Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 8, August 2022, pg.22 – 44

Modified LSB2 Steganography Method to Secure the Embedded Secret Message

Namer Ali Aletawi; Mansour A. Abu Sameha; Prof. Ziad Alqadi
Albalqa Applied University, Jordan Amman
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i08.003

Abstract:
LSB2 method of data steganography is a popular method of secret data hiding, this method is simple and capable of hiding long messages in a covering color image. LSB2 is not secure and it cannot protect the embedded secret message from being hacked. In this research paper a modified LSB2 method will be proposed, this method will solve the security issues by using a secret private key. This key will contain 8 components and will be used to rearrange the sequence of bits hiding in the covering image. The proposed method will deal with the hiding process by selecting the first bits of the message characters, the seconds and so on. An extra task will be added to LSB2 method; this task will perform the necessary substitution of the message binary matrix according to the contents pf the PK. The PK key be easily changed when the need arises without modifying the proposed algorithm.
The proposed method will be implemented using various messages and various covering images. The obtained results will be analyzed using various types of data analysis to prove the efficiency of data steganography. A quality analysis will be performed to prove the quality of the stego image, and speed analysis will be performed to prove the optimized throughputs provided by the proposed method.
Keywords: Steganography, PK, stego image, covering image, secret message, MSE, PSNR, CC, NSCR, throughput.

© 2022, IJCSMC All Rights Reserved

Introduction

Digital color image [1-6] is a huge data container, and it usually it has a huge size which can be easily deployed for many applications such hiding secret data in it. Digital color image is represented by a 3D matrix, one 2D matrix for each color as shown in figure 1 [7-14] . Each color can be processed separately, and it can be easily extracted as shown in figure 2. The pixel values are within the range 0 to 255, these values match the ASCII values of any secret message, so the pixel values can be easily used to represent the ASCII charters as shown in figure 3 [15-22].

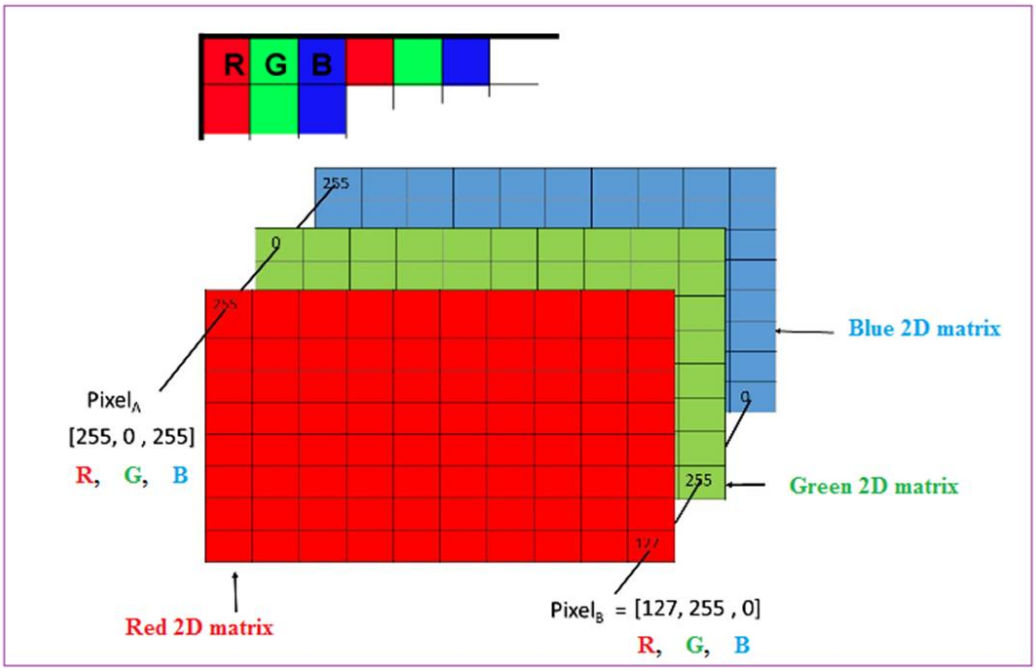

Figure 1: Color image representation

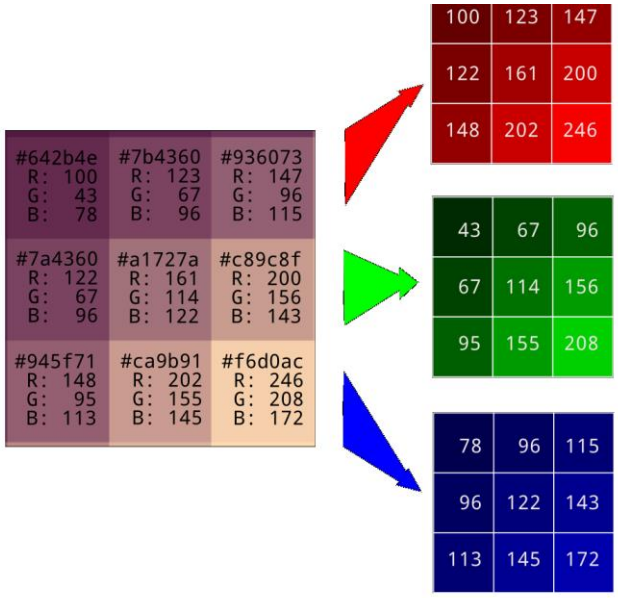

Figure 2: Color image matrices

© 2022, IJCSMC All Rights Reserved

Figure 3: Color pixels values

Data steganography as shown in figure 4 is a process of hiding (embedding) secret data in a digital media. Due to the big size of color image, it is preferable to use a color image as a covering media. The image holding the message is called stego image [48-55].

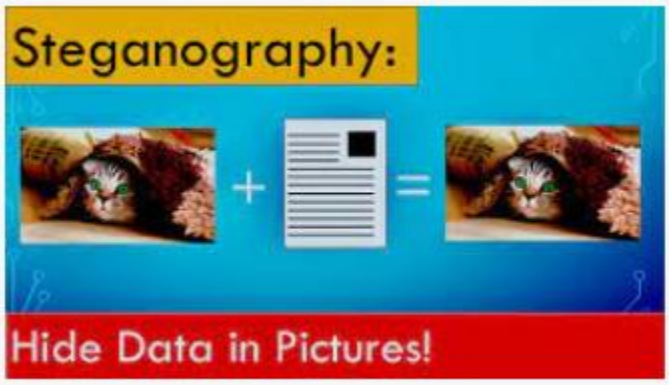

Figure 4: Data steganography

Message hiding must keep the stego image closed to the covering image, the changes in the stego image must not be noticed by human eyes, and here the mean square error between the covering image and the stego one must be very low [23-30].

Many methods are recently used for data steganography; most of these methods are based on least significant bit (LSB) and LSB2 methods of data steganography.

LSB method reserves 8 bytes from the covering image to hide one character from the secret message. The standard LSB method insert the message into the covering image character by character and it is very simple to implement.

