Image Segmentation to Secure LSB2 Data Steganography

Hatim Ghazi Zaini
Department of Computer Engineering
Taif University
Taif, Saudi Arabia
h.zaini@tu.edu.sa

Abstract-A digital color image usually has a high resolution, thus its size is good enough and the image can be used as a covering (holding) image to hide secrete messages (short and long). The methods commonly used for data steganography, e.g. LSB and LSB2 are not secure, so in this paper, a method of securing the LSB2 method is proposed. The proposed method is based on wavelet packet decomposition. The levels of decomposition will be kept in secret and one of the resulting segments will be used as a covering segment. MSE, PSNR, hiding time, and extraction time will be experimentally analyzed to prove that the proposed method is capable of handling the process of hiding secret messages, either sort or long.

Keywords-steganography; LSB2; MSE; PSNR; hiding time; extraction time; WPT; decomposition level; segment; security

I. Introduction

Data steganography [1-3] is the process of hiding secret data into covering data. The covering data must be large enough in order to be capable to hide the secret data [4-5]. Data steganography [6-7] must provide the following important features [8]:

- The changes in the holding data must not affect them while the concealment process result must not be visible to the naked eye [2].
- The Mean Square Error (MSE) [9] between the original covering data and the holding data must very small and close to zero.
- The Peak Signal-to-Noise Ratio (PSNR) [10-11] between the original covering data and the holding data must very big in order to keep the quality of the holding data high.
- The secret data hiding time must be minimal.
- The secret data extraction time must be minimal.
- The hiding method must be secure and the process of hacking must be very complicated.
- The method must be simple to implement.
- The method must be capable of hiding secret data of various sizes (short and long messages).

One of the most common types of data that can be used to hide confidential messages is digital color images for the following reasons [12-15]:

- The wide spread use of digital images.
- The sheer volume of covering data that a digital image provides [16, 17].
- The ease of digital image processing [18-19].
- The possibility of reshaping the image before the process of masking data.
- The possibility of using a section of the image to implement the concealment process [20].

II. Hiding Data Methods

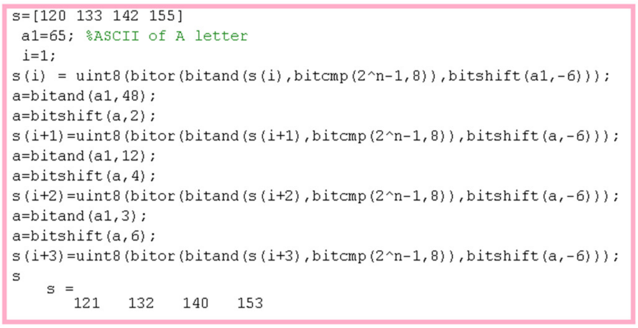
One of the most popular methods of data hiding is the Least Significant Bit (LSB) method which requires 8 bytes from the holding image to hide one character from the secret message. The LSB2 method is a modification of the LSB but it doubles the capacity of hiding by using 4 bytes from the covering image to hide one character from the secret message. The least two significant bits are used to hold data from the secret message as shown in Table I. The LSB2 adds minor changes to the covering image, ranging from +3 to -3. These changes in the pixel colors cannot be noticed by the human eye. The process of data hiding and data extracting using the LSB2 method is very simple, Figure 1 shows the process of hiding, while Figure 2 shows the process of data extracting.

TABLE I. HIDING A=65 D=01000001B

Covering bytes	120	133	142	155
Binary	01111000	10000101	10001110	10011011
Holding byte (binary)	011110**01**	100001**00**	100011**00**	100110**01**
Holding bytes	121	132	140	153

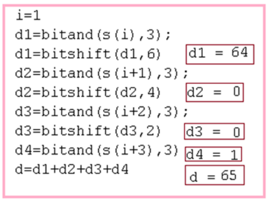
The LSB2 method adds minor changes to the covering image. These changes cannot be noticed by the human eyes, thus this method keeps the holding image very close to the covering one, and minimizes MSE and maximizes PSNR between the covering and the holding images. As we can see in Figures 3 and 4, the histograms of the two images are very close to other.

