VOL. 17, NO. 3, FEBRUARY 2022 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

COVER IMAGE REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY

Mohammad S. Khrisat[1], Adnan Manasreh[2], Hatim Ghazi Zaini[3] and Ziad A. Alqadi[1]
[1]Department of Computer Engineering, Faculty of Engineering Technology, AL-Balqa Applied University, Amman, Jordan
[2]Department of Electrical Engineering, Applied Science Private University, Amman, Jordan
[3]Computer and Information Technology College, Taif University, Taif, Kingdom of Saudi Arabia
E-Mail: adnan_m@asu.edu.jo

ABSTRACT

Protecting the data circulated through the various means of communication, whether the data is secret text messages or secret colored images, is very important to prevent intruders from eavesdropping on confidential data. In this paper research a method based on LSB will be introduced to be used easily for data steganography. The method will adds a hard to attack private key, this key will be generated as a result of cover image decomposition and image segments rearrangement, and it will be used to reproduce the cover image by replacing the cover image segments. The proposed method will control the data hiding capacity and adding a capability of hiding text messages and huge color images at the same time.

Keywords: steganography, cover, stego, PK, WPT, MSE, PSNR, capacity, throughput.

1. INTRODUCTION

Colored digital images [1], [2], [3]are considered one of the most widely used and circulated types of digital data through various social media, and the reasons are due to the ease of obtaining them and at the lowest cost due to the availability of the multimedia that is being generated [4], 5].

Color digital images [6], [7] have a high resolution, which provides a huge amount of data that can be used for multiple applications, including hiding confidential data. The digital image is represented by a three-dimensional matrix, one dimension for each color (red, green and blue), and this makes the tasks of processing it easy [8], [9], [10].

Digital color image can be easily resized using mostly or available now software, we can increase or decrease the image size by performing the image resizing operation, resizing can be applicable if we want to increase the capacity of the image (to hold big size of secret data), Figure-1 shows the outputs of image resizing.

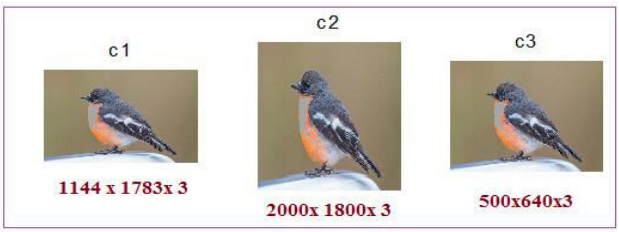

Figure-1. Image resizing.

Data steganography (see Figure-2) is the process of hiding secret data (message, digital image) into a covering digital color image, and here the method of data steganography must satisfy the following requirements [11], [12]:

- The stego image must be much closed to the cover image, which is not possible to the naked eye to notice the differences between the cover and the stego images. Achieving this can be done by minimizing the mean square error (MSE) between the two images and maximizing the value peak signal to noise ratio (PSNR) between the cover and stego images (see equations 1 and 2) [13], [14].
- The extracted image must be the same as the hidden image (no loss of information), and here MSE between the hidden and extracted images must equal zero, while the PSNR must be infinite [15], [16].
- The embedding method must be efficient by minimizing the hiding and extracting time, thus will increase the number of secret byte (hidden or extracted) in a unit of time (Throughput) [17], [18], [19].
- The embedded method must be secure to protect the hidden secret data from other third party, this can be done by connecting the hiding and extracting processes with a special generated private key (PK).
- The cover image must have a big size to provide a huge capacity of hiding messages and color images.
- Providing a possibility of cover image resizing to meet the necessary capacity.