© 2022, IJCSMC All Rights Reserved

LSB method adds minor changes to the covering bytes and the changes in each byte range from -1 to +1, these changes in the colors can not be noticed by human eyes, and the MSE between the covering and stego images will be low. In LSB method both the covering image and the secret message must be converted to binary, then the binary message will replace the least significant bits of the associated bytes in the covering image, figure 5 and 6 show an examples of message hiding using LSB method [32-40].

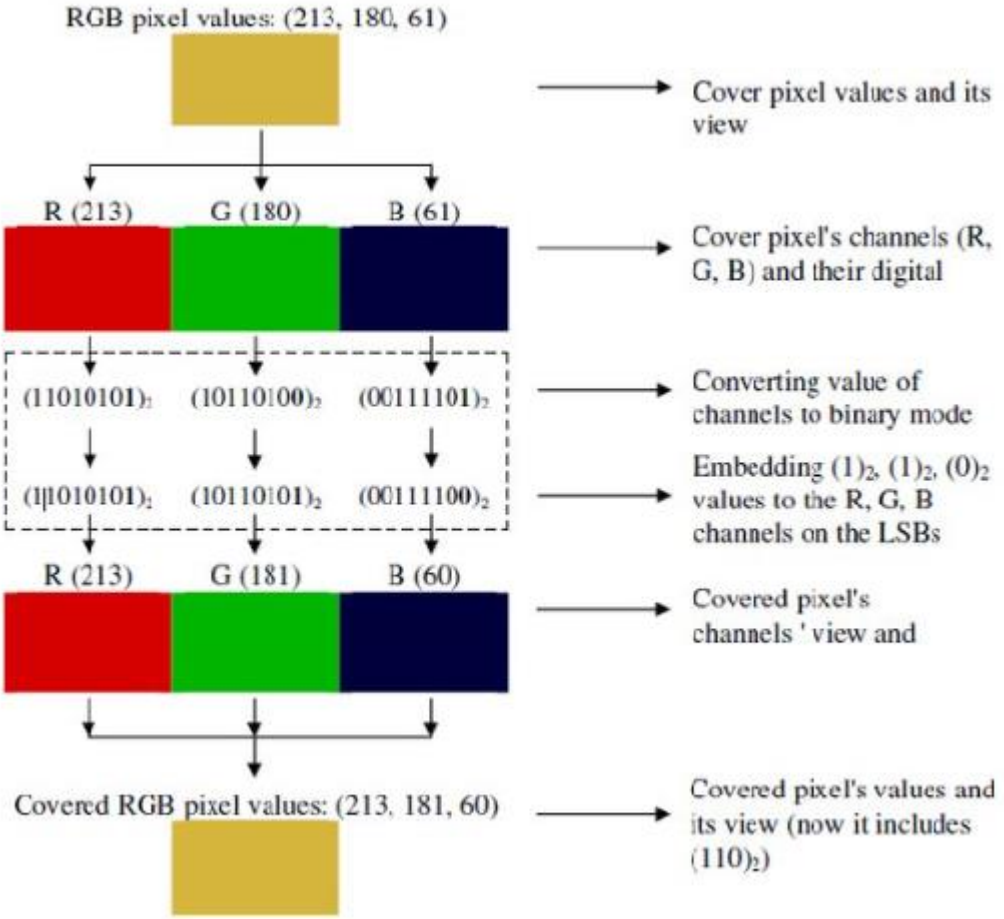

Figure 5: Message hiding using LSB method

© 2022, IJCSMC All Rights Reserved

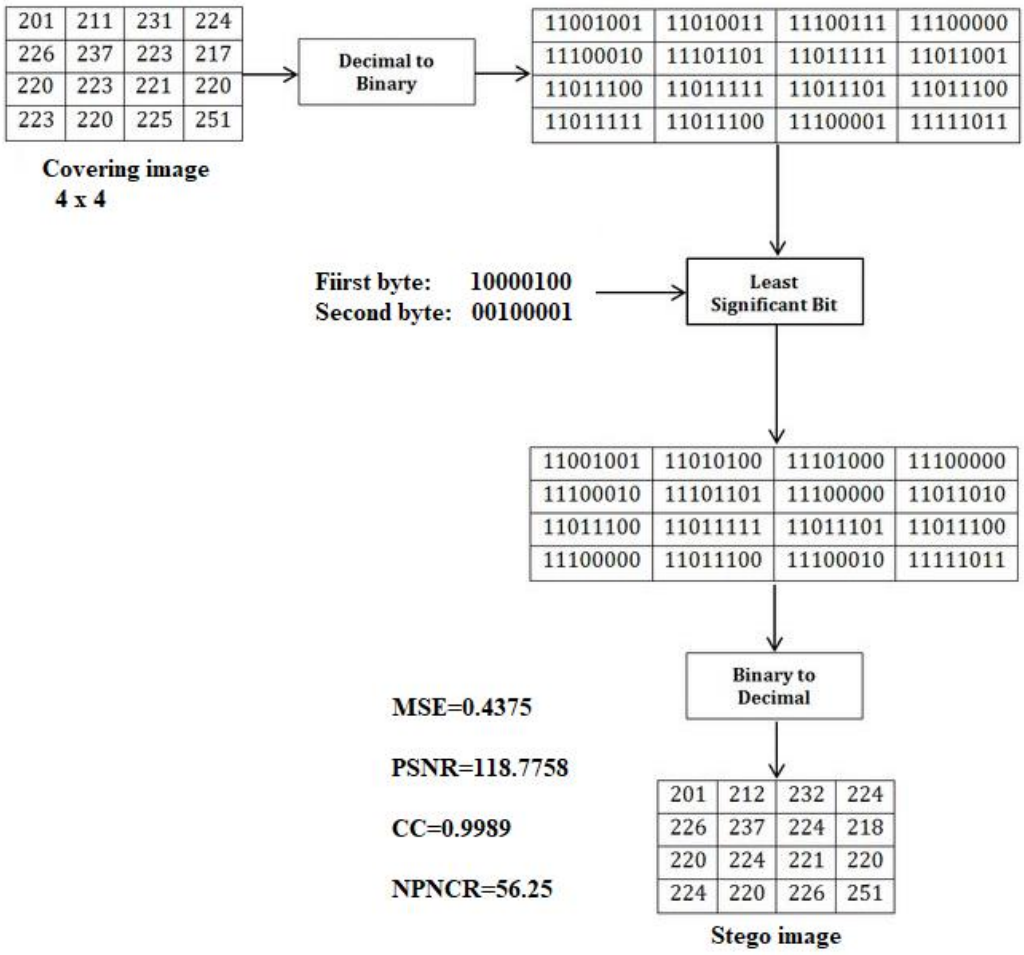

Figure 6: LSB message hiding example

The second popular method of data steganography is LSB2 method, this method reserves 4 bytes from the covering image to hide one character from the secret message as shown in figure 7.

LSB2 method doubles the capacity of hiding process, making the color image capable to hide very long messages; here the maximum message length will equal the images size in bytes divided by 4.

LSB2 methods adds minor changes to the image after applying the process of hiding, these changes are range from -3 to +3, because 2 LSB in the covering image bytes are to be replaced by 2 bits from the secret message character.

LSB2 method is very simple to implement and it provides good quality and performance, but it is not secure. Anyone with good programming experience can extract the message from the stego image, knowing that this image is holding a secret data.