Corresponding author: Hatim Ghazi Zaini



```
s=[120 133 142 155]
 a1=65; %ASCII of A letter
 i=1;
s(i) = uint8(bitor(bitand(s(i),bitcmp(2^n-1,8)),bitshift(a1,-6)));
a=bitand(a1,48);
a=bitshift(a,2);
s(i+1)=uint8(bitor(bitand(s(i+1),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,12);
a=bitshift(a,4);
s(i+2)=uint8(bitor(bitand(s(i+2),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,3);
a=bitshift(a,6);
s(i+3)=uint8(bitor(bitand(s(i+3),bitcmp(2^n-1,8)),bitshift(a,-6)));
s
    s =
       121    132    140    153
```

Fig. 1. The data hiding process.



```
i=1
d1=bitand(s(i),3);
d1=bitshift(d1,6)       d1 = 64
d2=bitand(s(i+1),3);
d2=bitshift(d2,4)       d2 = 0
d3=bitand(s(i+2),3);
d3=bitshift(d3,2)       d3 = 0
d4=bitand(s(i+3),3)     d4 = 1
d=d1+d2+d3+d4           d = 65
```

Fig. 2. The data extraction process

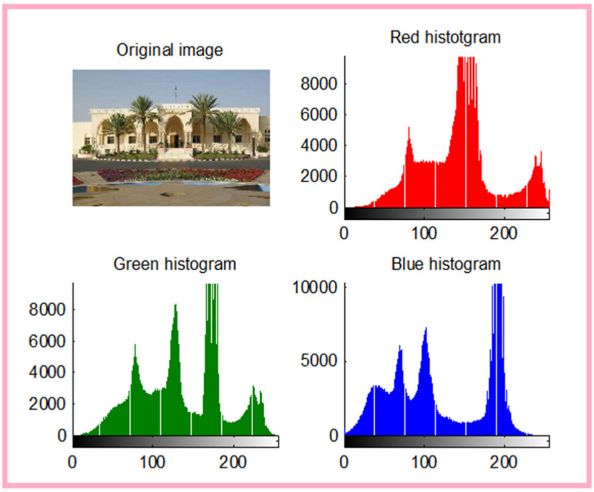


Fig. 3. Covering image.

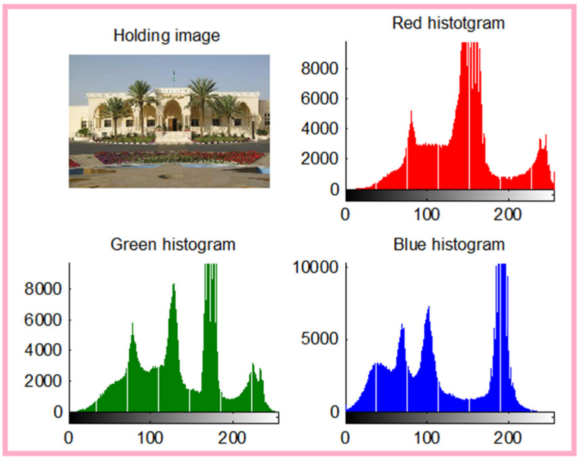


Fig. 4. The same image holding a 50 byte character message.

III. AIM OF THE STUDY

LSB2 is a method of secret data is an easy-to-implement and quick-to-perform way, but one of its main flaws is its lack of security in the data-stripping device, due to its ease of penetration from non-authorized parties. Accordingly, the aim of this research is to update this method by strengthening it with the required protection operations and thus to prevent intruders from the possibility of obtaining or knowing the secret messages included in the digital image, provided that the advantages of the concealment method are preserved and without negatively affecting the efficiency of the method.

IV. RESEARCH METHOD

The hiding process is going to be implemented in four phases. The information in the first two phases must be kept confidential in order to secure the data.

- Color image rearrangement. The color channels are rearranged, then the color image 3D matrix is reshaped into a one row matrix. The reshaping can be done either row-wise or column-wise.
- Row matrix decomposition. The principles of wavelet packet tree decomposition [21, 22] are used to decompose the image row matrix. In this phase, we have to select the number of levels needed to divide the image into segments, and then we have to select the segment [23] where we must hide the secret massage (Figure 5).
- The LSB2 method of data hiding is applied.
- The holding image is rearranged back.

The extraction process will be implemented in 3 phases.

- Image rearrangement: Here we have to use the information used in the hiding process.
- After we get the number of decomposition levels and the segment number, image decomposition is applied.
- The LSB2 method to extract the message from the selected segment is applied.

