Steganography using dual tree complex wavelet transform with LSB indicator technique

Namar A Taha[1], Zainab Qasim[1], Amna Al-Saffar[1], and Alaa A. Abdullatif[1]
[1]University of Baghdad, College of Education for Pure Science-Ibn Al-Haitham, Computer Science Department

ABSTRACT

Image steganography is undoubtedly significant in the branch of multimedia communication security. The undetectability and large payload capacity are two of the important characteristics of any form of steganography.
In this paper, the level of image security is improved by combining the steganography and cryptography techniques in order to produce the secured image. The proposed method depends on using LSBs as an indicator for hiding encrypted bits in dual tree complex wavelet coefficient DT-CWT. The cover image is split into non-overlapping blocks of size (3*3). After that, a Key is produced by extracting the center pixel (pc) from each block to encrypt each character in the secret text. The cover image is converted using DT-CWT, then the produced key is used to determine the starting pixel in each block for hiding and the direction of hiding (clockwise or anticlockwise).

The proposed method is applied on many images with different embedding rate, and many metrics are used to evaluate the performance of the proposed method, namely: Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), correlation factor (CF) and Structural Similarity Index Measure (SSIM). It achieves in average 52.225 dB of PSNR, 0.3215 of MSE, 0.9952 of SSIM and 0.9997 of CF with embedding rate 1.5.

Keywords: Cryptography, Steganography, Dual Tree complex wavelet and Least Significant Bit indicator

Corresponding Author:

Namar A. Taha,
Departement of computer science, College of Education for Pure Sciences,
University of Baghdad, Iraq
E-mail: namar.t@ihcoedu.uobaghdad.edu.iq

1. Introduction

In multimedia communication, Steganography and encryption become more important. It is beneficial to join hiding and encryption in a united process to improve both the performance and the security of multimedia application [1, 2].
Two of the major specialties of information security systems are Cryptography and information hiding which provide secure communication. Hiding the existence of the message and making it imperceptible is Information hiding, while mixing up the message into an unreadable form is cryptography techniques. Watermarking and steganography are the sub-major classification of information hiding. Digital contents commonly use watermarking for copyright protection [3, 4].
In steganography, the secret communication between two parties must be achieved by studying the techniques of hiding the contents of a secret message as well as the process of communicating it. To achieve this goal, steganography algorithms or "stego algorithms" use one of many different natural cover data types, then embed the secret information or the secret message into it to result in stego-data that is virtually identical to its natural cover.
On the other side, stego-analysis involves analyzing (possibly modified) cover data to determine the presence of an embedded message in it. Therefore, the problem can be seen classified into natural and stego-data class [5, 6].
In steganography, the cover media hidden can be in (image, text, video or audio) file form. Because of their high capacity and their easy availability over the internet, and owing to the insensitivity of the visual system in humans, digital images are more preferred than steganography [7].

Depending on the type of the embedding process, steganographic techniques are classified into two categories; spatial and transform domains. The spatial domain technique essentially involves hiding the information bits directly on the cover image pixel. Whereas the transform domain method involves employing a suitable image transformation which allows the embedding of more bits without changing the pixel values of the spatial domain stego-image.

Several transform domain methods may be used; (DCT) discrete cosine transform, (DWT) the discrete Wavelet Transform, (DTCWT) dual-tree complex wavelet transform, and the Discrete Fourier Transform (DFT) are some of the most widely used transforms [8, 9]

One of the tools for data hiding is (DWT) discrete wavelet transform which is considered to be an important technique. Lossless embedding applications, which include military, legal and medical imaging domains, as well as advance research on network transmission security, require high capacity.

Discrete wavelet transform (DWT) for diagonal features and shift invariance lacks directional selectivity. The dual tree complex wavelet transform (DT-CWT) provides shift invariance in addition to great directional selectivity, but has a modest amount of redundancy [10].

The (DTCWT) dual-tree complex wavelet transform, which is a modification of the original DWT version of the traditional (DWT), is aimed towards boosting the directional selectivity that is impaired in (DWT). (CWT) Complex Wavelet Transform is the complex adaptation of the Discrete Wavelet Transform (DWT). (DTCWT) dual tree complex wavelet transform is a two-tree structure in contrast to the single-tree structure of the (DWT) [11].

