IJSES
Volume 6, Issue 1, pp. 49-55, 2022.
International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Highly Secure Method for Secret Data Transmission

Dr. Mohamad T. Barakat, Prof. Ziad A. Alqadi
Albalqa Applied University, Faculty of Engineering Technology, Jordan, Amman

Abstract— *In this research, we present a new method for protecting confidential and private data, which combines the two processes of data cryptography and data steganography. The data protection process in the proposed method depends on the use of a colored digital image used to generate the private key to carry out the encryption and decryption process, where this image is agreed upon by the sender and receiver and is not transmitted and is kept secret. The image_key is used to generate the secret key for any text message, regardless of its length. The proposed method uses some improved procedures to hide data in the digital carrier image. The use of these procedures will raise the efficiency of the method compared to the least significant method, which is frequently used in the process of data hiding. It will be shown how the proposed method will decrease the hiding and extraction times and how it will be improved the value of the quality parameters MSE and PSNR.*

Keywords— *Cryptography, steganography, crypto-steganography, image_key, PK, efficiency, MSE, PSNR.*

I. INTRODUCTION

Secret and private messages are widely circulated through various social media, which requires the protection of these messages from the danger of tampering and data thieves, and the process of penetrating these messages and understanding their contents. Multiple processes are used to protect confidential messages, including data cryptography, data steganography, and these two processes can be combined using a process of crypto- steganography [21-25].

Colored digital images are one of the most important types of data that can be used to provide the necessary protection for confidential messages. The reason for this is due to several things, the most important of which are [1-5]:

- ✓ Ease of obtaining the image from multiple sources and at the lowest cost.
- ✓ Ease of processing the digital image, because it is represented by a three-dimensional matrix (one dimension for each color of the three colors: red, green and blue) and as shown in the figure1 . Therefore, digital image processing operations are nothing but matrix processing operations.
- ✓ The pixel values and the values of each of the three colors in the digital image range between 0 and 255, and these values correspond to the ASCII values of the symbols that make up the text message (see figure 2) [26-32].