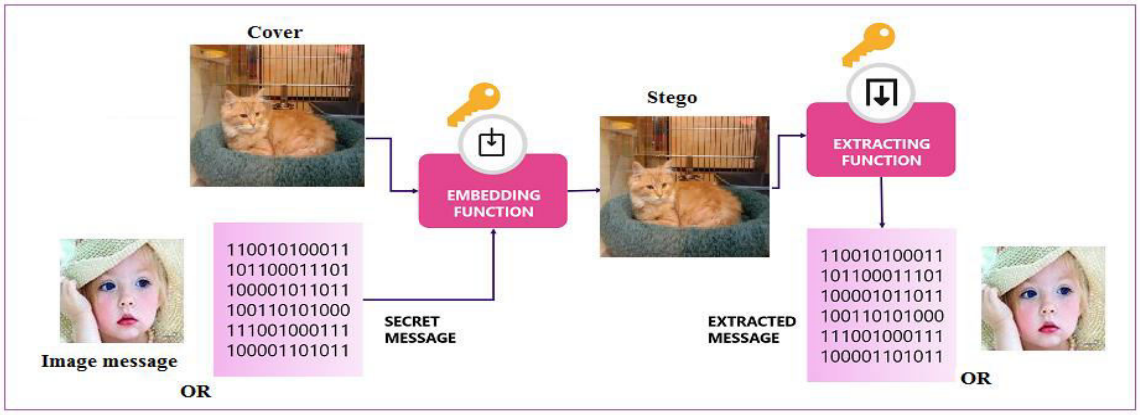

Figure-2. Data steganography process.

MSE between messages S and R, n: message length

$$MSE_{SR} = \frac{1}{N}\sum_{j=0}^{n-1}[S(j) - R(j)]^2 , N = n \quad (1)$$

$$PSNR_{SR} = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_{SR}} \quad (2)$$

Many popular methods of data steganography are based on least significant bit (LSB)[19], [20], [21] method of data hiding, this method provides a good parameters but it is not secure, this method reserves 8 bytes from the cover image to hide one byte from the secret data, the least significant bits from the set of 8 bytes are replaces by the secret byte bits as show in Figure-3:

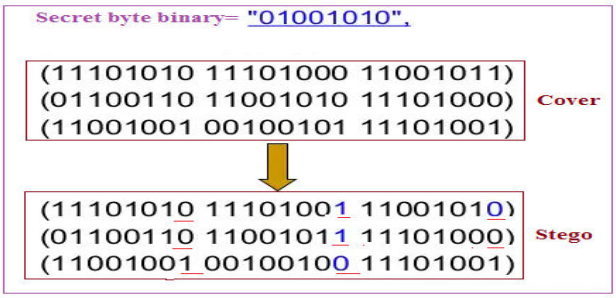

Figure-3. Hiding secret byte 74.

2. COVER IMAGE REARRANGEMENT

This task is needed to form the PK which will be used to secure LSB method of data steganography. The cover image will be divided into segments using wavelet packet tree (WPT) [22], [23] decomposition; this operation can be done [24], [25] by applying the matlab function `[c,l] = wavedec(double(b),6,'db1');`, as shown in Figure-4.

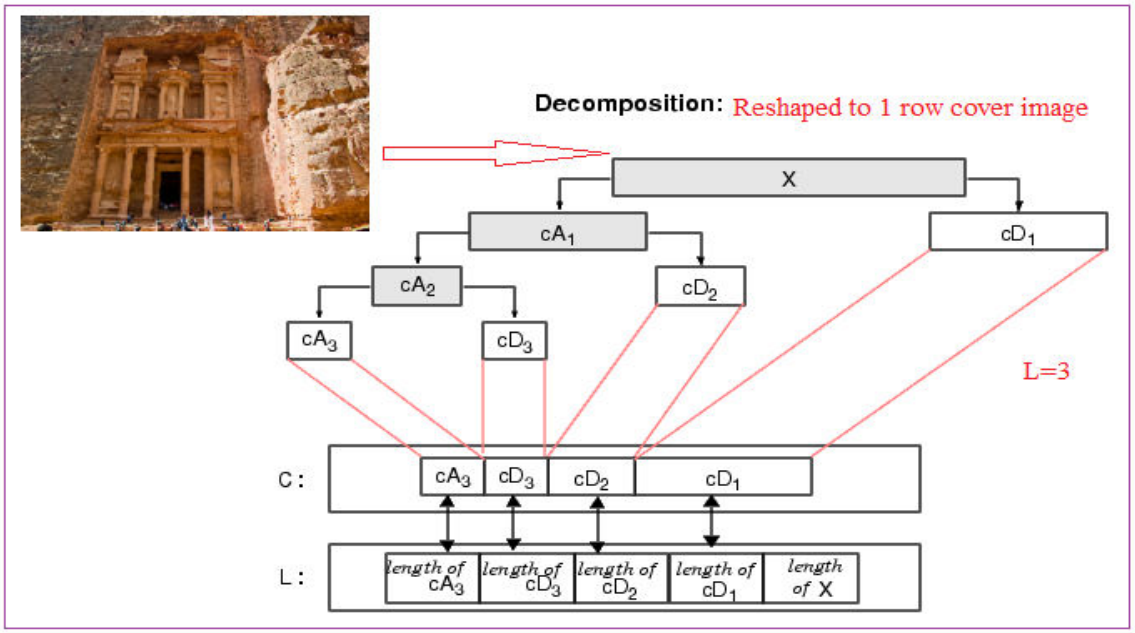

Figure-4. Image decomposition.