One of the very old image steganography methods is least significant bit (LSB) substitution, where secret data bits are used in place of LSB bits of the pixels (one, two, three, or four). This straightforward technique can be detected by RS analysis [12].

The proposed algorithm changes LSBs as an indicator for hiding secret bits instead of inserting them directly, making the method more robust against steganalysis. This is the advantage of this algorithm over traditional LSB algorithm.

This paper proposing the rest of research is ordered as follow; Section 2 outlines the dual complex transform with its general equation. Section 3 describes the proposed algorithm with its block diagram and the corresponding simulations, and discussions are done in section 4. Finally, section 5 comprises the conclusion of the paper.

2. Dual-tree complex wavelet transform (DT-CWT)

The Dual-tree complex wavelet transform (DT-CWT) is essentially a complex-valued extended version of the standard discrete wavelet transform (DWT). In comparison to other alternative transforms like CWT and DWT, the primary advantage of DT-CWT transform is that there is a higher amount of sub band planes allowing more secret bits to be embedded onto it. Moreover, these sub bands display a greater degree of shift-invariance in their magnitude [13].

The DT- CWT utilizes two separate real DWTs which break down a signal into real and imaginary parts**.** one DWT produces the real component of the transform while the other DWT produces the imaginary component. Figures 1&2 are showing the Filter Banks for both decomposition and reconstruction that require the implementation of the DT- CWT and its inverse. Two separate sets of filters are used for two real wavelet transforms, with each fulfilling the Filter Banks requirements. These two different sets are designed conjointly in such a way that makes the overall transform approximately analytic.

For the upper filter banks, the low and high-pass/filter pair are represented by $h_0(n)$, $h_1(n)$

For the lower filter banks, the low and high-pass/filter pair are represented by $g_0(n)$, $g_1(n)$

The two real wavelets linked to each of the real wavelets' transform are denoted by $\psi_h(t)$ and $\psi_g(t)$. The filters which need to be designed have to conform to the Filter Banks conditions.

As a result, the complex wavelet as in equation 1 is approximately analytic [14][14]:

$$\psi\,(t) := \psi_h(t) + \psi_g(t) \qquad (1)$$

It should be noted that all the filters are real. Therefore, a complex arithmetic is not needed for implementing the DT-CWT. The inverse of the dual-tree CWT is simple in much the same way as the forward transform. To perform the inverse transform, the real part and the imaginary part should both be inverted. The real two signals are obtained from the inverted form of each of the two real DWTs. Finally, the final output is obtained from the average of these signals. It must be noted that the initial signal x(n) can be retrieved from the real part or the imaginary part alone [15, 16].

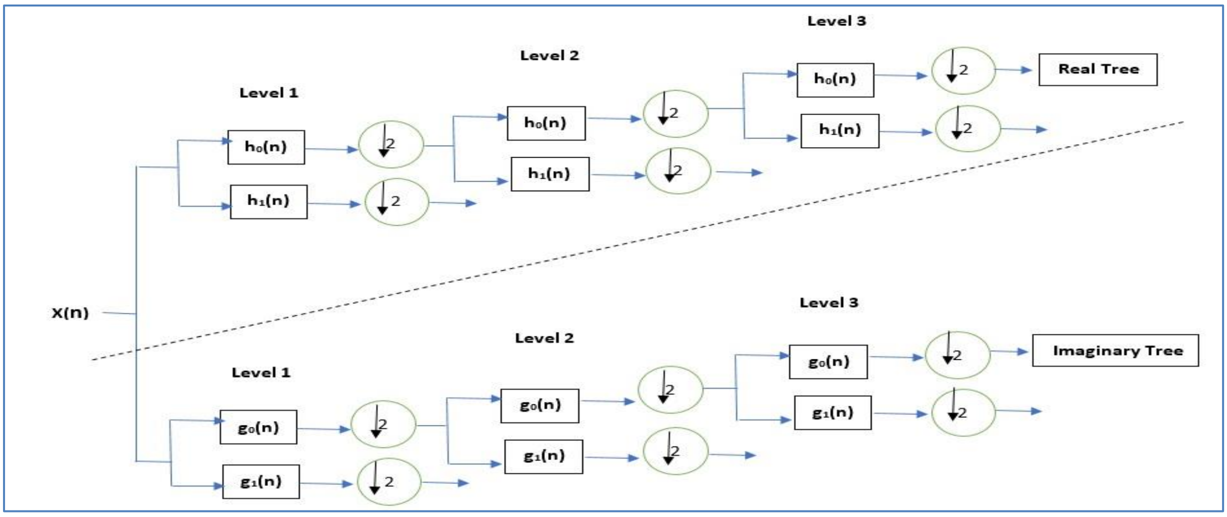


Figure 1. The decomposition process of dual-tree complex wavelet transforms (DTCWT)