© 2022, IJCSMC All Rights Reserved

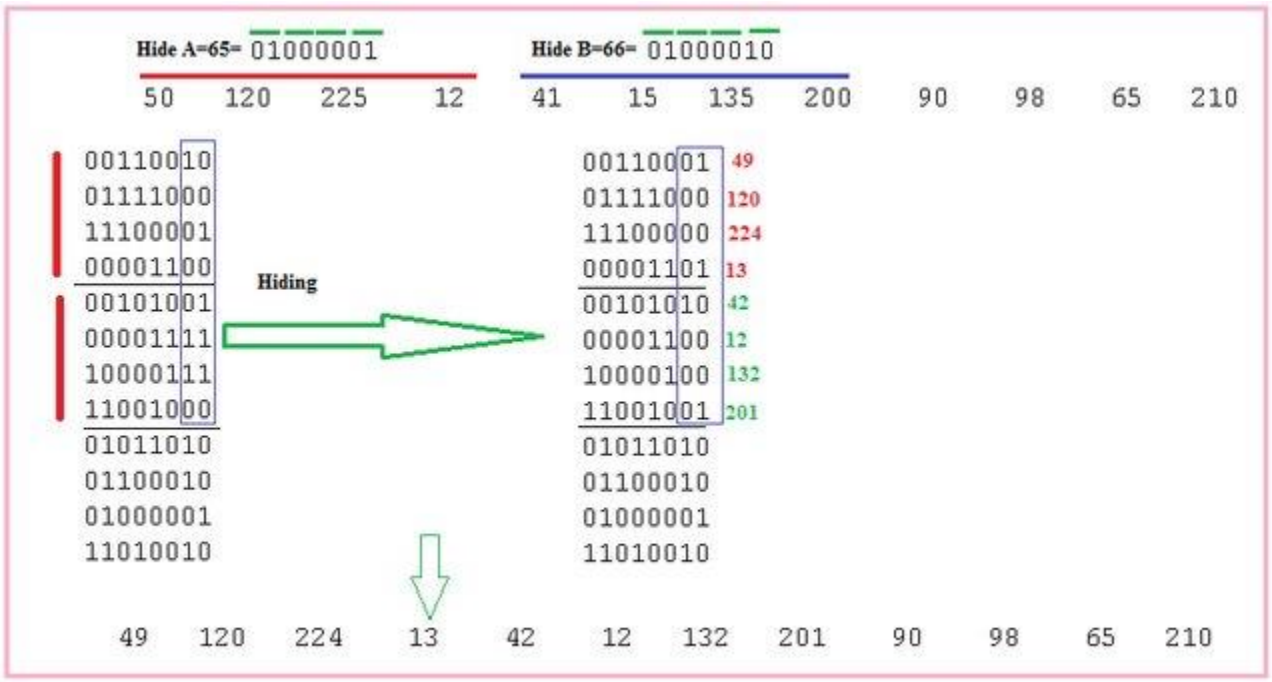

Figure 7: LSB2 data hiding

The Proposed Method

The process of arranging the data of the secret message to be hidden in the digital image is not important as long as we can retrieve the same secret message. Therefore, the arrangement process can be controlled to shorten the execution time and thus increase the speed of the hiding and retrieval process.

The LSB2 method of data steganography reserves 4 consecutive bytes from the covering image to hold one character of the secret message, for each character in the secret message the following operations must be performed (see figure 8):

- Convert the character to decimal
- Convert the decimal value of the character to binary
- Reshape the binary value into 4 by 2 matrix
- Insert the reshaped matrix in the associated 4 bytes of the covering image.

© 2022, IJCSMC All Rights Reserved

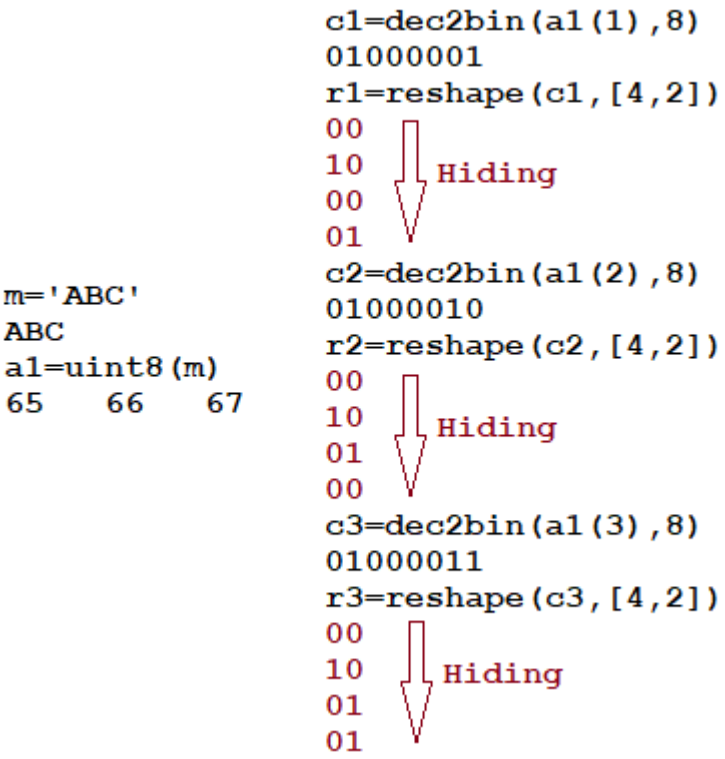

Figure 8: LSB2 data hiding

To speed up the process of data hiding and extracting a modified LSB2 (MLSB2) method is proposed. This method is based on creating character binary matrix, this matrix is a 2D matrix, one row for each characters and 8 columns for the binary value of the character as shown in figure 9.
The character binary matrix must be reshaped to 2 columns matrix, this matrix must replace the associated 2 LSB in the covering image bytes. Using this modification, the MLSB2 of data hiding can be implemented as shown in figure 10 applying the following steps:

1) Get the message and the message length (L)
2) Convert the message to decimal
3) Get the message binary matrix by converting the decimal message to binary
4) Reshape the message binary matrix to two columns matrix
5) Get a part of reshaped to one row covering image equal to L*4
6) Convert the covering image part to binary
7) Insert the message 2 column matrix in the covering image
8) Convert the image part to decimal
9) Fix the decimals in the stego image