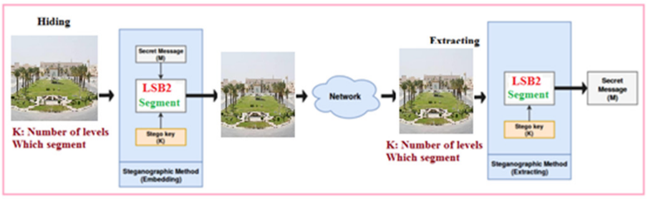


Fig. 5. The diagram of the proposed method.

V. RESULTS AND DISCUSSION

Twelve images were processed, and each of them was rearranged by replacing the color channels from red, green, and blue to blue, red, and green. Each image matrix was reshaped from 3D form to 1D column-wise. The number of the selected decomposition levels was defined as 7, and segment 6 was selected for message hiding. Figure 6 shows the segments of one image.

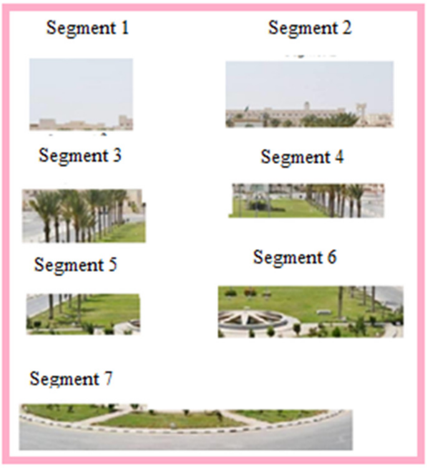


Fig. 6. Image (with small size) 1 segments.

TABLE II. SEGMENT SIZES

Image#	Segment size(byte)						
	S1	S2	S3	S4	S5	S6	S7
1	2358	2358	4715	9429	18857	37713	75425
2	1219	1219	2437	4874	9747	19494	38988
3	8100	8100	16200	32400	64800	129600	259200
4	80325	80325	160650	321300	642600	1285200	2570400
5	67598	67598	135195	270389	540777	1081553	2163105
6	1911	1911	3821	7642	15284	30567	61133
7	8100	8100	16200	32400	64800	129600	259200
8	2359	2359	4718	9436	18872	37744	75488
9	2359	2359	4718	9436	18872	37744	75488
10	2365	2365	4730	9460	18920	37839	75677
11	29532	29532	59063	118125	236250	472500	945000
12	95614	95614	191227	382454	764907	1529814	3059628

TABLE III. SEGMENT LOCATIONS

Image #	Segment 6 size (byte)	Starting row	Starting column	# of colors
1	37713	113	37	3
2	19494	1	38	3
3	129600	1	90	3
4	1285200	803	267	3
5	1081553	245	245	3
6	30567	41	41	3
7	129600	1	90	3
8	37744	137	45	3
9	37744	137	45	3
10	37839	50	50	3
11	472500	1	150	3
12	1529814	1	286	3

The obtained segments for each image are of different sizes and locations and when the decomposition level changes the segments, their sizes, and their locations also changed. Tables II and III show the image segment information after applying 7 image decomposition levels. Segment 6 was chosen in each color image and a message with a length of 50 characters was selected and hided in each covering image. Table IV shows the obtained experimental results. We can notice the following facts:

- The quality of the holding images is very high, the MSE value is very low, while the values of PSNR are very high.
- The hiding and extraction times are minimal.
- Increasing the image size leads to increased PSNR values as shown in Figure 7.
- If the size of one segment does not meet the message length, we can use more segments.
- It is very difficult to know the segment number and the segment size without knowing the decomposition levels.

TABLE IV. HIDING A 50 CHARACTER MESSAGE IN SEGMENT 6 OF EACH IMAGE

Image #	Resolution (pixel)	Size (byte)	MSE	PSNR	Hiding time (s)	Extraction time (s)
1	151×333	150849	0.0024	171.2046	0.00015	0.00012
2	152×171	77976	0.0050	163.7287	0.0010	0.0010
3	360×480	518400	0.00079282	182.2244	0.0010	0.0010
4	1071×1600	5140800	0.000077420	205.4879	0.0030	0.0025
5	981×1470	4326210	0.000096389	203.2964	0.0020	0.0020
6	165×247	122265	0.0031	168.4323	0.0012	0.0012
7	360×480	518400	0.00081790	181.9130	0.0010	0.0010
8	183×275	150975	0.0022	172.0226	0.0010	0.0010
9	183×275	150975	0.0025	170.8047	0.0010	0.0010
10	201×251	151353	0.0029	169.1633	0.0010	0.0010
11	600×1050	1890000	0.00019365	196.3198	0.0025	0.0025
12	1144×1783	6119256	0.000062426	207.6406	0.0030	0.0030