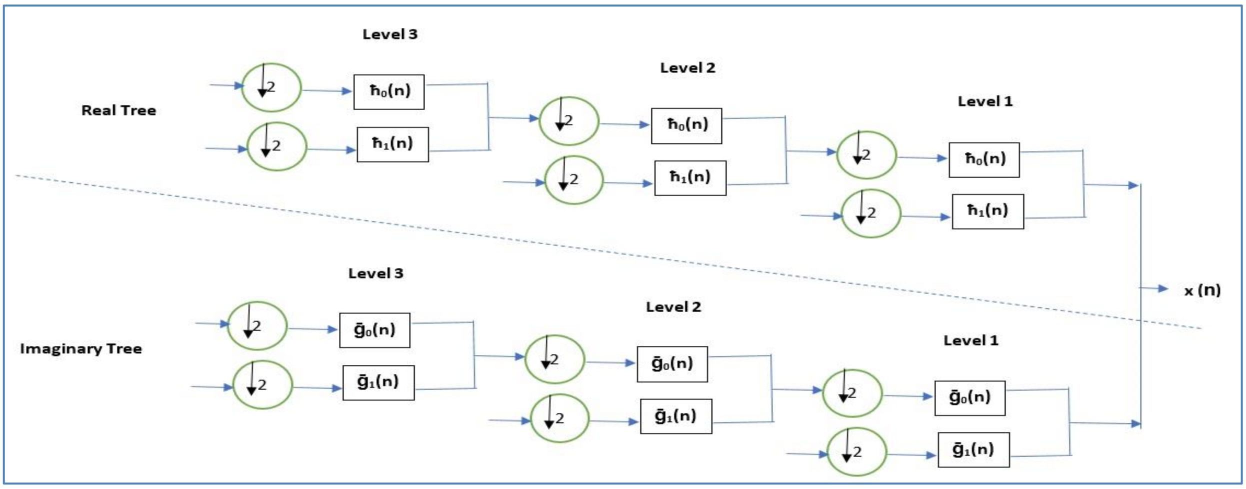


Figure 2. The reconstruction process of dual-tree complex wavelet transforms (DTCWT)

3. Proposed method

The proposed algorithm uses the coefficient of DT-CWT to hide encrypted bits by using the two LSBs as indicators, as illustrated in Figure 3

First, the color cover image is separated into three channels: red, green, and blue. Then, starting with blue, the channel is divided into non overlapping blocks with size 3*3. After that, the Key (K) is produced by extracting the center pixel, which is denoted by Pc, from each block. The secret text is converted into binary, and then each character is encrypted using the Key (K). The encryption process depends on changing the sequence of bits in each character. The starting bit in each character, and the direction of changing the sequence are determined by Str and (Dir) which are extracted from the key as shown in equation 2 and equation 3.

$$Str\ [i] = (K[i] \bmod 8) + 1 \quad (2)$$

$$Dir[i] = K[i] \bmod 2 \quad (3)$$

Where K is the center pixel in each block, i =1 to length

If Dir =0 the direction of encoding is to the right, else the encoding is to the left.

The cover image is transformed using DT-CWT, and then the coefficients are divided into blocks 3*3. The starting pixel in each block for hiding as well as the direction are also determined by Str and Dir (if Dir =0 the direction of hiding is anticlockwise else the direction is clockwise). For the hiding process, each two secret bits is compared with two MSBs, then the two LSBs are changed as indicator for secret bits.

