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.45 – 66

Two PKs to Protect LSB Method of Data Steganography

Prof. Ziad Alqadi
Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i08.004

Abstract: ***LSB method of data steganography is very popular and easy method of data hiding, but it si not secure. In this research paper a simple and easy modifications will be added to LSB method to increase the security level of data hiding. Two PKs will be used to protect the hidden secret message, the first PK1 will be generated using a selected parameter values to run CLMM, this key will be converted to form a lockup table to apply message encryption-decryption. The second PK2 will be used to apply bits' substitution of the character binary matrix, the two keys will provide a necessary key space, which can resist hacking attacks, the two keys will be sensitive to any minor changes in the PKs contents, any changes in the PKs values in the message retrieving phase will be considered as a hacking attempt.***

The proposed method will be implemented using various messages and various covering images, the obtained results will be analyzed, several types of results analysis will be performed to prove the quality, performance, security and sensitivity of the proposed method.

Keywords: Steganography, cryptography, PK, CK, CLMM, lockup table, MSE, PSNR, CC, NSCR, throughput.

Abbreviations

The following abbreviations were used in this research paper:

PK: private key

CK: Chaotic key

CLMM: Chaotic logistic map model

CBM: character binary matrix

© 2022, IJCSMC All Rights Reserved

CC: correlation coefficient

MSE: mean square error

NSCR: number of samples change ratio

PSNR: peak signal to noise ratio

Introduction

Steganography involves hiding sensitive information inside an ordinary [47-55], non-confidential file or message, so that it won't be discovered. Sensitive information will then be extracted from the normal file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption to mask or protect data.

Digital color image [1-10] is a huge data incubator; this data bank can be employed to apply various applications (such as message steganography) for the following reasons:

- Easy to obtain and without any cost.
- Digital color image can be represented by a 3D matrix (see figure 1) (one 2D matrix for each color: red, green and blue), and processing this matrix is very easy.
- Each color matrix can be easily extracted and treated separately.
- The pixels and the colors values fall in the range 0 to 255, and the same range is used to represent the ASCII values of the message characters [11-15].

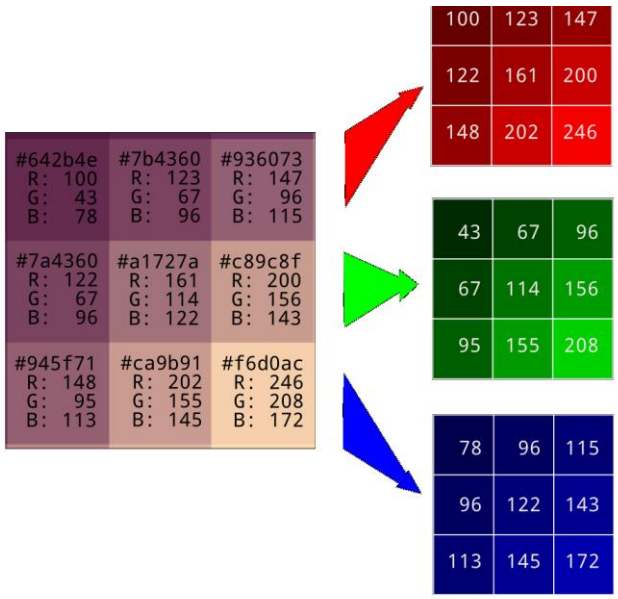

Figure 1: 3D color image matrix

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography [50-55].

The various terms used to describe image steganography include (see figure 2):

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.