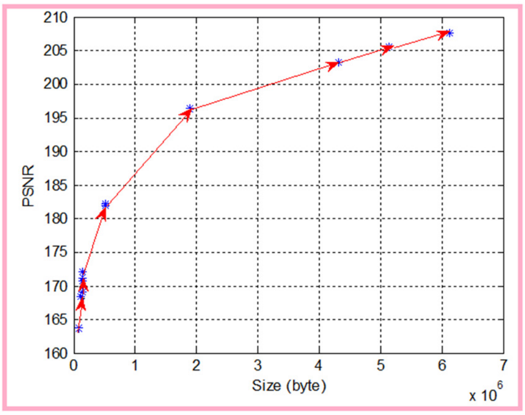


Fig. 7. PSNR as a function of image size.

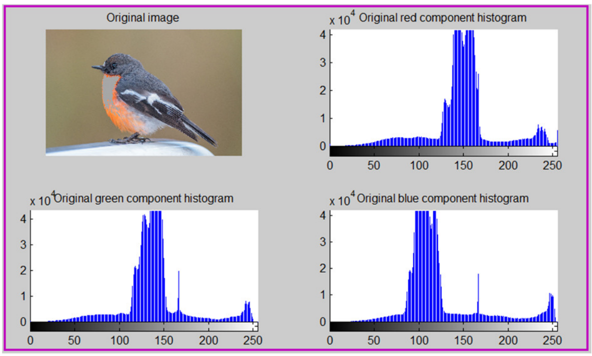


Fig. 8. Covering image and histograms.

Figures 8 and 9 show the covering and the holding images in image #12, with message size = 331776. Table V shows the obtained results after hiding messages with various sizes in segment 6. From Table V we can conclude the following:

- The MSE values remain low and the PSNR values remain high even after hiding long-length messages.
- The quality of the holding image is close to the quality of the covering image.
- Increasing the message length will lead to decreasing PSNR as shown in Figure 10.
- Increasing message length will lead to increased hiding time as shown in Figure 11.
- Increasing message length will lead to rapidly increasing extraction time, as shown in Figure 12.

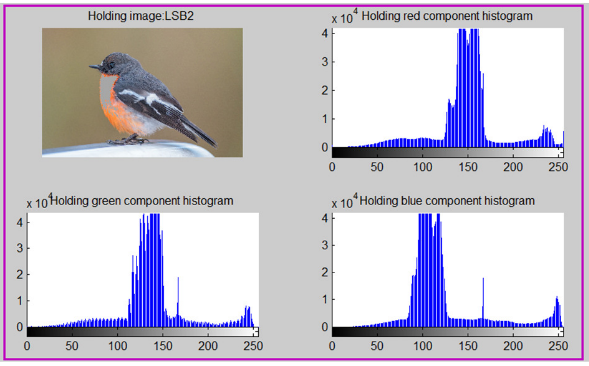


Fig. 9. Holding image and histograms (big size image).

TABLE V. HIDING VARIOUS MESSAGES IN IMAGE 12, SEGMENT 6

Message size (bytes)	MSE	PSNR	Hiding time (s)	Extraction time (s)
162	0.00025036	193.7515	0.0040	0.000120
324	0.00047963	187.2502	0.0060	0.001000
648	0.00097087	180.1985	0.0090	0.0040
1296	0.0020	173.2242	0.0150	0.0080
2592	0.0039	166.3545	0.0260	0.0240
5184	0.0078	159.3298	0.0510	0.0700
10368	0.0155	152.4668	0.1000	0.2660
20736	0.0311	145.5429	0.2020	0.6040
41472	0.0620	138.6369	0.4340	1.2770
82944	0.1247	131.6397	0.9130	3.5160
165888	0.2489	124.7307	1.5750	11.5300
331776	0.4981	117.7943	3.0810	43.4310

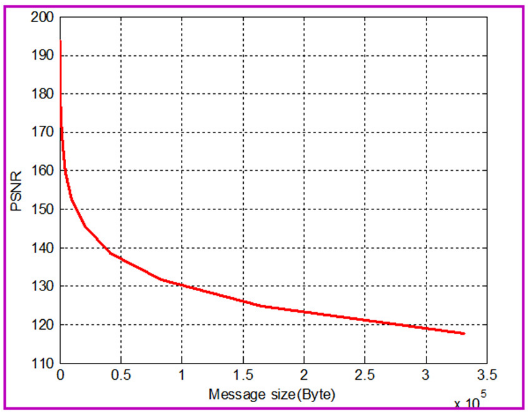


Fig. 10. PSNR vs message length.