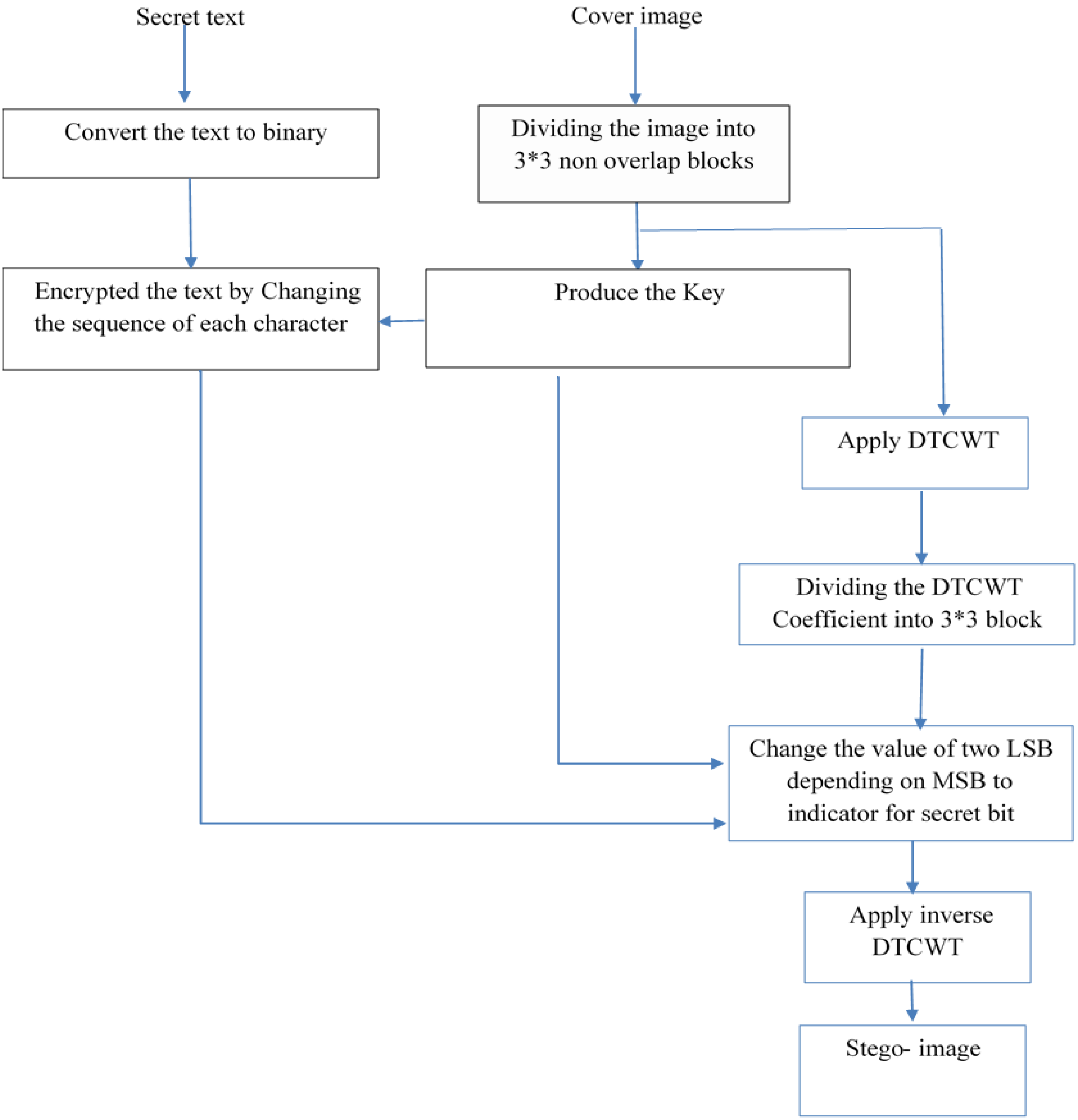

Secret text
Cover image
Convert the text to binary
Dividing the image into 3*3 non overlap blocks
Encrypted the text by Changing the sequence of each character
Produce the Key
Apply DTCWT
Dividing the DTCWT Coefficient into 3*3 block
Change the value of two LSB depending on MSB to indicator for secret bit
Apply inverse DTCWT
Stego- image

Figure 3. The block diagram of the proposed method

3.1. Embedding data algorithm

The following algorithm showed the steps of embedding process.
Input: color cover image, secret text.
Output: stego-image.
Begin
Step 1: divide the color image into three channels (R, G, B).
Step 2: divide each channel into non-overlapping blocks with size [3 x 3]. Staring with the blue channel.
Step3: produce the key (K) by extract the center pixel (pc) from each block.

Step 4: encrypting each character of the secret text by rearrange its bits using the value of (Str) for start bit and (Dir) for the direction which produce by eq. (2) and eq. (3) respectively.
Step 5: Apply dual tree complex wavelet transform to original cover image, and divide the coefficients into [3x3] blocks.