Getting the L array we can form the image segments with lengths and sizes, these segments can be then rearranged as shown in Figure-5:

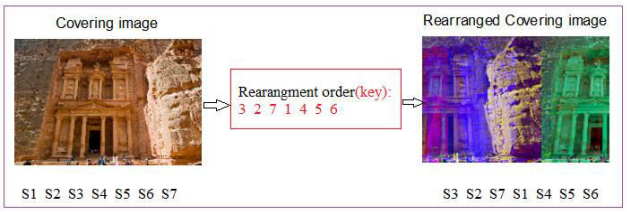

Figure-5. Image segments rearrangement.

The process of cover image WPT decomposition based on the selected number of composition levels will divide the cover image into segments, each segment location and size are included in the array L. The PK must equal the rearrangement sequence and must be known by the data sender and receiver.

3. THE PROPOSED METHOD

The proposed method uses the operations image reshaping and image resizing(when the capacity of the cover image is not enough to hold the secret data, these operation can be performed as shown in Figures 6 and 7:

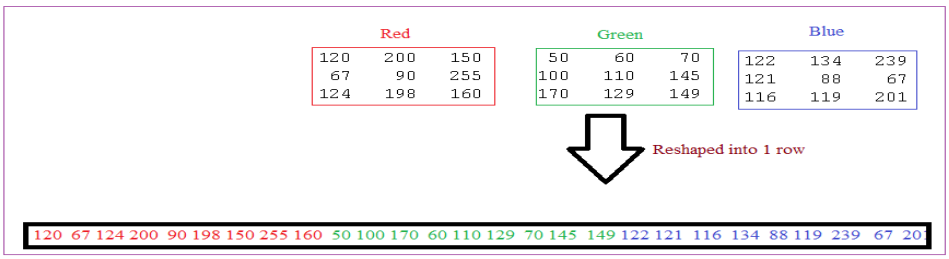

Figure-6. Data reshaping.

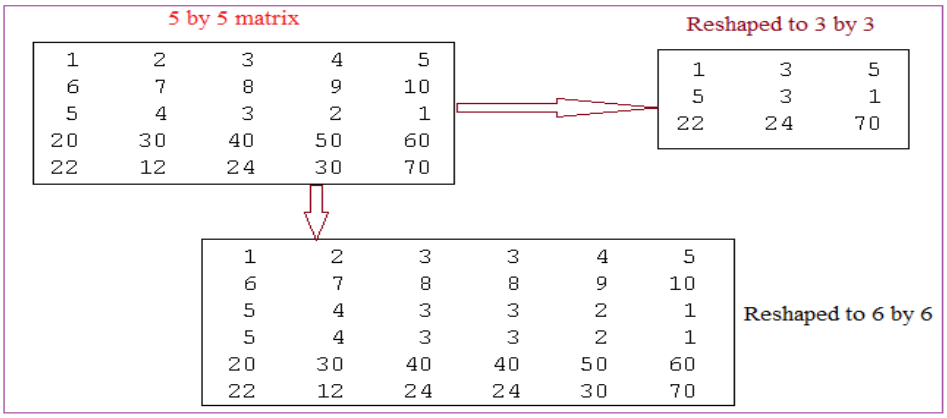

Figure-7. Data resizing.

The proposed method is based on LSB technique and it can be implemented applying the following steps (see Figures 8 and 9):

Secret data hiding:

This task can be implemented (see Figure-8) applying the following steps:

Step 1: Get the cover image and the secret data.
Step 2: Resize the cover image if the capacity less than the size of secret data multiplied by 8.
Step 3: Reshape the cover image to 1 row matrix.
Step 4: Apply WPT decomposition.
Step 5: Get the segments (location and size) from the L array.
Step 6: Select the sequence of rearrangement to be used as a PK.
Step 7: Rearrange the 1 row matrix according to the selected sequence (PK).
Step 8: Reshape the cover image back to 3D matrix.
Step 9: Apply LSB to hide the data.
Step 10: Rearrange the image back to get the stego image.