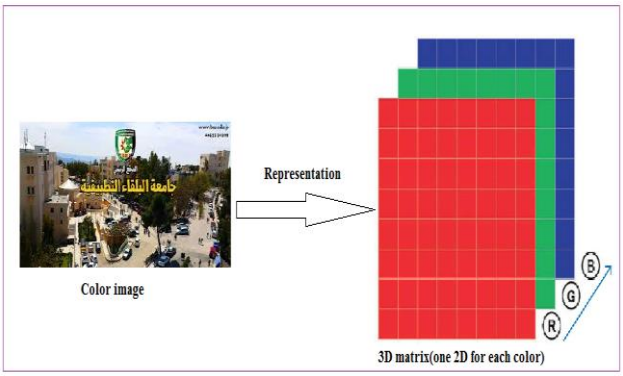


Figure 1: Color image representation

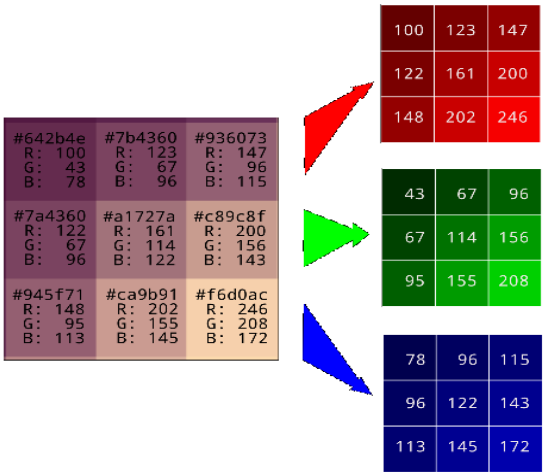


Figure 2: Colors values

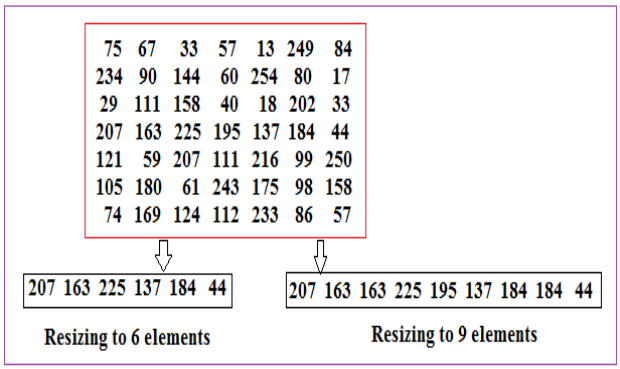


Figure 3: Matrix resizing example

- ✓ The digital color image has a huge amount of data, which provides an excellent digital environment for processing data, including text messages.
- ✓ The possibility of using the matrix of each color separately and the possibility of using specific parts of the image to carry out various processing operations.
- ✓ The ability to extract and retrieve data from a digital image using the image resizing process (see figures 3 and 4)). Through this process, private keys can be generated with lengths commensurate with the lengths of text messages [6-11].

International Journal of Scientific Engineering and Science
Volume 6, Issue 1, pp. 49-55, 2022. ISSN (Online): 2456-7361

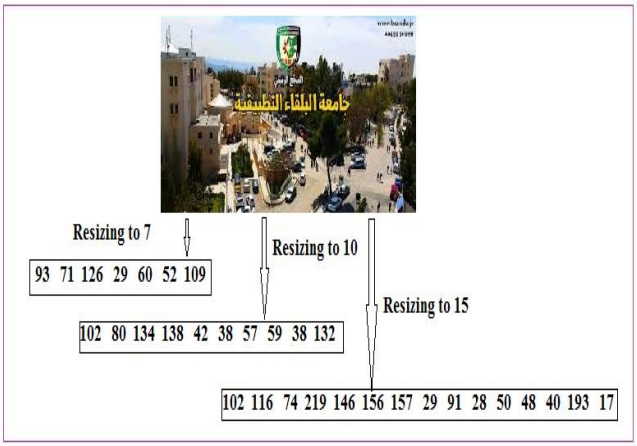


Figure 4: Image resizing example

Data steganography as shown in figure 5 is the process of hiding secret data in a covering image to produce a stego_image. Here the method of data steganography must add a minor change to the image and these changes must not be noticed by human naked eyes. To see whether the method of data steganography meet the requirement of image quality we can calculate the mean square error (MSE)between the covering image and the stego_image, this value must very small, or/and we can use the value of peak signal to noise ratio (PSNR), this value must be big enough, MSE and PSNR between 2 images can be calculated using equations 1 and 2 [14-20].

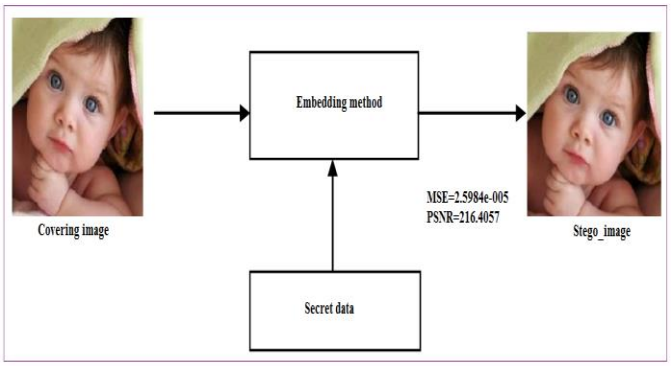


Figure 5: Data steganography process

MSE of x channel

$$MSE_x = \frac{1}{N}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[S(i,j) - R(i,j)]^2 \quad , N = m * n \tag{1}$$

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

$$PSNR = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_t} \tag{2}$$

Data cryptography is the process of data encryption and decryption (see figure 6), encryption means destroying the data so MSE between the original and the encrypted data must be very high (PSNR must be very low), while decryption means recovering the original data without any changes, here MSE must equal 0 and PSNR must equal infinite [20-25].

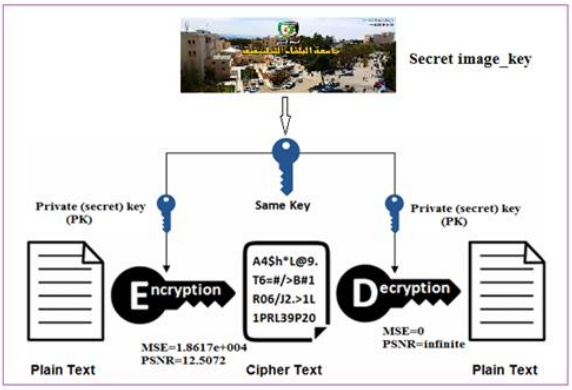


Figure 6: Data cryptography process

Data cryptography can be implemented using a secret private key (PK), this key is only known by the sender and receiver and it can be easily obtained from an image which can be used as a secret image_key.