Step 6: determined the staring pixel in the block for hiding by using (Sta) and the direction of the hiding process by using (Dir).
Step 7: change the two LSB to be an indicator for the secret encrypted bits as follows:

```
     If the two secret bits are the inverse of two MSBs then
     -   LSBs= 00.

     Else if the two secret bits are the inverse of MSB and the same of the second then
       -   LSB=01
     Else if the two secret bits are the same of MSB and the inverse of the second then
       -   LSB=10
     Else
       -   LSB=11
End
```

Step 8: apply the invers of the dual tree complex wavelet transform.
Step 9: reconstruct the stego- image.

3.2. Extracting data algorithm

The following algorithm showed the steps of extracted process.
Input: stego-image
Output: secret text
Begin
Step 1: divide the stego-image into three channels (R, G, B).
Step 2: divide each channel into non-overlapping blocks with size [3 x 3]. Staring with the blue channel.
Step3: produce the key (K) by extract the center pixel (pc) from each block.
Step 5: Apply dual tree complex wavelet transform to stego- image, and divide the coefficients into [3x3] blocks.
Step 6: determined the staring pixel in the block for extracting by using (Str), and the direction of the extract process by (Dir) using eq. (2) and eq. (3) respectively.
Step 7: use the two LSB as indicator for extract the secret encrypted bits

```
If LSB= 00 then
     -   The two secret bits are the inverse of two MSBs
Else If LSB=01 then
     -   The two secret bits are the inverse of MSB and the same of the second
Else if LSB=10 then
     -   The two secret bits are the same of MSB and inverse of second
else
     -   The two secret bits are the same of two MSBs.
End {if}
```

Step 8: rearrange the bits in each extracted character to convert them to original sequence using Str and Dir.
Step 9: Convert the extracted bits into text.

The proposed method can be explained using the following numerical example

-Assume that the secret message is   M = {Hello ………
-divide each channel into non overlapping blocks with size [3*3] starting with the blue channel and block format is as follows:

P1	P2	P3
P4	Pc	P5
P6	P7	P8

Produce the Key by extract the center pixel Pc from each block
For example, K = [135 146   95 ………….]
-Calculate the Sta, Dir from each Pc in the Key by using eq (2) and eq (3)
Sta = [6   3   8 ……]
Dir = [1   0   1 …….]
-Convert the secret text to binary [01001000   01100101 01101100 …………]
-Encrypt the secret text by changing the sequence of bits using Str and Dir, for the first character

Char (1) = [0 1**0** 01 0 0 0]

When Str (1) = 6 and Dir (1) =1 start from bit 6 with the direction being to left
The char (1) encrypted as follows
Char¯(1) = [0 1 0 0 0 0 1 **0**]
-Convert the image into dual-tree complex wavelet transform suppose the first block after DT-CWT

Block =

130	122	140
75	97	90
155	140	145

-Start embedding from pixel 6 according to the value of Str, and the direction of embedding is clockwise (P6, P4, P1, P2, P3, P5, P8 and P7) according the value of Dir. Then, change two LSBs as indictor for secret encrypted bits.

4. Results and Discussion

For testing the functioning of the proposed method, many color images with the size (256 × 256) are used as cover such as (a) Barbara, (b) tulips, (c) airplane, (d) tree, and (e) Lena as shown in figure 4.

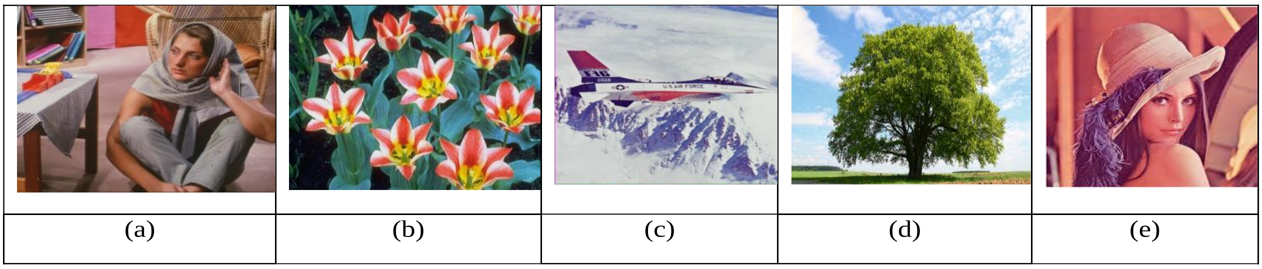


Figure 4. The cover images (a) Barbara, (b) tulips, (c) airplane, (d) tree, and (e) Lena