© 2022, IJCSMC All Rights Reserved

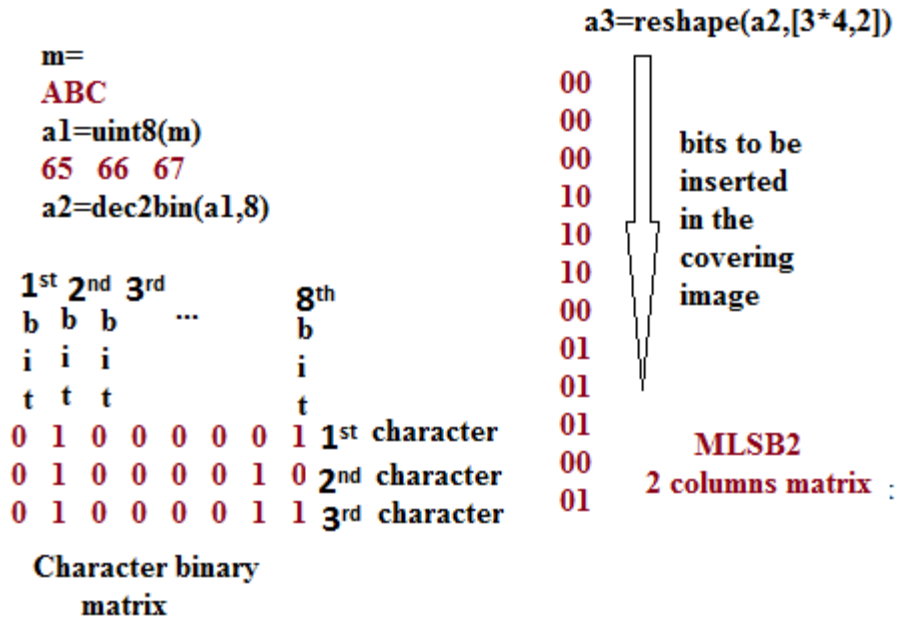

Figure 9: MLSB2 requirement

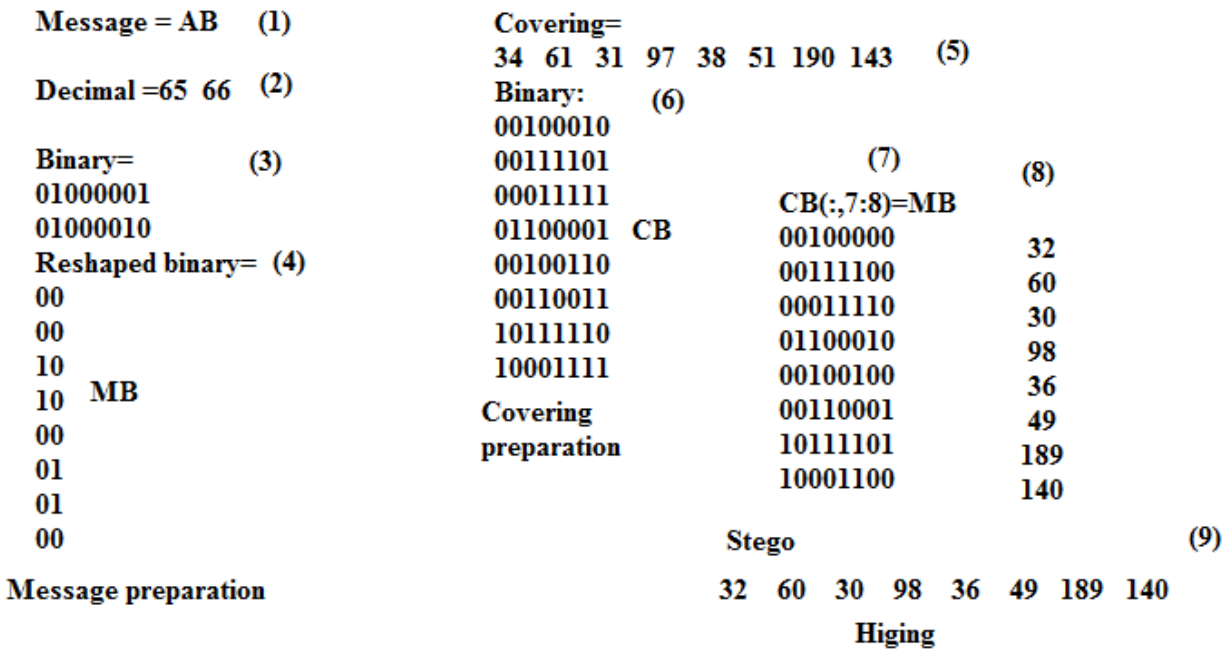

Figure 10: MLSB2 data hiding

© 2022, IJCSMC All Rights Reserved

The process of data extraction can be implemented applying the following steps (see figure 11):

1) Get a part from the reshaped stego image equal L*4
2) Convert the part to binary
3) From the binary part extract all the 2 LSBs
4) Reshape the obtained 2 columns matrix to 8 columns
5) Convert the matrix to decimal
6) Convert the decimal to character

```
a=stego  (1)
32  60  30  98  36  49 189 140

a1=dec2bin(a,8) (2)
  00100000
  00111100
  00011110
  01100010
  00100100
  00110001
  10111101
  10001100

      (3)
b=a1(:,7:8)
00
00
10
10
00
01
01
00

        (4)
b1=reshape(b,[2,8])
01000001
01000010

b2=bin2dec(b1)  (5)
     65
     66

b3=b2'        (6)
     65     66

b4=char(b3)  (7)
AB
```

Figure 11: MLSB2 extracting process

The MLSB2 method is not secure; to protect the hidden message a private key (see figure 12) can be used to rearrange the character binary message as show in figure 13. The PK contains 8 components; each component has a value within the range 1 to 8. This PK will add a necessary security to the method and it provides 8^8 combinations, and the key space will equal 16,777,216.