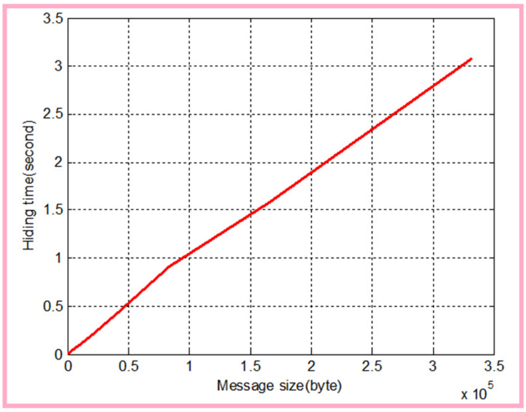


Fig. 11. Hiding time vs message length.

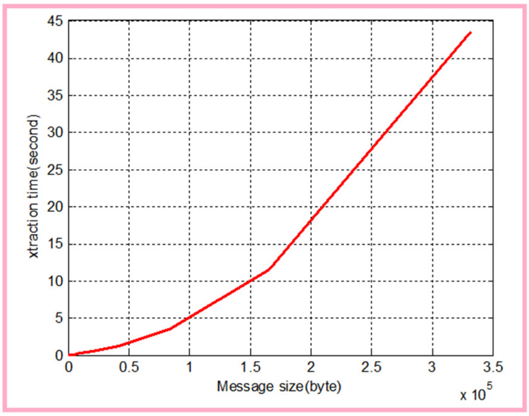


Fig. 12. Extraction time vs message length.

The obtained experimental results showed that the proposed method can be recommended to be used instead of the LSB2 method, because it can add a security level without affecting the efficiency and capacity of the LSB2 method. From the obtained results we can see that the quality parameters are better when we use images with big sizes.

VI. CONCLUSION

In this paper, a secure LSB2 method of data steganography was proposed, implemented, and analyzed. The obtained experimental results showed that selecting the image rearrangement method, the number of decomposition levels, and a segment number will increase the security level of the LSB2 method. Using image segments for data hiding will keep the parameters of the LSB2 method without negative changes. The values for MSE, PSNR, hiding time, and extraction time remain optimal.

REFERENCES

[1] Z. Alqadi, B. Zahran, Q. Jaber, B. Ayyoub, and J. Al-Azzeh, "Enhancing the Capacity of LSB Method by Introducing LSB2Z Method," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 76–90, Mar. 2019.

[2] Z. Alqadi, B. Zahran, Q. Jaber, B. Ayyoub, J. Al-Azzeh, and A. Sharadqh, "Proposed Implementation Method to Improve LSB Efficiency," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 306–319, Mar. 2019.

[3] Z. Alqadi, R. J. Rasras, M. R. A. Sara, and B. Zahran, "Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED)," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 3228–3235, Nov. 2019, https://doi.org/10.30534/ijatcse/2019/90862019.

[4] A. Abu-Ein, A. Ziad, and J. Nader, "A Technique of Hiding Secrete Text in Wave File," *International Journal of Computer Applications*, vol. 151, no. 4, pp. 15–18, Oct. 2016, https://doi.org/10.5120/ijca2016911732.

[5] R. Abu Zneit, J. Al-Azzeh, Z. Alqadi, B. Ayyoub, and A. Sharadqh, "Using Color Image as a Stego-Media to Hide Short Secret Messages," *International Journal of Computer Science & Mobile Computing*, vol. 8, no. 6, pp. 106–123, Jun. 2019.

[6] J. Al-Azzeh, Z. Alqadi, B. Ayyoub, and A. Sharadqh, "Improving the security of LSB image steganography," *JOIV : International Journal on Informatics Visualization*, vol. 3, no. 4, pp. 384–387, Nov. 2019, https://doi.org/10.30630/joiv.3.4.233.