To protect the process of data steganography we can combine data steganography with data cryptography to get the benefits of the two operation as shown in figure 7 [14].

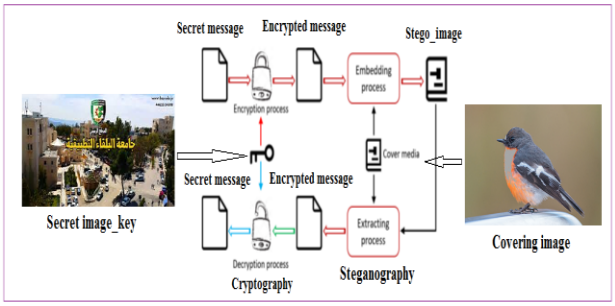


Figure 7: Combining data cryptography with data steganography

II. Related Works

Many methods of data steganography are based on the least significant bit (LSB) method [4], [11], this method is very simple and it can be executed applying the following steps [12], [13]:

- Select the carrier image.
- Convert the carrier image to binary.
- Select the secret message, and convert it to binary.
- For each byte of the secret message reserve 8 bytes of the image, and use LSB of each to insert on bit of the message byte.
- Convert the binary image to decimal to get the stego_image

Figure 8 Illustrates an example of LSB operations:

International Journal of Scientific Engineering and Science
Volume 6, Issue 1, pp. 49-55, 2022. ISSN (Online): 2456-7361

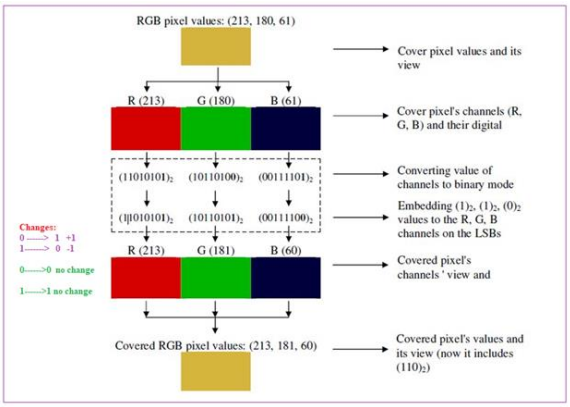


Figure 8: LSB method example

From the figure, it becomes clear to us that the changes in the carrier image are slight, ranging between -1 and +1, which cannot be observed with the naked eye.

Multiple methods are used to hide confidential data in color digital images, and many of these methods depend on the LSB method, as this method provides many advantages, the most important of which are:

- ✓ Ease of programming and implementation.
- ✓ Its ability to hide large messages in a digital color image, where the length of the message can reach the size of the image divided by eight.
- ✓ This method provides excellent values for the image quality parameters (MSE and PSNR), so it is difficult to observe the change in the data-carrying image with the naked eye.
- ✓ The method has high efficiency because the time to hide the data and the time to retrieve it is relatively short.

Despite the advantages of the LSB method, it has some disadvantages that need to be addressed, including:

- ☒ The method is not secure and anyone with the necessary software skills can retrieve the secret message from the stego_ image.
- ☒ Determining the length of the secret message is not mandatory and by guessing it is possible to retrieve the secret data from the stego_ image.
- ☒ It is necessary to improve the quality parameters of the method, especially when the length of the secret message is large and the size of the carrier image is small.

III. The Proposed Method

The proposed method requires knowing the secret image_key to generate the PK required in the encryption and decryption phases, the secret message length and the bit plate as an input to perform the hiding and extracting phases, these parameters can be considered as a private key and they must be kept in secret between the sender and receiver, using other message length in the extracting phase will cause extracting rubbish data as we will see in the implementation part.