© 2022, IJCSMC All Rights Reserved

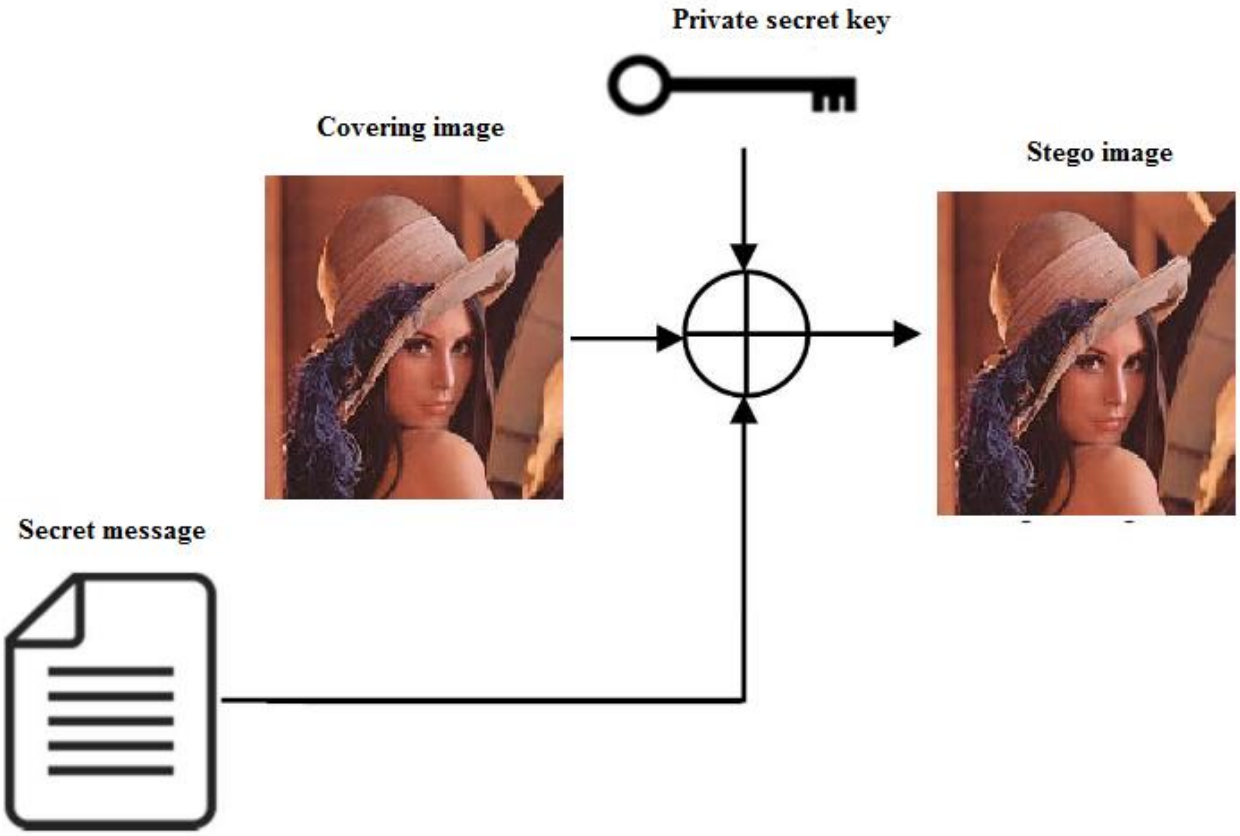

Figure 12: Using PK to secure MLSB2 method

```
a=message
   AB          (1)

a1=uint8(a) (2)
  65    66

a2=dec2bin(a1,8)  (3)
01000001
01000010

   PK=            (4)
   57283461

a3(:,1)=a2(:,5);
a3(:,2)=a2(:,7);
a3(:,3)=a2(:,2);
a3(:,4)=a2(:,8);
a3(:,5)=a2(:,3);
a3(:,6)=a2(:,4);
a3(:,7)=a2(:,6);
a3(:,8)=a2(:,1);
```

(5)

```
a3 =
 00110000
 01100000
```

(6)

```
a4=reshape(a3,[8,2])
00
00
00
10
10
10
10
00
```

```
b=covering  (7)
34  61  31  97  38  51  190  143

b1=dec2bin(b,8) (8)
00100010
00111101
00011111
01100001
00100110
00110011
10111110
10001111
```

(9)

```
b1(:,7:8)=a4
00100000
00111100
00011100
01100010
00100110
00110010
10111110
10001100
```

(10)

```
b2=bin2dec(b1)
     32
     60
     28
     98
     38
     50
    190
    140

b3=b2'   (11)
Stego=
32   60   28   98   38   50  190  140
```

Figure 13: MLSB2 using PK

© 2022, IJCSMC All Rights Reserved

The following code can be easily used to apply data hiding using MLSB2 method:

```
in=imread('C:\Users\Dr.Tayseer\Desktop\drziad\MAVAV\a12.jpg');
[n1 n2 n3]=size(in);ss=n1*n2*n3;
m='Ziad Alqadi Albalqa Amman Jordan Steganography';
L=length(m);
a=reshape(in,[1,n1*n2*n3]);
tic
m1=uint8(m);
m22=dec2bin(m1,8);
m2(:,1)=m22(:,3);
m2(:,2)=m22(:,5);
m2(:,3)=m22(:,2);
m2(:,4)=m22(:,7);
m2(:,5)=m22(:,1);
m2(:,6)=m22(:,4);
m2(:,7)=m22(:,8);
m2(:,8)=m22(:,6);
a1=a(1,1:L*4);
a2=dec2bin(a1,8);
m3=reshape(m2,[L*4,2]);
a2(:,7:8)=m3;
a3=bin2dec(a2)';
a(1,1:L*4)=a3;
a4=reshape(a,[n1 n2 n3]);
ht=toc;
```

The data extracting must use the PK in reverse form as shown in figure 14:

```
(1)
b3=stego
32   60   28   98   38   50 190 140

(2)
b4=dec2bin(b3,8)
00100000
00111100
00011100
01100010
00100110
00110010
10111110
10001100

(3)
b5=b4(:,7:8)
00
00
00
10
10
10
10
00

(4)
b6=reshape(b5,[2,8])
00110000
01100000

PK:      (5)
57283461

(6)
b7(:,1)=b6(:,8);
b7(:,2)=b6(:,3);
b7(:,3)=b6(:,5);
b7(:,4)=b6(:,6);
b7(:,5)=b6(:,1);
b7(:,6)=b6(:,7);
b7(:,7)=b6(:,2);
b7(:,8)=b6(:,4);

b7 =
01000001
01000010

b8=bin2dec(b7) (7)
    65
    66

b9=b8'      (8)
65    66
b10=char(b9) (9)
AB
```

Figure 14: MLSB2 extraction using PK

© 2022, IJCSMC All Rights Reserved

The following code can be easily used to apply data extracting using MLSB2 method:

```
%Extracting
tic
a5=reshape(a4,[1,n1*n2*n3]);
a6=a5(1,1:L*4);
a7=dec2bin(a6,8);
m45=a7(:,7:8);
m44=reshape(m45,[L 8]);
m4(:,1)=m44(:,5);
m4(:,2)=m44(:,3);
m4(:,3)=m44(:,1);
m4(:,4)=m44(:,6);
m4(:,5)=m44(:,2);
m4(:,6)=m44(:,8);
m4(:,7)=m44(:,4);
m4(:,8)=m44(:,7);
m5=reshape(m4,[L,8]);
m6=bin2dec(m5)';
et=toc;
m7=char(m6)
```

Implementation and Experimental Results

The stego image must has a good quality [38-48], it must be closed to the covering image, the quality of the stego image can be measures visually or/and by calculating MSE, PSN, CC, and NSCR between the covering and the stego images.

(1) Quality between two images can be measured by Mean square error (MSE) and peak signal to noise ratio (PSNR), high value of MSE and low value of PSNR points to the low quality, while low MSE and high PSNR points to the high quality. A good method of data steganography must provide a high quality. MSE and PSNR can be calculated using equations 1 and 2:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \text{dB}, \quad (1)$$

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2, \quad (2)$$

Where: MAX is the maximum possible value of gray value (In our case the maximum value is 255), *N* is the total number of samples, xi and yi are the corresponding sample values of the covering and stego images.

(2) Correlation Analysis

Correlation coefficient expresses the dependency between corresponding sample values. This is another statistical evaluation for testing the quality of the algorithm of data steganography. Calculating correlation coefficient determines the level of correlation between two files and the correlation coefficient is always in range [−1,1]. Values between |1–0.7| is considered as strong correlation (samples from the source files are similar to samples from the encrypted file), correlation between |0.7–0.3| is considered as medium correlation and values between |0.3–0| is considered as weak correlation.

