for secured data transfer. Indian Journal Science of Technology. 2014; 7(July):897–904.
13. Yadav P, Mishra N, Sharma S. A secure video steganography with encryption based on lsb technique. In: International Conference on Computational Intelligence and Computing Research. Enathi, India; 2013. p. 1–5.
14. Kumar R, Chand S. A New Image Steganography Technique Based on Similarity in Secret Message. In: Confluence 2013: The Next Generation Information Technology Summit (4th International Conference) [Internet]. Noida, India: Institution of Engineering and Technology; [cited 2016 Jan 23]. p. 376–9. Available from: http://digital-library.theiet.org/content/conferences/10.1049/cp.2013.2344
15. Masud Karim SM, Rahman MS, Hossain MI. A new approach for LSB based image steganography using secret key. In: 14th International Conference on Computer and Information Technology (ICCIT 2011) [Internet]. Dhaka, Bangladesh: IEEE; 2011 [cited 2016 Jan 22]. p. 286–91. Available from: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6164800
16. Das R, Tuithung T. A novel steganography method for image based on Huffman Encoding. In: Proceedings - 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, NCETACS-2012 [Internet]. Shillong, \india: IEEE; 2012. p. 14–8. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6203290&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6203290
17. Akhtar N, Johri P, Khan S. enhancing the security and quality of lsb based image steganography. In: 2013 5th International Conference on Computational Intelligence and Communication Networks [Internet]. Mathura, India: IEEE; 2013. p. 385–90. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6658020
18. Liu J, Zhou K, Tian H. Least-significant-digit steganography in low bitrate speech. In: 2012 IEEE International Conference on Communications (ICC) [Internet]. Ottawa, Canada: IEEE; 2012 [cited 2016 Jan 16]. p. 1133–7. Available from: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6363997
19. Weiqi Luo, Fangjun Huang, Jiwu Huang. Edge Adaptive Image Steganography Based on LSB Matching Revisited. IEEE Trans Inf Forensics Secur [Internet]. 2010 Jun [cited 2016 Jan 16];5(2):201–14. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5411758
20. Prabakaran G, Bhavani R. A modified secure digital image steganography based on Discrete Wavelet Transform. In: Computing, Electronics and Electrical Technologies [ICCEET] [Internet]. Kumaracoil, India: IEEE; 2012. p. 1096–100. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6203811
21. Kundur D, Hatzinakos D. Digital watermarking using multiresolution wavelet decomposition. In: Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '98 (Cat No98CH36181) [Internet]. Seattle, USA: IEEE; 1998 [cited 2016 Jan 16]. p. 2969–72. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=678149
22. Junejo N, Ahmed N, Unar MA, Rajput AQK. Speech and image compression using discrete wavelet transform. In: IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication [Internet]. Princeton, USA: IEEE; 2005 [cited 2016 Jan 16]. p. 45–8. Available from: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=1426508
23. Farahani MRD, Pourmohammad A. A DWT Based Perfect Secure and High Capacity Image Steganography Method. In: International Conference on Parallel and Distributed

Computing, Applications and Technologies [Internet]. Taipei, Taiwan: Taiwan; 2013. p. 314–7. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6904273

24. Kumar V, Kumar D. Performance evaluation of DWT based image steganography. In: IEEE 2nd International Advance Computing Conference (IACC) [Internet]. Patiala, India: IEEE; 2010 [cited 2016 Jan 22]. p. 223–8. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5423005
25. Al-ataby A, Al-naima F. A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. Int Arab J Inf Technol. 2010; 7(4):358–64.
26. Sweldens W. The lifting scheme: a custom-design construction of biorthogonal wavelets. appl comput harmon anal [internet]. 1996 Apr; 3(2):186–200. Available from: dx.doi.org/10.1006/acha.1996.0015
27. Wang Z, Li Q. Information content weighting for perceptual image quality assessment. IEEE Trans Image Process. 2011; 20(5):1185–98.
28. Vidya G, Preetha RH, Shilpa GS, Kalpana V. Image steganography using ken ken puzzle for secure data hiding. in. 2014; 7(September):1403–13.
29. Swain G. Digital image steganography using nine-pixel differencing and modified lsb substitution. Indian Journal Science of Technology. 2014; 7(September):1444–50.