© 2022, IJCSMC All Rights Reserved

- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

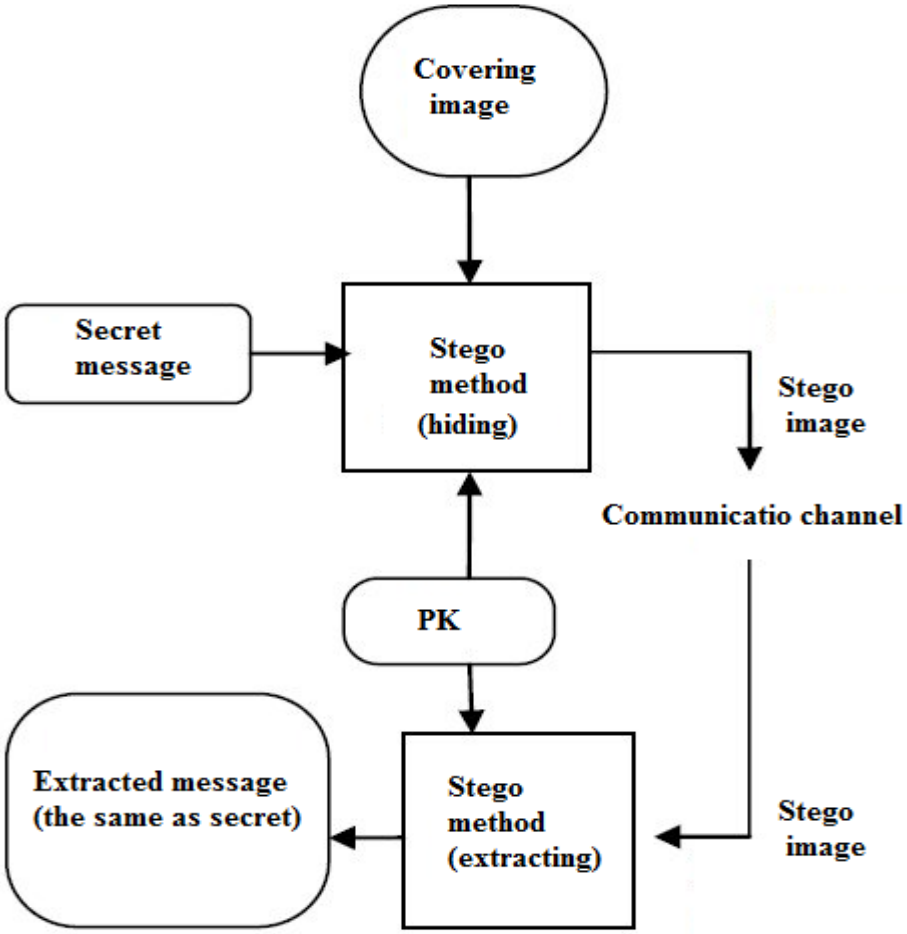

Figure 2: Stego model

It's fair to say that steganography and cryptography aim to shield messages and data from prying eyes at their most fundamental level. However, they employ an alternative means of security [16-24].
Information is converted into unintelligible ciphertext in cryptography. Someone intercepting this message could tell immediately that encryption was used. In contrast, steganography hides a message without altering its original format; table 1 shows the main differences between steganography and cryptography [25-30]:

Table 1: Steganography vs cryptography

Factor	Steganography	Cryptography
Explanation	It's a method to conceal the fact that communication is taking place	It's a method for making information unintelligible
Aim	Maintain communication security	Enable data protection
Key	Optional, but increases security when utilized	Necessary prerequisite

© 2022, IJCSMC All Rights Reserved

Data Visibility	No	Yes
Failure	Once hidden information is decoded, the data can be used by anyone	You can recover the original message from the ciphertext if you can access the decryption key
Data Structure	Does not modify the data's general structure (High quality of stego image)	Modifies the overall data structure (low quality of encrypted data)

The aim of this paper research is to add a security mechanism to LSB method of data steganography and provide a high level of hidden message protection by using two private keys. An encryption phase will be added to LSB method to encrypt the message before hiding using a lockup table generated by implementing a chaotic logistic map model (CLMM) based of selected values of chaotic parameters. The hiding process will base on LSB method of data hiding with a simple modification, another private key will be used here to apply binary matrix rearrangements before hiding [31-35].