© 2022, IJCSMC All Rights Reserved

Correlation coefficient can be calculated using equation 3:
N is the total number of samples, xi and yi are the sample values of the covering and stego files, $\bar{x}$ and $\bar{y}$ are the mean values of samples, and finally cov (x, y) is covariance between both files.

$$\mathbf{CC}_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (3)$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2,$$

$$cov(x,y) = \sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}),$$

(3) Number of Sample Change Rate

Number of sample change rate (NSCR) is robustness test for establishing the quality of data steganography algorithms. The purpose of the test is to compare the corresponding sample values of the covering and stego image files and to show the difference in percent. NSCR can be calculated using equation 6:

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \quad (4)$$

where

$$D_i = \begin{cases} 1, x_i \neq y_i \\ 0, Otherwise \end{cases}$$

© 2022, IJCSMC All Rights Reserved

A message of length 500 character was hidden in a big covering image with size =6119256 bytes, figures 15 and 16 show the covering and the stego images:

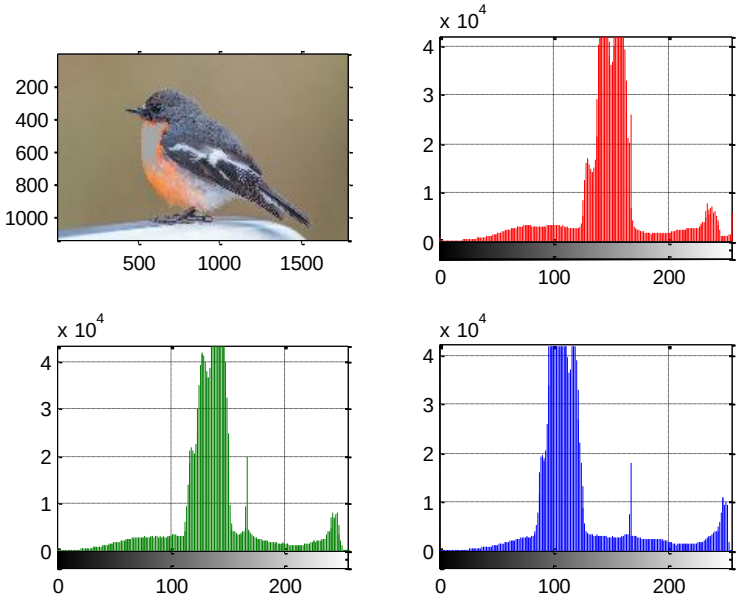

Figure 15: Big covering image

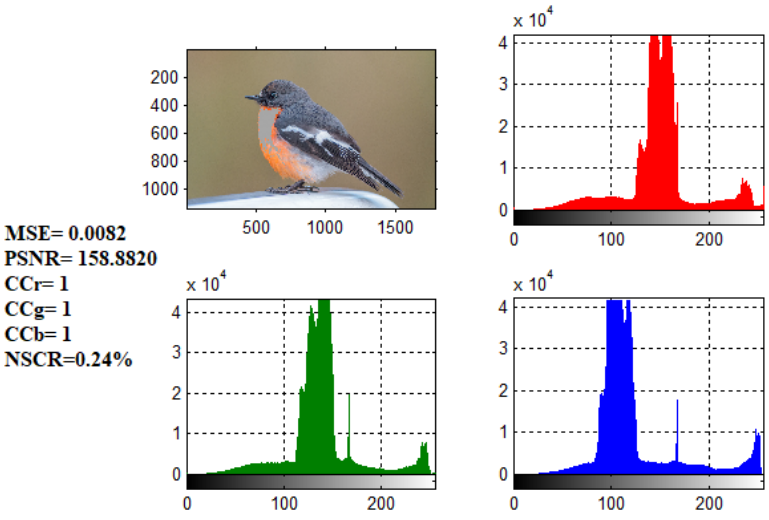

Figure 16: Big stego image

© 2022, IJCSMC All Rights Reserved

The same message was hidden in a smaller covering image with size = 150975, figure 17 and 18 show the covering and stego images:

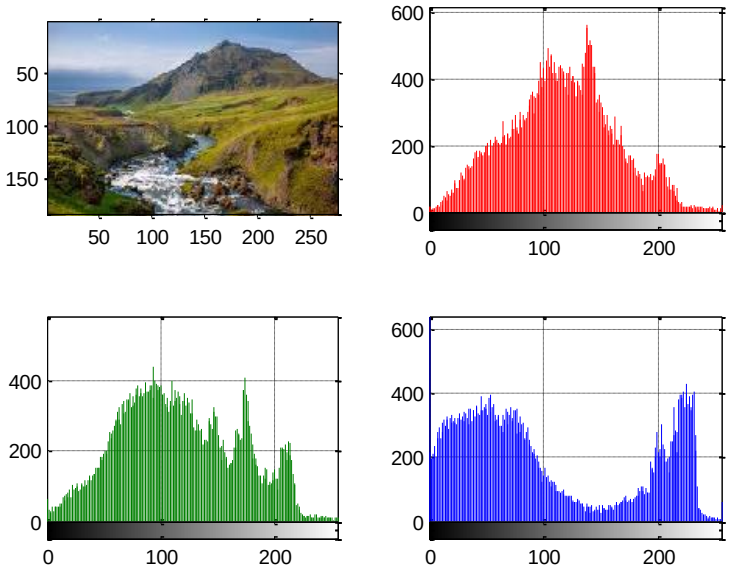

Figure 17: Smaller covering image

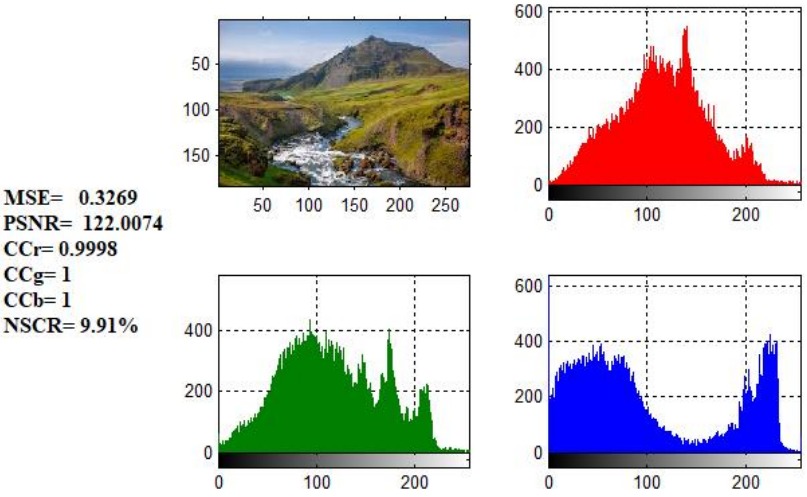

Figure 18: Smaller stego image

Visually from the previous figures we can see that the qualities of the stego images are acceptable, and according to the calculated quality parameters we can recommend using covering image with big size, this image can be easily used to hide short and long messages keeping the process of steganography efficient.