The proposed method for embedding the secret message will be implemented applying the following algorithm:

Algorithm: Hiding phase

Inputs:

Covering image (I), secret message (txt), bit plate (b), secret image_key (SK)

Processing:

1. Retrieve image size(S), Retrieve message size (m), calculate message binary size (N=m*8).
2. Resize SK to get PK with size equal m.
3. XOR PK with the ASCII code of the message to get the encrypted message(etxt)
4. Find p and h. (p = 2^b, h = 2^(b-1)).
5. Reshape the image I to one row array (I1).
6. Find the deference between S and N (addl).
7. From I1 get an array of size equal N (I2).
8. From I2 get a sign array (si) (1 if greater than zero, zero otherwise).
9. For k = 1 to N
10. If si (k) = 0 then si (k) =1.
11. I2 (k) =round (I2 (K)).
12. If I2 (k) mod p >=h then I2 (k) = I2 (k) –h.
13. End for
14. Convert encrypted message to binary (bt).
15. Reshape bt to one row array (bint).
16. Compute d (d=h*48).
17. Subtract d from h*bint to get bi.
18. Add bi to I2 to get I3.
19. Concatenate bi with zeros (1, addl) to get binadd.
20. Multiply si by I3 to get I4.
21. Concatenate I4 with I1 (N+1: S) to get I5.
22. Reshape I5 to 3D matrix to get the stego_image (intl).

Output:

Stego_image (intl)

The process of data extraction will be implemented applying the following algorithm:

Algorithm: Extraction phase

Inputs:

Stego_image (I), Length of secret message (siz), bit plate (b) (the same as in hiding phase), secret image_key(SK).

Processing:

1. Retrieve image size (n), calculate message binary size (bsiz=m*8).
2. Find p and h.
3. Reshape the image I to one row array (I1).
4. Find the deference between n and bsiz (addl).
5. From I1 get an array of size equal bsiz (I2).
6. Create a zero array br of size (1, bsiz);
7. For k = 1 to bsiz
8. Divide I2 (k) by p.
9. If the remainder >=h, then make rb (k) equal 1.
10. End for
11. Get rbi by converting rb to binary (rbi = (dec2bin(rb,1))')
12. Reshape rbi to get rbin (rbin = reshape (rbi, siz,8)
13. Get the message rectxt by converting rbin to decimal (rectxt = (bin2dec (rbin))').
14. Resize SK to get PK.
15. XOR rectxt with PK to get the decrypted message (drectxt).

International Journal of Scientific Engineering and Science
Volume 6, Issue 1, pp. 49-55, 2022. ISSN (Online): 2456-7361

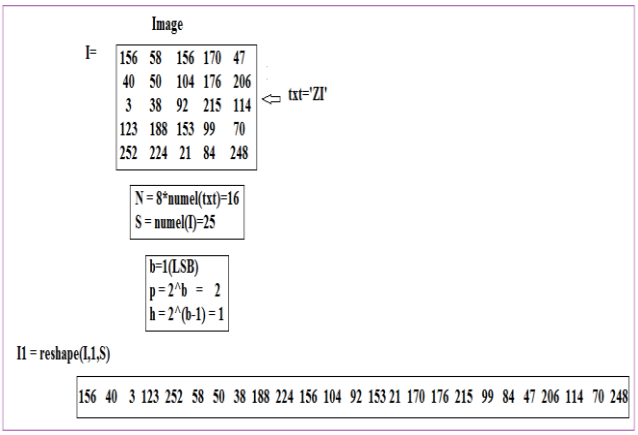
16. Convert drectxt to character to get the secret message m

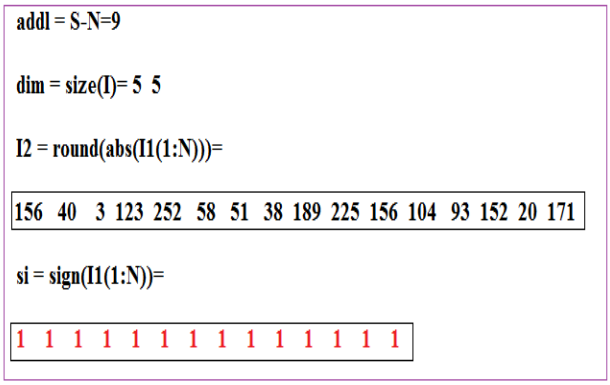
Output:

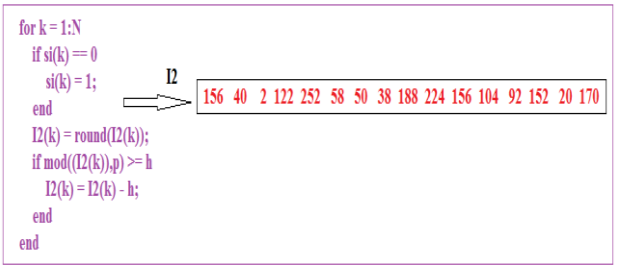
The secret message (drectxt).