The proposed method is tested both, quantitively and qualitatively. The quantitative evaluation uses four different criteria, PSNR, SSIM, MSE, and CF, while the qualitatively evaluation is done using histogram changeability analysis. The experiment is tested with three different embedding rates (0.9, 1.2 ,1.5) as shown in table 1.

Table 1. The PSNR, MSE, SSIM and CF values for different cover images and different Embedding rates for the proposed method

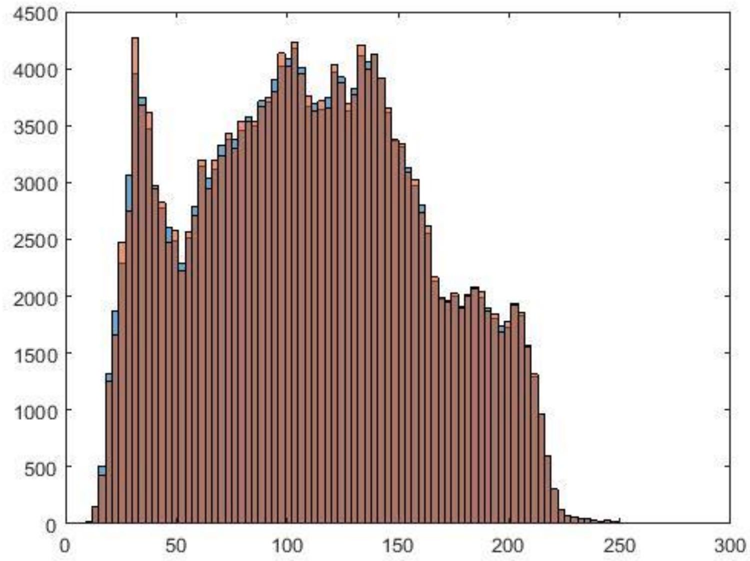
	er	PSNR	MSE	SSIM	CF
Barbara	0.9	53.3095	0.3034	0.9969	0.99986
	1.2	52.7447	0.3456	0.9963	0.99984
	1.5	52.1503	0.3963	0.9956	0.99981
tulips	0.9	53.5108	0.2897	0.9985	0.99991
	1.2	52.9668	0.3283	0.9983	0.99989
	1.5	52.4890	0.3665	0.9980	0.99988
airplane	0.9	53.4254	0.2954	0.9946	0.99968
	1.2	52.8154	0.3400	0.9937	0.99961
	1.5	52.2462	0.3876	0.9928	0.99954
tree	0.9	53.5509	0.2870	0.9959	0.99997
	1.2	52.9270	0.3314	0.9952	0.99996
	1.5	52.4267	0.3718	0.99462	0.99996
Lena	0.9	53.0564	0.3216	0.99587	0.99979
	1.2	52.4040	0.3738	0.99507	0.99974
	1.5	51.8142	0.42821	0.99426	0.99970

Figure 5 shows the images after hiding data (stego-images), while figure 6 shows the difference between the histograms of cover and stego- images. It can be clearly seen that the pixel contrast between cover and stego-images, and the amount of distortion are altered in an undetectable way.

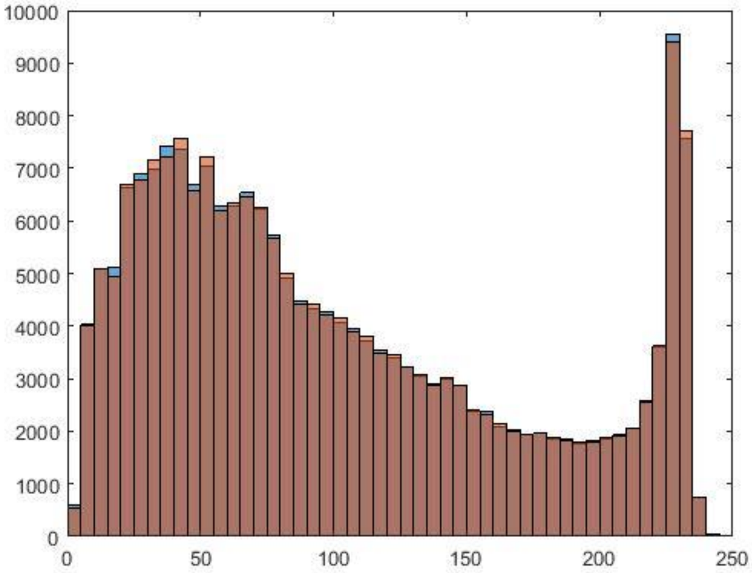
(a)	(b)	(c)	(d)	(e)