© 2022, IJCSMC All Rights Reserved

The image shown in figure 15 was selected as a covering image; various short messages were hidden using this image, tables 1 and 2 show the obtained values of the quality parameters:

Table 1: Obtained values of MSE, PSNR and NSCR

Message length(byte)	MSE	PSNR	NSCR (%)
100	0.00015508	198.5407	0.47065
200	0.00032357	191.1863	0.98
400	0.00064207	184.3334	1.99
500	0.00085566	181.4617	0.0251
1000	0.0016	175.1812	0.0489
2000	0.0033	167.8447	0.0987
3000	0.0049	164.0661	0.1464
4000	0.0067	160.8737	0.1972
5000	0.0082	158.9078	0.24

Table 2: Obtained values of CCs

Message length(byte)	CCr	CCg	CCb
100	1	1	1
200	1	1	1
400	1	1	1
500	1	1	1
1000	1	1	1
2000	1	1	1
3000	1	1	1
4000	1	1	1
5000	1	1	1

From tables 1 and 2 we can see that the quality of the stego image is acceptable, the PSNR remain high even if the message length is long, PSNR will remain high and it is slowly decreased when increasing the message length as shown in figure 19.

© 2022, IJCSMC All Rights Reserved

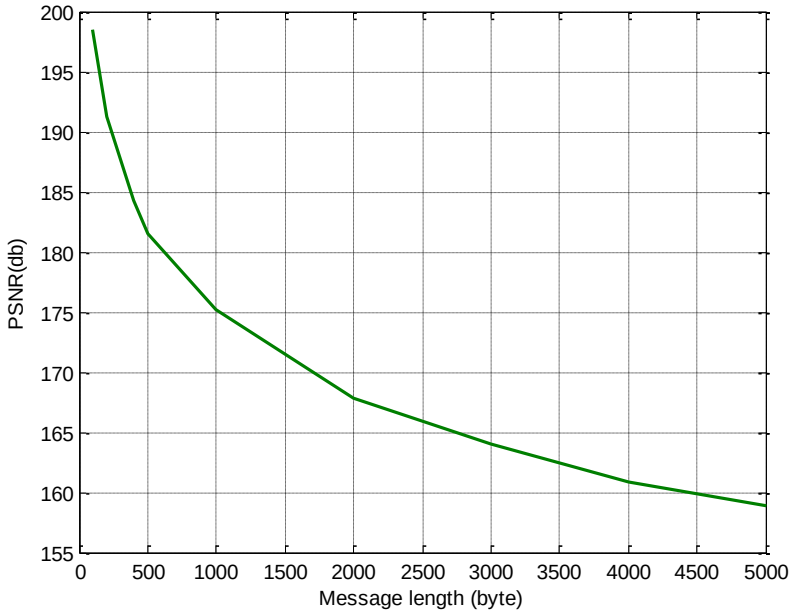

Figure 19: Message length VS PSNR

MLSB2 method provides a high capacity, the capacity will increase when increasing the covering image size, so it is recommended to use a covering image with big size, and this will provide the following advantages:

- Increasing the capacity of message steganography by allowing bedding a huge messages
- Keeping the quality of the stego image good even if we hide a huge message in the image.

Huge message were treated using MLSB2 method keeping the image with size equal 6119256 bytes as a covering image, tables 3 and 4 show the obtained quality parameters results:

Table 3: Obtained values of MSE, PSNR and NSCR for huge messages

Message length(K bytes)	MSE	PSNR	NSCR (%)
10	0.0168	151.6914	0.5021
20	0.0336	144.7690	1.0046
50	0.0829	135.7319	2.5077
100	0.1660	128.7802	5.0139
200	0.3353	121.7524	10.0496
300	0.5014	117.7278	15.0572
400	0.6694	114.8390	20.0909
500	0.8362	112.6147	25.1101
1000	1.6700	105.6971	50.1810

© 2022, IJCSMC All Rights Reserved

Table 4: Obtained values of CCs for huge messages

Message length(K byte)	CCr	CCg	CCb
10	1	1	1
20	1	1	1
50	0.9999	1	1
100	0.9998	1	1
200	0.9996	1	1
300	0.9994	1	1
400	0.9992	1	1
500	0.9990	1	1
1000	0.9990	0.9990	1

The results shown in tables 3 and 4 show that the quality parameters remain acceptable even if we hide a huge message in the covering image, figures 20 and 21 show the covering image and the stego image which holds a message with length equal 1 M bytes.

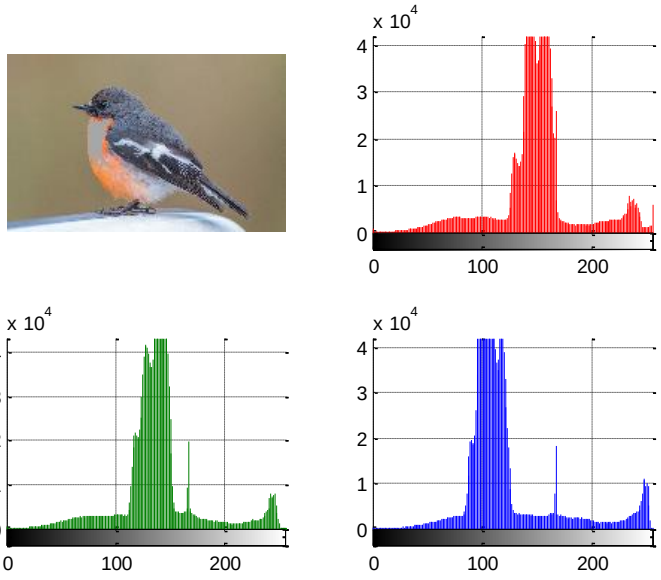

Figure 20: Covering image to hold huge message

© 2022, IJCSMC All Rights Reserved

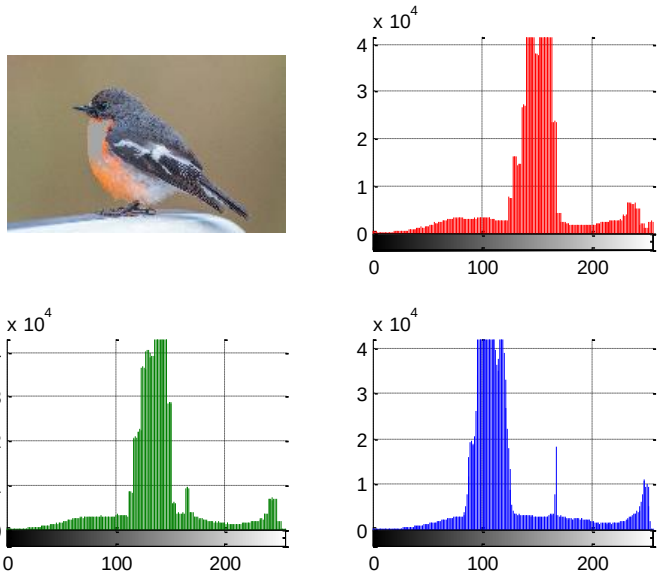

Figure 21: Stego image holding 1 M bytes message

The proposed MLSB2 method provides a good performance, the hiding and the extraction times are significantly small (there is a linear relationships between each time and the message size, see figure 22) and the average throughputs for data hiding and data extinction are high, tables (5 and 6) show the obtained performance parameters values for both medium and huge messages.