Data extraction

This task can be implemented applying the following steps (see Figure-9).

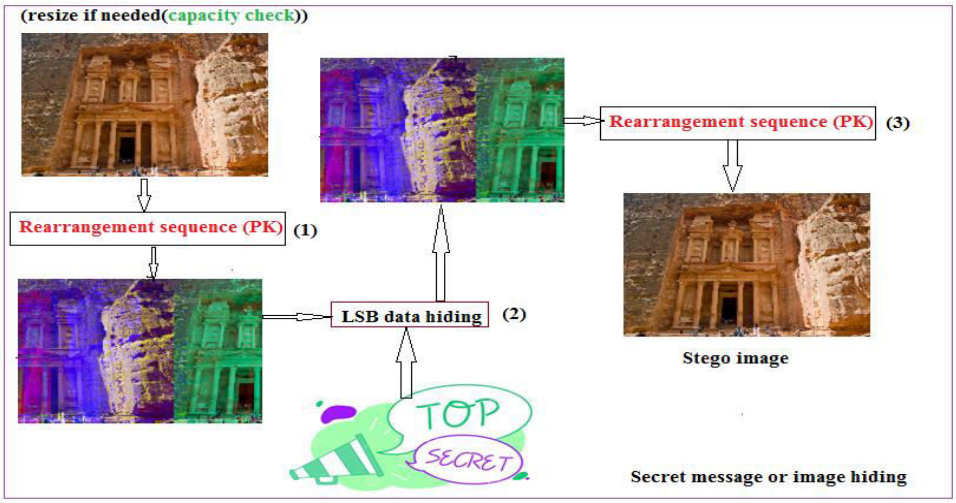

Figure-8. Hiding process.

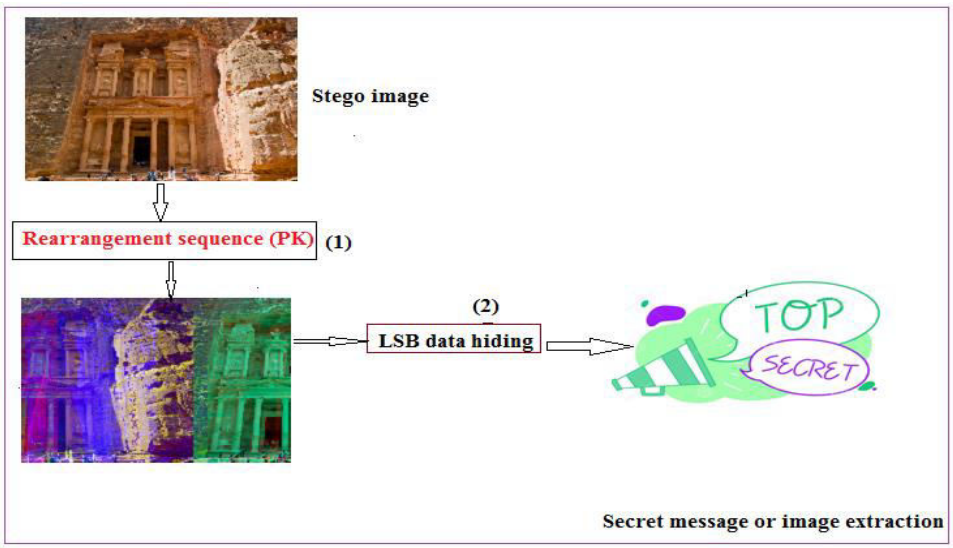

Figure-9. Extracting process.

Step 1: Get the stego image.
Step 2: Reshape the image to 1 row matrix.
Step 3: Rearrange the matrix using PK.
Step 4: Reshape the rearranged row matrix to 3D matrix.
Step 5: Apply LSB to extract the hidden data.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

A cover image was selected; other color images with various sizes were hidden using the proposed method, Figures 10 and 11 show an example of cover and stego images produced by the method, while Figure-12 shows the hidden and extracted images:

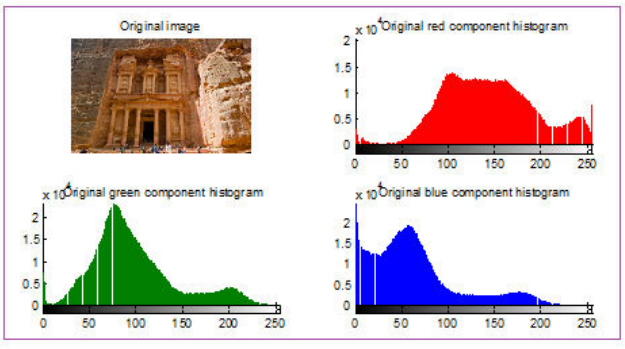

Figure-10. Cover image example.