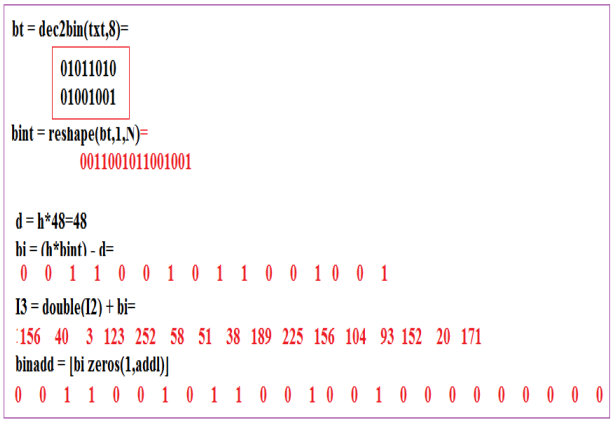
Below is a calculated example which shows the process of hiding and extracting a secret message:

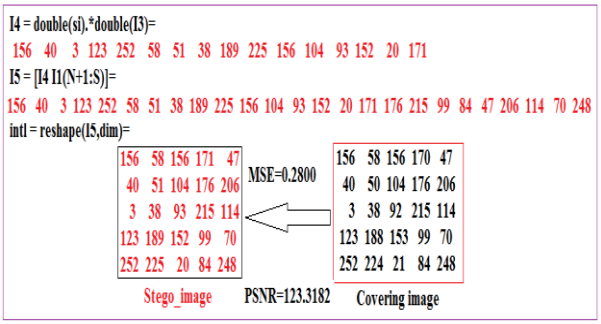
Data hiding



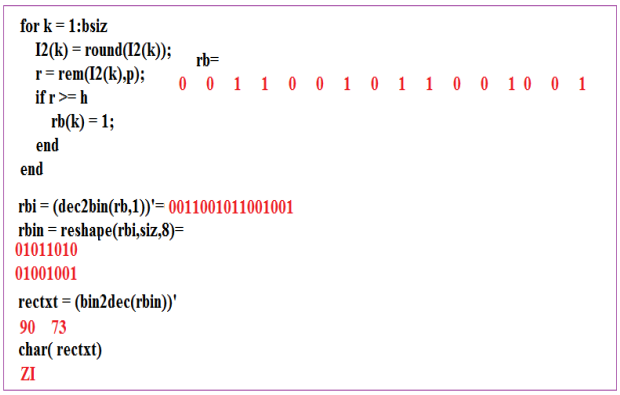








Data extraction



IV. Implementation and Experimental Results

The proposed method was implemented using various messages and various covering images, table 1 shows the images information, while figures 9 and 10 show the used images:

Table 1: Used images information

Image number	Resolution	Size (byte)	Capacity (byte)	Message max size (byte)
1	151 333 3	150849	18856	2357
2	152 171 3	77976	9747	1218
3	360 480 3	518400	64800	8100
4	1071 1600 3	5140800	642600	80325
5	981 1470 3	4326210	540780	67597
6	165 247 3	122265	15283	1910
7	360 480 3	518400	64800	8100
8	183 275 3	150975	18872	2359
9	183 275 3	150975	18872	2359
10	201 251 3	151353	18919	2364
11	600 1050 3	1890000	236250	29531
12	1144 1783 3	6119256	764907	95613

International Journal of Scientific Engineering and Science
Volume 6, Issue 1, pp. 49-55, 2022. ISSN (Online): 2456-7361