Figure 5. The stego- images (a) Barbara, (b) tulips, (c) airplane, (d) tree, and (e) Lena.

Barbara



tulips



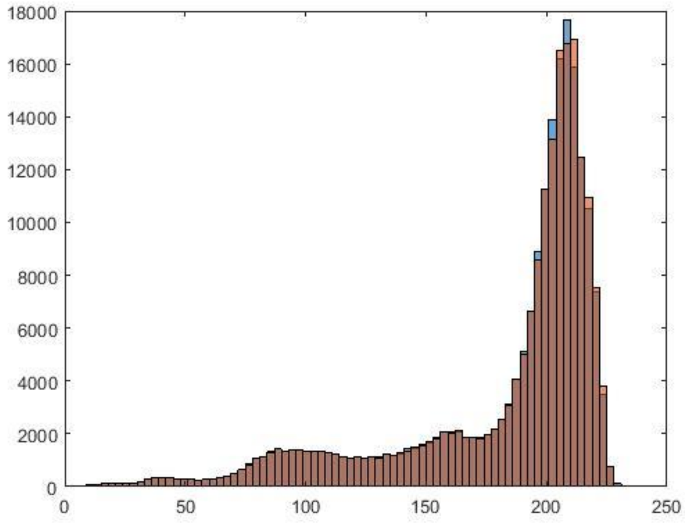
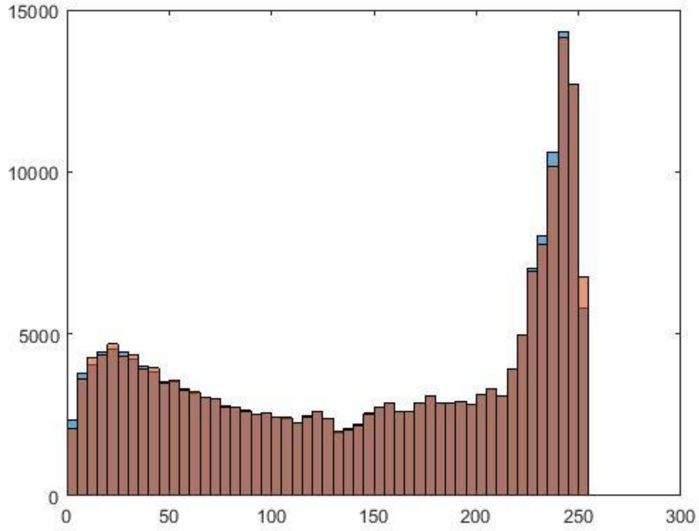
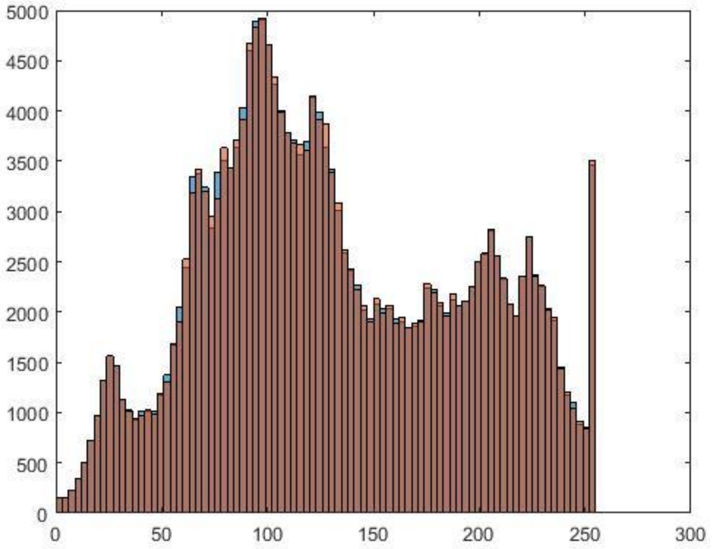
airplane	
Tree	
Lena	

Figure 6. The histogram of cover and stego- images

5. Conclusions

This paper put forward a high payload image steganography based upon DT-CWT that provides a greater number of sub-bands, and consequently more secret bits that can be embedded. In this paper, the standard LSB method for hiding is modified to make it more efficient and secure. This modification to the existing LSB method involves taking the last two bits of each pixel in the image and using them as an indicator for the hidden bits. This means that they are changed depending on the most significant bits. This method led to the increase in the payload capacity and security.