Table 5: Performance results for medium messages

Message length(byte)	HT(second)	ET(second)	HTP(K byte per second)	ETP(K byte per second)
100	0.0320	0.0023	3.0481	43.1802
200	0.0177	0.0028	11.0278	68.8957
400	0.1090	0.0120	3.5837	32.5521
500	0.0650	0.0060	7.5120	81.3802
1000	0.2680	0.0090	3.6439	108.5069
2000	0.2080	0.0150	9.3900	130.2083
3000	0.0760	0.0220	38.5485	133.1676
4000	0.0960	0.0280	40.6901	139.5089
5000	0.0944	0.0232	51.7266	210.1327
Average			18.7967	105.2814

© 2022, IJCSMC All Rights Reserved

Table 5: Performance results for long messages

Message length(K byte)	HT(second)	ET(second)	HTP(K byte per second)	ETP(K byte per second)
10	0.2150	0.0690	46.5116	144.9275
20	0.4120	0.1340	48.5437	149.2537
50	1.0120	0.3420	49.4071	146.1988
100	2.2470	0.6860	44.5038	145.7726
200	4.0820	1.3750	48.9956	145.4545
300	6.2650	2.1230	47.8851	141.3095
400	8.2480	2.7290	48.4966	146.5738
500	10.0580	3.3850	49.7117	147.7105
1000	20.4170	7.1620	48.9788	139.6258
Average			48.1149	145.2030

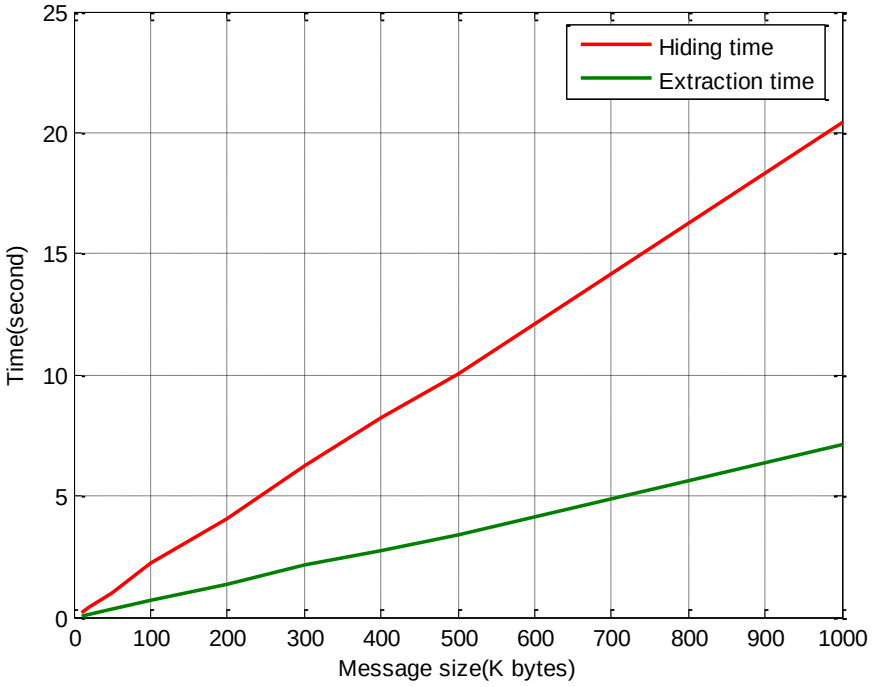

Figure 22: Hiding and extraction times VS message length

© 2022, IJCSMC All Rights Reserved

Conclusion

Simple and efficient modifications were added to LSB2 method of data steganography. These modifications kept LSB2 efficient and the quality of the stego image remain high. MLSB2 method used a private key to apply data hiding and data extraction; this key provided a necessary key space to protect the message steganography. The proposed MLSB2 method was implemented using various covering images and various messages, it was recommended to use a big in size covering image to maximize the capacity of MLSB2 method and to keep the quality parameters optimized. The obtained experimental results were used to calculate the quality parameters of the stego image (MSE, PSNR, CC, and NSCR), the obtained values for these parameters were good when using any message with any length (short, medium and long messages).

The performance of the proposed MLSB method was tested; the obtained results showed that the proposed method was efficient by providing a good throughput average and keeping the hiding and extracting time optimal.

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] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi , A Novel Methodology to Extract Voice Signal Features , International Journal of Computer Applications, Volume 179 – No.9, January 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.

© 2022, IJCSMC All Rights Reserved

[17] Z.A. Alqadi, A. Abu-Jazar (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] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad , Analysis of Color Image Features Extraction using Texture Methods , TELKOMNIKA, vol. 17, issue 3, 2018.

[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.

[33] Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.

[34] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[35] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 648-656, 2021.

[36] Ziad Alqadi Mua'ad Abu-Faraj , Khaled Aldebei, DEEP MACHINE LEARNING TO ENHANCE ANN PERFORMANCE: FINGERPRINT CLASSIFIER CASE STUDY, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, vol. 56, issue 6, pp. 686-694, 2021.

[37] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 451-458, 2021.

© 2022, IJCSMC All Rights Reserved

[38] Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.

[39] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[40] Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[41] Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.

[42] Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.

[43] Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.

[44] [43] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, B. Al-Ahmad, and Z. Alqadi, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," IEEE Access, vol. 10, pp. 69388- 69397, 2022, doi:10.1109/ACCESS.2022.3187317.

[45] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Experimental Analysis of Methods Used to Solve Linear Regression Models," CMC-Computers, Materials & Continua, vol. 72, no. 3, pp. 5699-5712, 2022, doi:10.32604/cmc.2022.027364. (Web of Science Indexed, Scopus Indexed).

[46] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi:10.3390/sym0664. (Web of Science Indexed, Scopus Indexed)

[47] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi:10.18280/ts.390117. (Web of Science Indexed, Scopus Indexed)

[48] M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89. (Web of Science Indexed)

[49] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61. (Web of Science Indexed)

[50] M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8. (Web of Science Indexed)

[51] M. Abu-Faraj, and M. Zubi, "Analysis and Implementation of Kidney Stones Detection by Applying Segmentation Techniques on Computerized Tomography Scans," Italian Journal of Pure and Applied Mathematics, iss. 43, pp. 590-602, 2020. (Scopus Indexed)

[52] Prof. Ziad Alqadi, Bits Substitution to Secure LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 8, pp. 9 – 21, 2022.

[53] Mohammad S. Khrisat Prof. Ziad Alqadi, Enhancing LSB Method Performance Using Secret Message Segmentation, International Journal of Computer Science and Network Security, vol. 22, issue 7, pp. 1-6, 2022.

[54] Hatim Ghazi Zaini and Ziad A. Alqadi Mohammad S. Khrisat, Adnan Manasreh, COVER IMAGE REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY, Journal of Engineering and Applied Sciences, vol. 17, issue 3, pp. 294-302, 2022.

[55] Mohamad K Abu Zalata, Mohamad T Barakat, Ziad A Alqadi, Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 1, pp. 182 – 193, 2022.

[56] Dr. Mohamad barakat Prof. Ziad Alqadi, IMAGE TRANSFORMATION TO INCREASE THE SECURITY LEVEL OF LBS METHOD OF DATA STEGANOGRAPHY, International Journal of Engineering Technology Research & Management, vol. 6, issue 1, pp. 42-53, 2022.

© 2022, IJCSMC All Rights Reserved