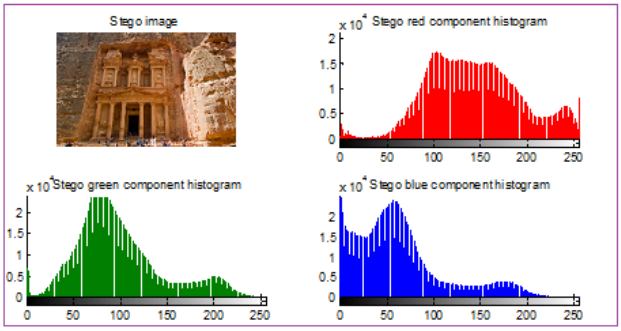

Figure-11. Stego image example.

Figure-12. Hidden and extracted images.

The image shown in Figure-11 was fixed and used as a cover image, the image size =1071x 1600x 3=5140800 bytes, capacity =642600 and PK=3, 2, 7, 1, 4, 5, 6, tables 1 and 2 show the obtained results using the proposed method.

Table-1. Results of MSE and PSNR.

Image to be hidden number	Size(byte)	Between cover and stego images		Between Hidden and extracted images		Resizing cover image
		MSE	PSNR	MSE	PSNR	
1	150849	1.5329e+003	37.4764	0	Infinite	no
2	77976	3.5719e+003	29.0167	0	Infinite	no
3	518400	2.5322e+003	32.4570	0	Infinite	no
4	4326210	2.3076e+003	33.3854	0	Infinite	yes
5	122265	2.0752e+003	34.4472	0	Infinite	no
6	518400	2.7603e+003	31.5943	0	Infinite	no
7	150975	2.5941e+003	32.2154	0	Infinite	no
8	150975	2.0644e+003	34.4995	0	Infinite	no
9	151353	2.6969e+003	31.8266	0	Infinite	no
10	1890000	2.5770e+003	32.2815	0	Infinite	yes

Table-2. Efficiency parameters results.

Image number	Size(byte)	Hiding time(second)	Extracting time(second)
1	150849	0.4940	0.2190
2	77976	0.4110	0.1470
3	518400	0.8260	0.5740
4	4326210	3.6220	0.7860
5	122265	0.4760	0.1890
6	518400	0.8180	0.5960
7	150975	0.5220	0.2180
8	150975	0.4930	0.2220
9	151353	0.5010	0.2170
10	1890000	1.7790	0.7280
Average	8.0574e+005	0.9942	0.3896
Throughput		8.1044e+005	2.0681e+006

The same covering image was used to hide-extract secret messages with various lengths, Figure-13 show the stego image holding a message of 27 characters, while Table-3 shows the obtained results of manipulating various data messages.

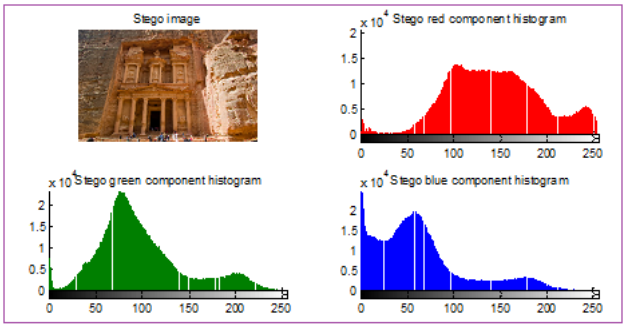

Figure-13. Stego image holding 27 characters message.

Table-3. Results for data messages steganography.

Message length(byte)	Between cover and stego images		Hiding time (Seconds)	Extracting time (Seconds)
	MSE	PSNR		
27	1.9647e-005	219.2013	0.3340	0.2490
58	4.2406e-005	211.5075	0.3360	0.2493
127	9.3176e-005	203.6355	0.3400	0.2498
259	1.8732e-004	196.6519	0.3419	0.2501
523	3.7562e-004	189.6945	0.3432	0.2507
733	5.2968e-004	186.2576	0.3441	0.2512
835	6.0496e-004	184.9287	0.3459	0.2534
1675	0.0012	177.9892	0.3710	0.2592
2020	0.0015	176.0899	0.3803	0.2612

Figures 14, 15, and 16 illustrate the relationship between the message length and MSE, PSNR and efficiency parameters respectively.