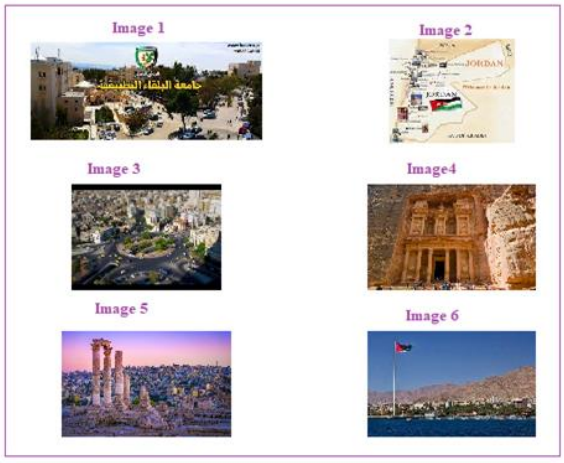


Figure 9: Used images 1 to 6

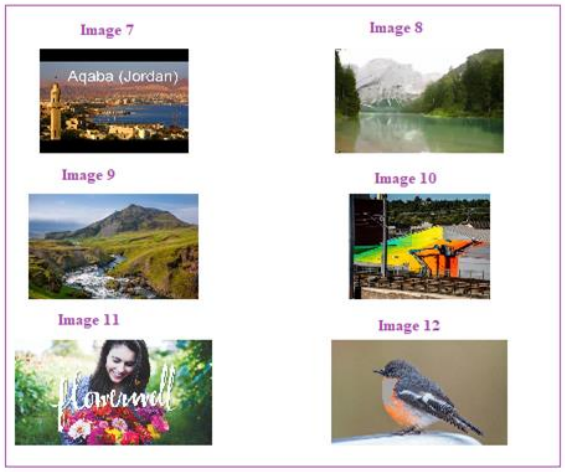


Figure 10: Used images 7 to 12

Image 1 was selected as an image_key, figure 11 shows an extracted PK key used in the encryption-decryption processes.

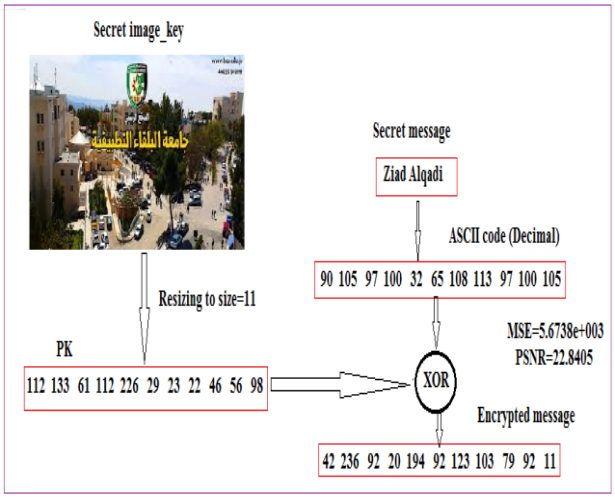


Figure 11: Image_key and extracted PK example

Image 12 was selected as a covering image, figure 12 shows a sample outputs of the implementation:

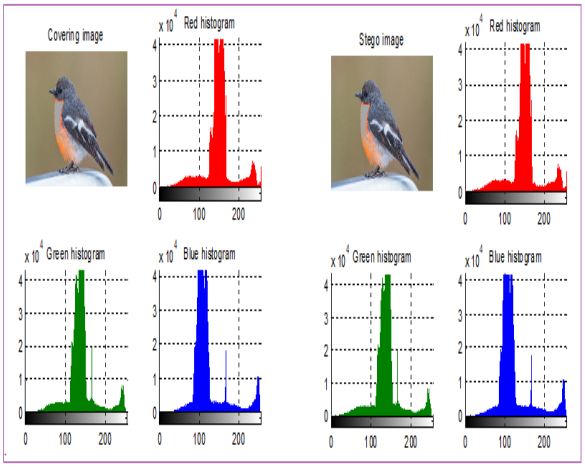


Figure 12: Sample implementation outputs

Several messages were selected and implemented using the proposed and the LSB methods, table 2 and 3 show the obtained results:

Table 2: Obtained quality parameters

Message number	Length(byte)	LSB quality parameters		Proposed quality parameters	
		MSE	PSNR	MSE	PSNR
1	52	1.8875e-004	196.5762	3.1867e-005	214.3648
2	104	3.8796e-004	189.3715	6.9453e-005	206.5739
3	208	7.7902e-004	182.4001	1.3907e-004	199.6307
4	416	0.0015	175.7225	2.8353e-004	192.5072
5	832	0.0030	168.7776	5.5219e-004	185.8414
6	1664	0.0061	161.8786	0.0011	178.9962
7	3328	0.0121	154.9706	0.0022	172.0721
8	6656	0.0241	148.0605	0.0044	165.1280
9	13312	0.0484	141.1045	0.0087	158.3200
10	26624	0.0969	134.1704	0.0174	151.3625
	5319.6	**0.0193**	**165.3032**	**0.0035**	**182.4797**