The Proposed Method

The proposed method is a modification of least significant bit of data steganography (LSB). LSB method of data hiding is a simple and efficient method of hiding secret messages in covering color images and it can be implemented applying the following steps:

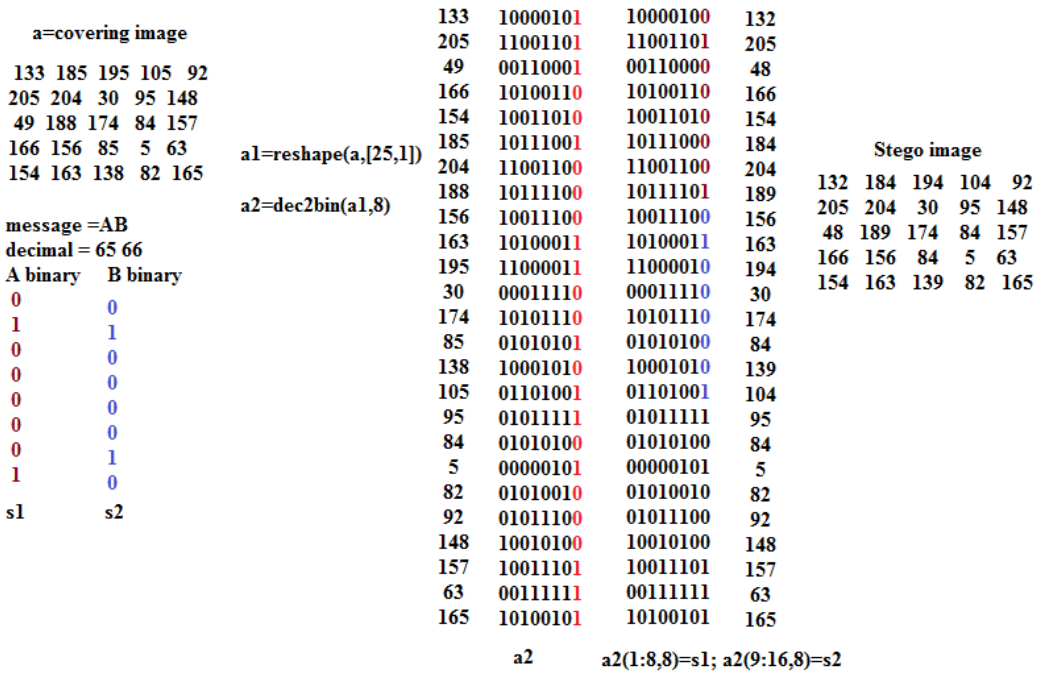

Figure 3: LSB hiding process

Hiding process:

- Get the message (see figure 3)
- Get the message length (L)

© 2022, IJCSMC All Rights Reserved

- Convert the message to decimal
- Get the covering image
- Reshape the covering image to one column matrix
- Convert the column matrix to binary(CBM)
- For each decimal character do the following
    - Convert the decimal character to binary
    - Store the binary value of the character in the associated LSBs of the CBM
- Convert CBM to decimal
- Reshape the results back to image to get the stego image

Extracting process

The extracting process can be implemented applying the following steps (see figure 4):