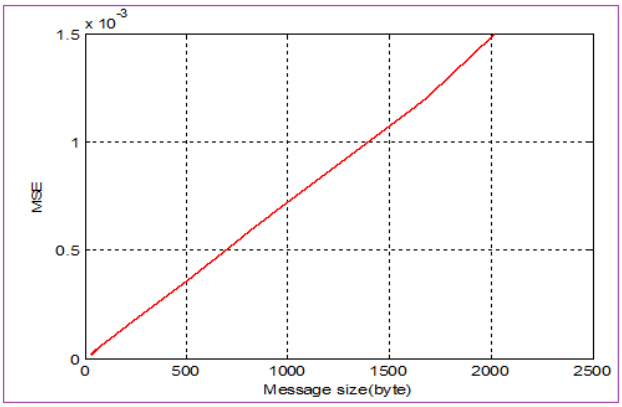

Figure-14. Relationship between MSE and message length.

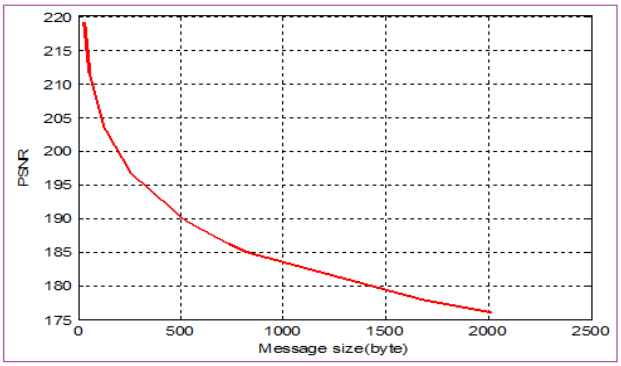

Figure-15. Relationship between PSNR and message length.

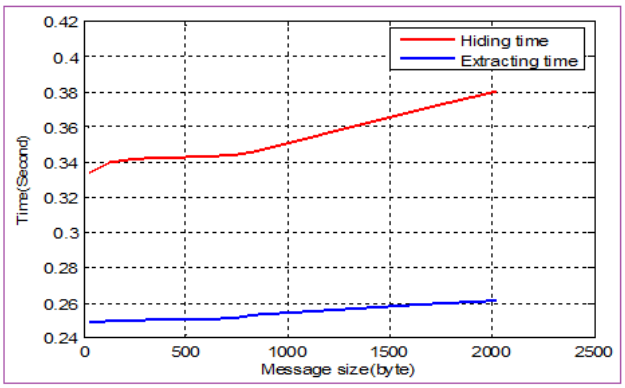

Figure-16. Relationship between MSE and efficiency parameters.

From the obtained results of the proposed method implementation we can see the following facts:

- The proposed method provides a high level of security, it is very difficult to guise the PK, because it is very difficult to know the number of levels used to decompose the cover image and it is very difficult to know the number of segments and how these segments are rearranged to reproduce the cover image.
- LSB provides good values of MSE and PSNR, and the proposed method does not negatively affect these parameters.
- The throughput of the proposed method is very high as a results of decreasing the hiding and extracting times.
- Excellent results are obtained for character messages steganography.

- The Capacity of the cover image can be increased to hide bigger in size secret data.
- The proposed method can be easily used to hide character data messages and color images.

5. CONCLUSIONS

A simple, efficient and highly secure method of data steganography was proposed, tested and implemented. The obtained results showed that the proposed method can be used to protect the secret data during data communication using a special generated private key, this key contains a sequence of image segments and based on this sequence the cover image is to be rearranged. The proposed method does not negatively affect the good parameters of LSB and it can be easily used to process character messages and color images at the same time adding a feature of controlling the cover image capacity.

ACKNOWLEDGMENT

The researchers are grateful to the Applied Science Private University, Amman, Jordan, for the full financial support grated to this research project.

REFERENCES

[1] Dr. Mohamad Tariq Mohamad Barakat, Dr. Hatim Ghazi Zaini, Prof. Ziad AlQadi. 2021. Text File Encryption_Decryption Using Key Quitient and remainder. International Journal of Engineering Technology Research & Management. 5(4): 9-21.