Table 3: Obtained efficiency parameters

Message number	Length(byte)	LSB efficiency parameters		Proposed efficiency parameters	
		HT (second)	ET (second)	HT (second(	ET (second)
1	52	0.2070	0.0820	0.0980	0.0090
2	104	0.2080	0.0860	0.0990	0.0120
3	208	0.2120	0.0880	0.0993	0.0130
4	416	0.2133	0.0890	0.0997	0.0134
5	832	0.2490	0.0900	0.1037	0.0139
6	1664	0.2520	0.0904	0.1050	0.0170
7	3328	0.2530	0.0906	0.1069	0.0260
8	6656	0.2560	0.0909	0.1090	0.0440
9	13312	0.2670	0.1050	0.1330	0.0840
10	26624	0.2810	0.1340	0.1670	0.1540
Average	**5319.6**	**0.2398**	**0.0946**	**0.1121**	**0.0386**

From tables 2 and 3 we can see that the proposed method improved the efficiency and quality parameter of the LSB method, this is can be seen in figures 13 and 14.

International Journal of Scientific Engineering and Science
Volume 6, Issue 1, pp. 49-55, 2022. ISSN (Online): 2456-7361

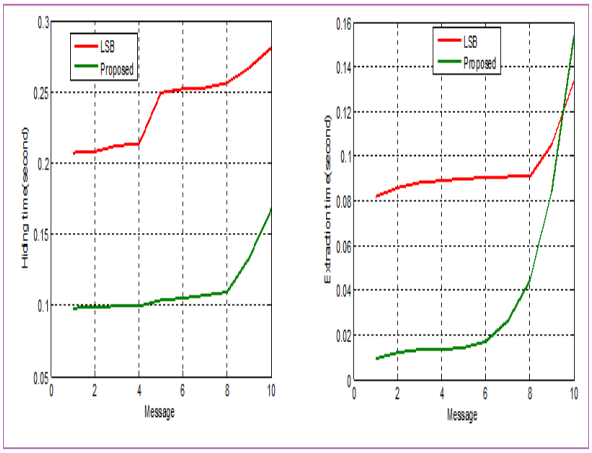


Figure 13: LSB and proposed method efficiency parameters comparisons

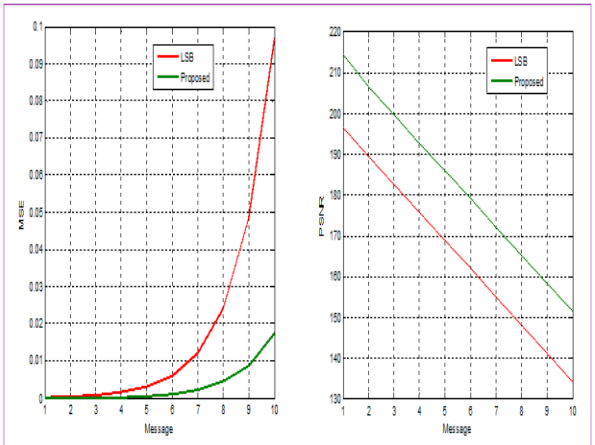


Figure 14: LSB and proposed method Quality parameters comparisons

The message:' Ziad Alqadi: Albalqa Applied University Amman Jordan' with length=52 was treated using the selected images and keeping image 1 as an image_key, table 4 and 5 show the obtained results

Table 4: Quality parameters for the selected message

Image number	LSB	PSNR	Hiding time	Extraction time
1	0.0013	177.2336	0.0363	0.0073
2	0.0027	170.0435	0.0372	0.0070
3	4.2245e-004	188.5196	0.0400	0.0068
4	4.0266e-005	212.0253	0.0918	0.0068
5	4.4381e-005	211.0523	0.1051	0.0068
6	0.0018	174.2584	0.0362	0.0068
7	4.3403e-004	188.2493	0.0404	0.0071
8	0.0013	177.3954	0.0360	0.0085
9	0.0014	176.4142	0.0368	0.0066
10	0.0013	177.2669	0.0367	0.0068
11	1.0370e-004	202.5650	0.0582	0.0068
12	3.4154e-005	213.6714	0.1024	0.0071