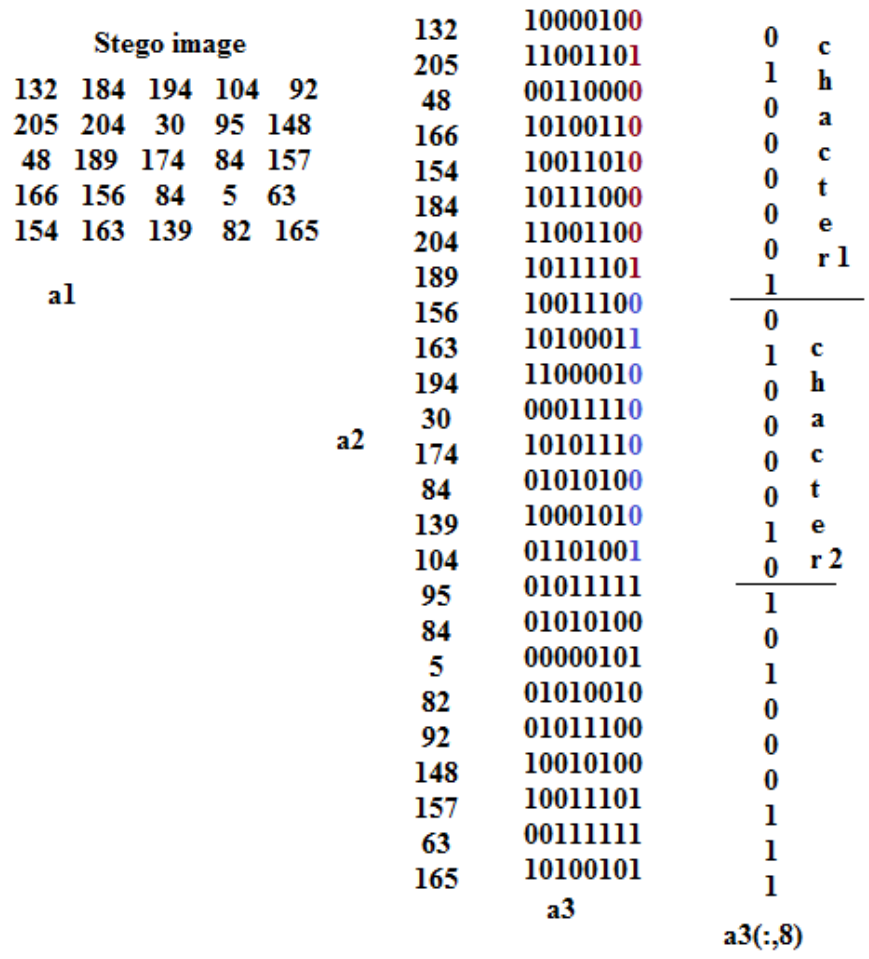

Figure 4: LSB extracting process

© 2022, IJCSMC All Rights Reserved

- Get the stego image
- Reshape the stego image into one column matrix
- Convert the column matrix to binary
- For each character do the following
    - Get the associated 8 LSBs from the binary matrix
    - Convert the binary results to decimal
    - Convert the decimal to character

The LSB method of data steganography produces a stego image with high quality, any modification in the image bytes will range from -1 to 1, these modifications make the colors closed to the covering colors, and the changes cannot be noticed by eyes. The capacity of LSB method depended on the covering image size and it is equal the image size divided by 8. Regardless the advantages of LSB method, this method is not secure, any third party will good programming experience can extract the message, knowing that LSB method was used to hide the secret message.

The proposed method will add a security mechanism to LSB method of data steganography; figure 5 shows the block diagram of the proposed method:

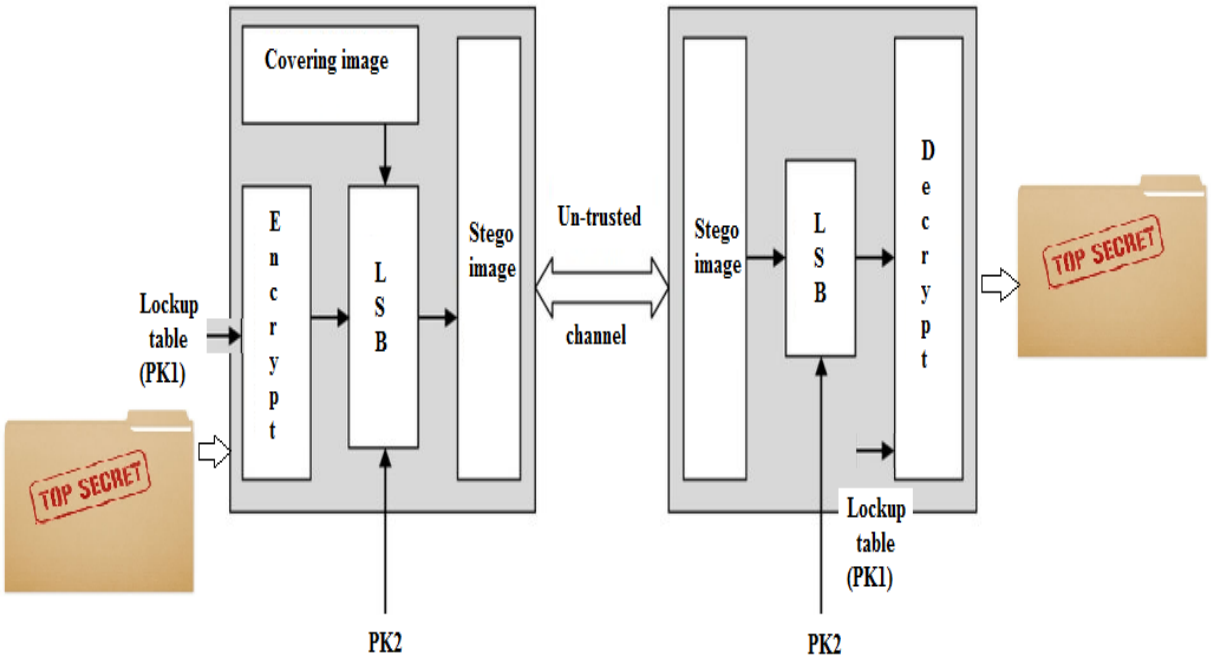

Figure 5: Proposed method diagram

© 2022, IJCSMC All Rights Reserved

The proposed method use two PKs, PK1 is used in the encryption-decryption phase, and PK2 is used in the hiding extracting phase. The proposed method is implemented using the following phase:

Encryption-decryption phase:

This phase use PK1 to generate a lockup table to be used to encrypt-decrypt the secret message. In this phase a chaotic logistic map model (CLMM) will be implemented using the contents of PK1, which contains the values of the chaotic parameters, these values are used to generate a chaotic key (CK) with 256 elements, the CK then will be converted to lockup table using the sort matlab function, below is the sequence of operations required to generate the needed lockup table.

```
R1=256;
%PK1
r1=3.95;x1=0.325;
for i=1:R1
        x1=r1*x1*(1-x1);
      %CK
       key1(i)=x1;

end
[notused,kk1] = sort(key1);
%Lockup table
kk1=kk1-1;
```

In the encryption phase the decimal value of the character is used as an index, and the character decimal value is replaced by the contents of the index in the lockup table to get the encrypted character decimal.
In the decryption phase, the encrypted character decimal is to be replaced by the index, where the decimal is located in the lockup table. Figure 6 shows a simplified example of applying encryption-decryption using lockup table:

```
R1=10;
r1=3.95;x1=0.325;
for i=1:R1
        x1=r1*x1*(1-x1);
      key1(i)=x1;
 end
[notused,kk1] = sort(key1);
kk1=kk1-1;
```

PK1=3.95, 0.325

CLK ⇨ 0.8665 0.4568 0.9801 0.0769 0.2803 0.7969 0.6392 0.9109 0.3206 0.8603

	0	1	2	3	4	5	6	7	8	9	index
IK ⇨	3	4	8	1	6	5	9	0	7	2	lockup table

Data to be encrypted:
0 0 7 8 9

3 3 0 7 2 encrypted data (data is index: encrypted is contents of index

0 0 7 8 9 decrypted:the index of encrypted data

Figure 6: Encryption_decryption using lockup table

Data hiding phase:
The proposed method data hiding apply hiding first bits of all characters, then second bits and so on, instead of hiding the message character by character (as in LSB method), this will save time and efforts, and the process of hiding will be implemented in burst way.

© 2022, IJCSMC All Rights Reserved

The process of data hiding can be implemented applying the following steps (see example in figure 7):

- Get the covering image
- Reshape the covering image into one row matrix.
- Get the encrypted message
- Get the message length (L)
- Convert the message to decimal
- Convert the decimal message to binary to obtain CBM
- Reshape CBM to one column matrix
- From the covering row matrix select a part of L*8 bytes
- Convert the part to binary
- Insert the message column in the LSBs of the image part
- Convert the image part to decimal
- Return the decimal part back to the image part
- Reshape the image row matrix to color matrix to get the stego image