[7] Z. Alqadi, A. Sharadqh, N. Asad, I. Shayeb, J. Al-Azzeh, and B. Ayyoub, "A highly secure method of secret message encoding," *International Journal of Research in Advanced Engineering and Technology*, vol. 5, no. 3, pp. 82–87, Jul. 2019.

[8] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, https://doi.org/10.48084/etasr.2380.

[9] A. Y. Hendi, M. Dwairi, Z. A. Al-Qadi, and M. S. Soliman, "A Novel Simple and Highly Secure Method for Data Encryption-Decryption," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 232–238, Apr. 2019.

[10] J. Azzeh, Z. Alqadi, and Q. Jaber, "A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images," *JOIV: International Journal on Informatics Visualization*, vol. 4, no. 1, pp. 40–44, Feb. 2020, https://doi.org/10.30630/joiv.4.1.232.

[11] Z. Alqadi and J. Nader, "Classification of matrix multiplication methods used to encrypt-decrypt color image," *International Journal of Computer and Information Technology*, vol. 5, no. 5, pp. 469–464, Nov. 2016.

[12] A. AlQaisi, M. AlTarawneh, Z. A. Alqadi, and A. A. Sharadqah, "Analysis of color image features extraction using texture methods," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1220–1225, Jun. 2019, https://doi.org/10.12928/telkomnika.v17i3.9922.

[13] Z. Alqadi, B. Zahran, and J. Nader, "Estimation and Tuning of FIR Lowpass Digital Filter Parameters," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 2, pp. 18–23, Feb. 2017, https://doi.org/10.23956/ijarcsse/V7I2/01209.

[14] Z. Alqadi, M. Aqel, and I. M. M. El Emary, "Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms," *World Applied Sciences Journal*, vol. 5, no. 2, pp. 211–214, 2008.

[15] A. A. Moustafa and Z. A. Alqadi, "A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image," *Journal of Computer Science*, vol. 5, no. 5, pp. 355–362, May 2009, https://doi.org/10.3844/jcssp.2009.355.362.

[16] M. Dwairi, Z. Alqadi, A. Abujazar, and R. Abu Zneit, "Optimized True-Color Image Processing," *World Applied Sciences Journal*, vol. 8, no. 10, pp. 1175–1182, Nov. 2010.

[17] J. Al Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, and M. Abu zaher, "A novel zero-error method to create a secret tag for an image," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 13, pp. 4081–4091, Jul. 2018.

[18] Z. A. A. Alqadi, M. K. A. Zalata, and G. M. Qaryouti, "Comparative analysis of color image Steganography," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 11, pp. 37–43, Nov. 2016.

[19] Z. Alqadi, M. Khrisat, A. Hindi, O. Majed, and M. Dwairi, "Simple and Highly Secure, Efficient and Accurate Method (SSEAM) to Encrypt-Decrypt Color Image," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 9, no. 4, pp. 64–69, Apr. 2020, https://doi.org/10.17148/IJARCCE.2020.9413.

[20] R. Z. Rasras, M. R. A. Sara, Z. A. AlQadi, and R. A. Zneit, "Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3, pp. 748–754, May 2019, https://doi.org/10.30534/ijatcse/2019/64832019.

[21] A. Hindi, M. Dwairi, and Z. Alqadi, "Analysis of Digital Signals using Wavelet Packet Tree," *International Journal of Computer Science and Mobile Computing*, vol. 9, no. 2, pp. 96–103, Feb. 2020.

[22] M. Khrisat, A. Hindi, Z. Alqadi, and M. Dwairi, "Valuable Wavelet Packet Information to Analyze Color Images Features," *International Journal of Current Advanced Research*, vol. 9, no. 2, pp. 21252–21255, Mar. 2020.

[23] M. J. Aqel, Z. ALQadi, and A. A. Abdullah, "RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication," *International Journal of Engineering & Technology*, vol. 7, no. 3.13, pp. 104–107, Jul. 2018, https://doi.org/10.14419/ijet.v7i3.13.16334.

[24] M. O. Al-Dwairi, A. Y. Hendi, and Z. A. AlQadi, "An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images," *Engineering, Technology & Applied Science Research*, vol. 9, no. 3, pp. 4165–4168, Jun. 2019, https://doi.org/10.48084/etasr.2525.

[25] A. Y. Hindi, M. O. Dwairi, and Z. A. AlQadi, "A Novel Technique for Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 4942–4945, Dec. 2019, https://doi.org/10.48084/etasr.2955.