Also, the experimental results indicate that the performance is greatly improved in several aspects such as stego-image undetectability and retrieval accuracy.

The good PSNR and SSIM values provided by the proposed approach prove the robustness of this work. The value of SSIM of the secret images provides evidence that the data is successfully retrieved at the receiving end.

References

[1] F. A. Abdullatif, A. A. Abdullatif, and N. A. Taha, "Data hiding using integer lifting wavelet transform and DNA computing," *Periodicals of Engineering and Natural Sciences,* vol. 8, no. 1, pp. 58-66, 2020.

[2] J. Chen, J. Zhou, K.-W. Wong, and Z. Ji, "Enhanced cryptography by multiple chaotic dynamics," *Mathematical Problems in Engineering,* vol. 2011, 2011.

[3] A. A. Abdullatif, F. A. Abdullatif, and S. A. Naji, "An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques," *Periodicals of Engineering and Natural Sciences,* vol. 7, no. 4, pp. 1607-1617, 2019.

[4] R. Atta, M. Ghanbari, and L. F. IEEE, "A high payload data hiding scheme based on dual tree complex wavelet transform," *Optik,* vol. 226, p. 165786, 2021.

[5] S. Chakraborty and S. K. Bandyopadhyay, "A Steganography Approach to hiding two images using DNA microarray," *Int. J. Innov. Res. Comput. Commun. Eng,* vol. 1, no. 2, pp. 158-162, 2013.

[6] X. ShuangKui and J. Wu, "A Modification-Free Steganography Method Based on Image Information Entropy," *Security and Communication Networks,* vol. 2018, 2018.

[7] K. Joshi, S. Gill, and R. Yadav, "A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image," *Journal of Computer Networks and Communications,* vol. 2018, 2018.

[8] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cognitive Systems Research,* vol. 60, pp. 20-32, 2020.

[9] N. A. Taha, A. Al Saffar, A. A. Abdullatif, and F. A. Abdullatif, "Image Steganography using Dynamic Threshold based on Discrete Cosine Transform," in *Journal of Physics: Conference Series,* 2021, vol. 1879, no. 2: IOP Publishing, p. 022087.

[10] S. Kumar and S. Muttoo, "Image steganogaraphy based on complex double dual tree wavelet transform," *International Journal of Computer and Electrical Engineering,* vol. 5, no. 2, p. 147, 2013.

[11] J. Yadav and K. Sehra, "Large Scale Dual Tree Complex Wavelet Transform based robust features in PCA and SVD subspace for digital image watermarking," *Procedia computer science,* vol. 132, pp. 863-872, 2018.

[12] G. Swain, "High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis," *Security and communication networks,* vol. 2018, 2018.

[13] T. S. a. M. Krishnamurthy, "Performing Image Steganography Using Dual Tree Complex Wavelet Transform (Dtcwt) And Haar Wavelet," *International Journal of Advanced Information Science and Technology (IJAIST),* vol. 4, no. 5, pp. 34-47, 2015.

[14] I. W. Selesnick, R. G. Baraniuk, and N. C. Kingsbury, "The dual-tree complex wavelet transform," *IEEE signal processing magazine,* vol. 22, no. 6, pp. 123-151, 2005.

[15] H. H. Mahmoud and H. M. Ahmed, "Convolution Neural Network with Dual Tree Complex Wavelet Transform Preprocessor for Universal Image Steganalysis," *Journal of Al-Qadisiyah for computer science and mathematics,* vol. 11, no. 3, pp. Page 43-58, 2019.

[16] H. Vermaak, P. Nsengiyumva, and N. Luwes, "Using the dual-tree complex wavelet transform for improved fabric defect detection," *Journal of Sensors,* vol. 2016, 2016.