Table 5: Efficiency parameters for the selected message

Image number	LSB	PSNR	Hiding time	Extraction time
1	0.0064	161.3651	0.0537	0.0216
2	0.0139	153.5551	0.0404	0.0205
3	6.8673e-004	183.6610	0.1160	0.0238
4	2.1962e-004	195.0616	0.9523	0.0741
5	2.1867e-004	195.1049	0.7741	0.0714
6	0.0068	160.7505	0.5435	0.2740
7	6.8673e-004	183.6610	0.1159	0.0227
8	0.0035	167.5165	0.0533	0.0196
9	0.0065	161.1781	0.0636	0.0198
10	0.0070	160.4765	0.0556	0.0197
11	3.9418e-004	189.2123	0.3623	0.0399
12	1.8875e-004	196.5762	1.0893	0.1065

From table 4 and 5 we can see that it is better to use a covering image with big size, this will enhance the quality parameters without too much affecting the process efficiency.

The proposed method can be used to protect short and long messages, keeping the quality and the efficiency parameters acceptable, the obtained results shown in table 6 and figure 15 prove this.

Table 6: Results for long messages

Message size (K byte)	MSE	PSNR	Hiding time	Extraction time
1	6.6953e-004	183.9147	0.1042	0.0115
10	0.0067	160.8764	0.1146	0.0525
20	0.0134	153.9443	0.1368	0.1037
30	0.0201	149.9069	0.1407	0.1486
40	0.0268	147.0363	0.1721	0.2038
50	0.0335	144.8009	0.1744	0.2492
60	0.0402	142.9697	0.1879	0.2964
70	0.0468	141.4422	0.2246	0.3445
80	0.0535	140.1081	0.2258	0.3751
90	0.0602	138.9196	0.2590	0.4249

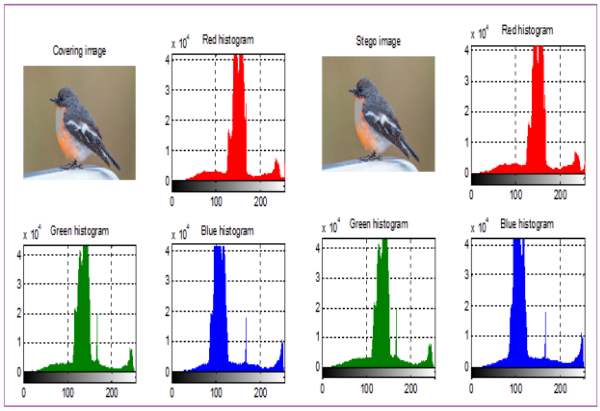


Figure 15: Covering and stego images for hiding a 90 K bytes' message

V. CONCLUSION

A method of combining data steganography and data cryptography was introduced. This method will provide an excellent protection to secure secret messages with any length (short and long secret messages). The protection can be achieved by using secret image_key to generate the PK necessary for the encryption-decryption phases, this image can suit any message with any length and it can be easily replaced by another image any time when the need arises. The proposed method uses simple operation to apply data hiding and data extraction. The proposed method was implemented and it was shown that the proposed method improves the values of the quality and efficiency parameters comparing with LSB method.

REFERENCES

[1] Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 – 62.
[2] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.
[3] Akram A. Moustafa and Ziad 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 5 (5): 355-362, 2009.
[4] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
[5] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.
[6] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.
[7] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.
[8] Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.
[9] A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.
[10] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.
[11] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, 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, 2018.
[12] Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.
[13] M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.
[14] M. Juneja, P. S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.
[15] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6 ISSN 2281-2911.
[16] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A Comparison Between Parallel And Segmentation Methods Used For Image Encryption-Decryption, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 2016.
[17] Z.A. Alqadi, A. Abu-Jazzar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.
[18] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.
[19] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.
[20] Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.
[21] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata: Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975 – 8887). Volume 153 – No2, November 2016.
[22] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.
[23] Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.
[24] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.
[25] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.
[26] Rashad J. Rasras, Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 14-26.
[27] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh; A Novel Based on Image Blocking Method to Encrypt-Decrypt Color; International Journal On Informatics Visualization Vol 3, (2019)
[28] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A Modified Lbp Method To Extract Features From Color Images", Journal of Theoretical and Applied Information Technology (JATIT), Vol.96. No 10, 2018.
[29] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher, "A novel Zero-error Method to Create a Secret Tag for an Image", Journal of Theoretical and Applied Information Technology (JATIT), Vol.96. No 13, 2018.pp: 4081-4091.
[30] J. Al-Azzeh, B. Zahran, Z. Alqadi," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.
[31] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.
[32] Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.