[2] Ziad Al Qadi, M. Elsayyed Hussein. 2017. Window Averaging Method to Create a Feature Victor for RGB Color Image. International Journal of Computer Science and Mobile Computing. 6(2).

[3] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi. 2019. Suggested Method to Create Color Image Features Victor. Journal of Engineering and Applied Sciences. 14(1): 2203-2207.

[4] Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A Abujazar, Rushdi Abu Zneit. 2010. Optimized true-color image processing. World Applied Sciences Journal. 10(8): 1175-1182.

[5] A. A. Moustafa, Z. A. Alqadi. 2009. Color Image Reconstruction Using A New R'G'I Model. Journal of Computer Science. 5(4): 250-254.

[6] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata. 2016. Creating a Color Map to be used to Convert a Gray Image to Color Image. International Journal of Computer Applications. 153(2).

[7] Ashraf Abu-Ein, Ziad A. A. Alqadi, Jihad Nader. 2016. A Technique Of Hiding Secretes Text In Wave File. International Journal of Computer Applications.

[8] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub. 2019. Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, IJCSMC. 8(6): 106-123.

[9] Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh. 2019. Improving the security of LSB image steganography, JOIV: International Journal on Informatics Visualization. 3(4): 384-387.

[10] Belal Ayyoub Ziad Alqadi, Ahmad Sharadqh, Naseem Asad Ismail Shayeb, Jamil Al-Azzeh. 2019. A highly secure method of secret message encoding. International Journal of Research in Advanced Engineering and Technology. 5(3): 82-87.

[11] Ahmad Sharadqh Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh. 2019. Proposed Implementation Method toImprove LSB Efficiency. International Journal of Computer Science and Mobile Computing. 8(3): 306-319.

[12] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh. 2019. Enhancing the Capacity of LSB Method by Introducing LSB2Z Method. International Journal of Computer Science and Mobile Computing. 8(3): 76-90.

[13] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh. 2019. Proposed Implementation Method to Improve LSB Efficiency. International Journal of Computer Science and Mobile Computing. 8(3): 306-319.

[14] Dr. Mohammad S. Khrisat Prof. Ziad Alqadi, Simple, Qualities. 2021. Efficient and Secure Method to Encrypt Voice Signal. International Journal of Computer Applications. 183(7): 25-29.

[15] Ziad alqadi Hatim Ghazi Zaini. 2021. Replaced ASCII table to encode-decode secret messages. International Journal of Advanced Research in Computer and Communication Engineering. 10(3): 67-74.

[16] Hatem Zaini Prof. Ziad Alqadi. 2021. Color Image Cryptography Using Huge Random Private Key.

Word journal of engineering research and technology. 7(3)

[17] : 42-52.

[18] Dr. Mohammad S. Khrisat, Prof. Ziad Alqadi 2021. Analysis of Text Files Encryption-Decryption Methods. Ijetrm. 5(3): 48-54.

[19] Prof. Ziad A. Alqadi Anwar Al Abadi. 2021. Using Large Color Image to Encrypt-Decrypt Smaller Ones. IJETRM. 5(2): 71-81.

[20] Prof. Ziad Alqadi. 2021. Efficient and Highly Secure Method of Message Encryption. IJETRM. 5(2): 58-64.

[21] Prof. Ziad A. Alqadi Anwar Abadi. 2021. Using color image to encrypt-decrypt wave file. IJARCCE. 9(12): 99-106.

[22] Musbah Aqel Ziad A. Alqadi. 2009. Performance analysis of parallel matrix multiplication algorithms used in image processing. World Applied Sciences Journal. 6(1): 45-52.

[23] Mohammad S. Khrisat, Ziad Alqadi, Saleh A Khawatreh 2020. Improving WPT color image decomposition. International Journal of Computer Science and Information Security (IJCSIS). 18(7): 13-21.

[24] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat. 2020. Two ways to improve WPT decomposition used for image features extraction. European journal for scientific research. 157(2): 195-205.

[25] Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi. 2020. Creating Human Speech Identifier using WPT. International Journal of Computer Science and Mobile Computing. 9(2): 117-123.

[26] Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi. 2020. Analysis of Digital Signals using Wavelet Packet Tree. International Journal of Computer Science and Mobile Computing. 9(2): 96-103.