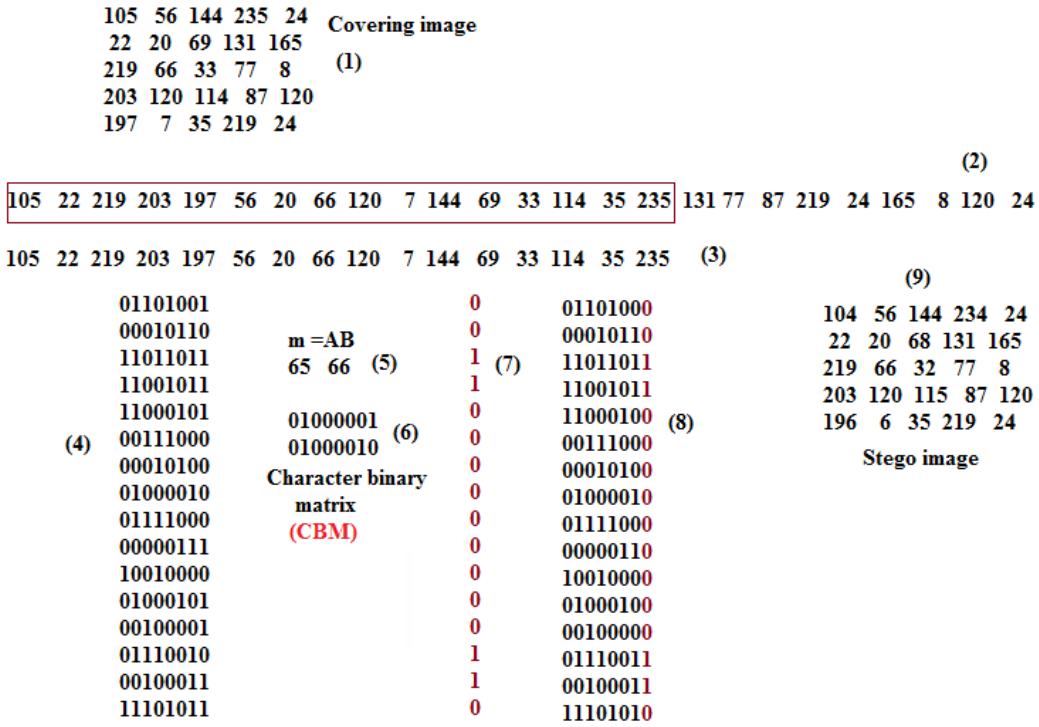

Figure 7: Hiding process

© 2022, IJCSMC All Rights Reserved

Extracting phase:

This phase as shown in figure 8 can be implemented applying the following steps:

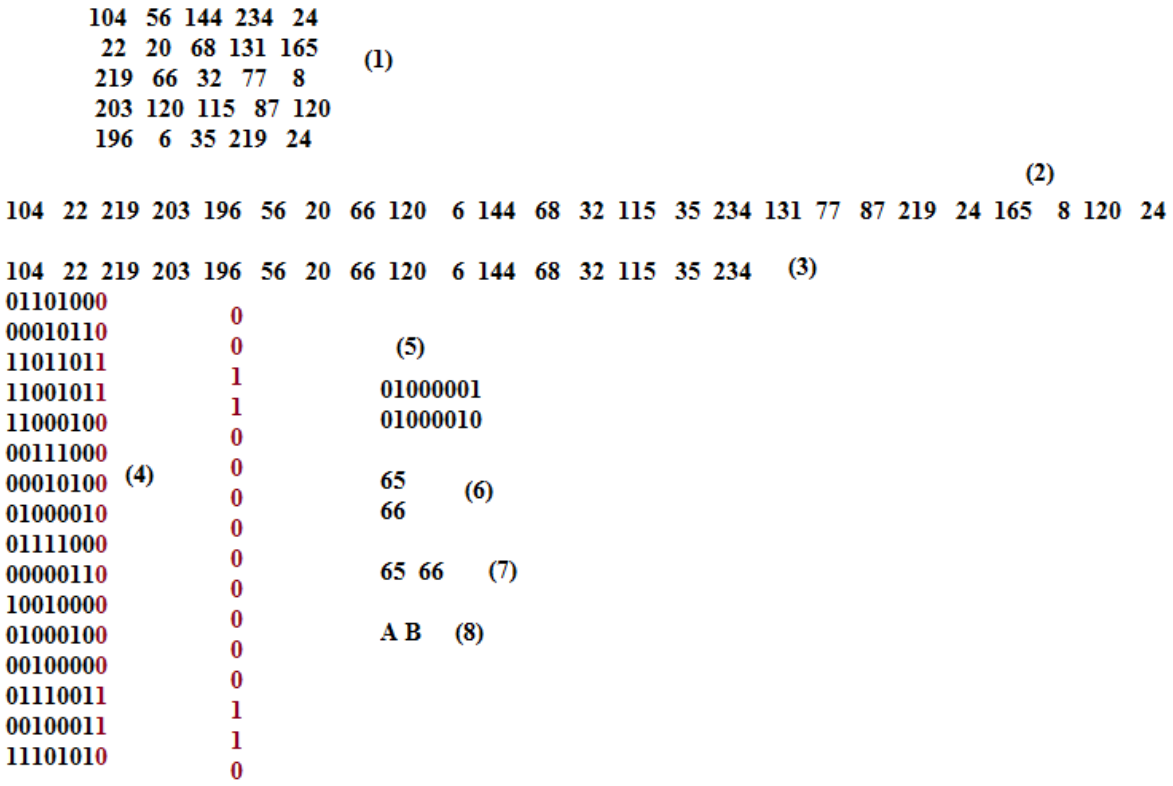

Figure 8: Extracting process

- Get the stego image
- Reshape the image to one row matrix
- Get a part from the row matrix equal L*8
- Convert the part to binary
- From the binary part get the LSBs
- Reshape the received binary column to L by 8 matrix
- Convert the matrix to decimal
- Convert the decimal matrix to character to get the secret message

To secure the process of hiding PK2 can be used. PK2 contains 8 components; each of them has a value from 1 to 8, the contents of PK2 point to the sequence of CBM bits substitution (rearrangement). CBM bits are to be arranged according to the contents of PK2 before hiding and after extracting as shown in figures 9 and 10:

© 2022, IJCSMC All Rights Reserved

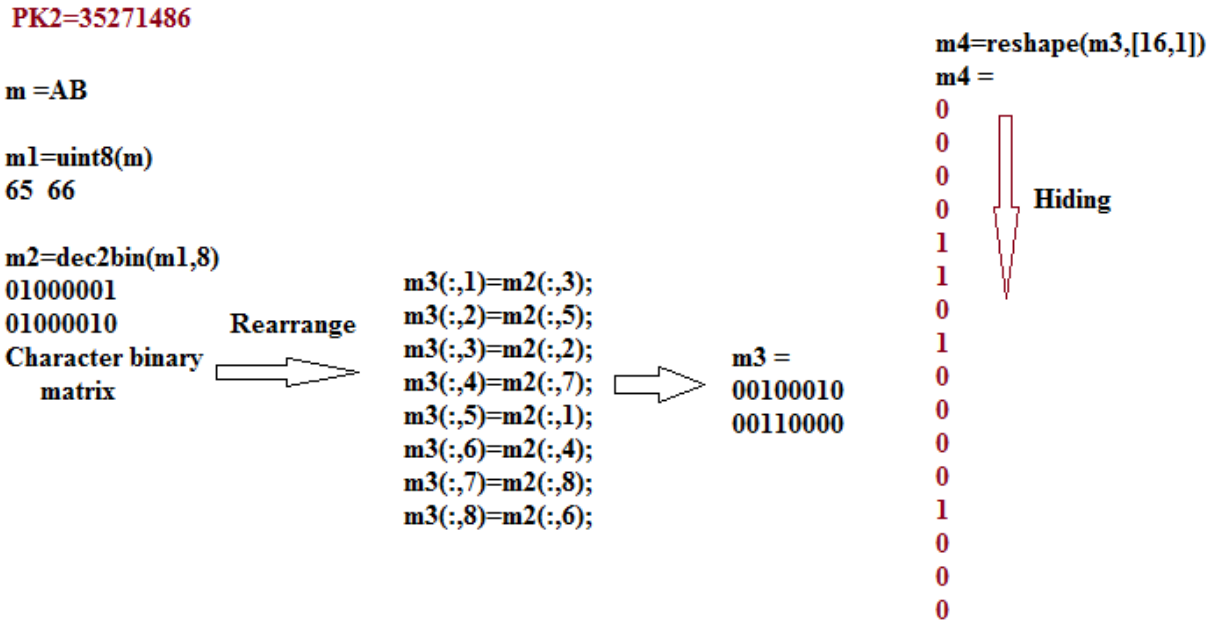

Figure 9: Using PK2 to rearrange CBM in the hiding phase

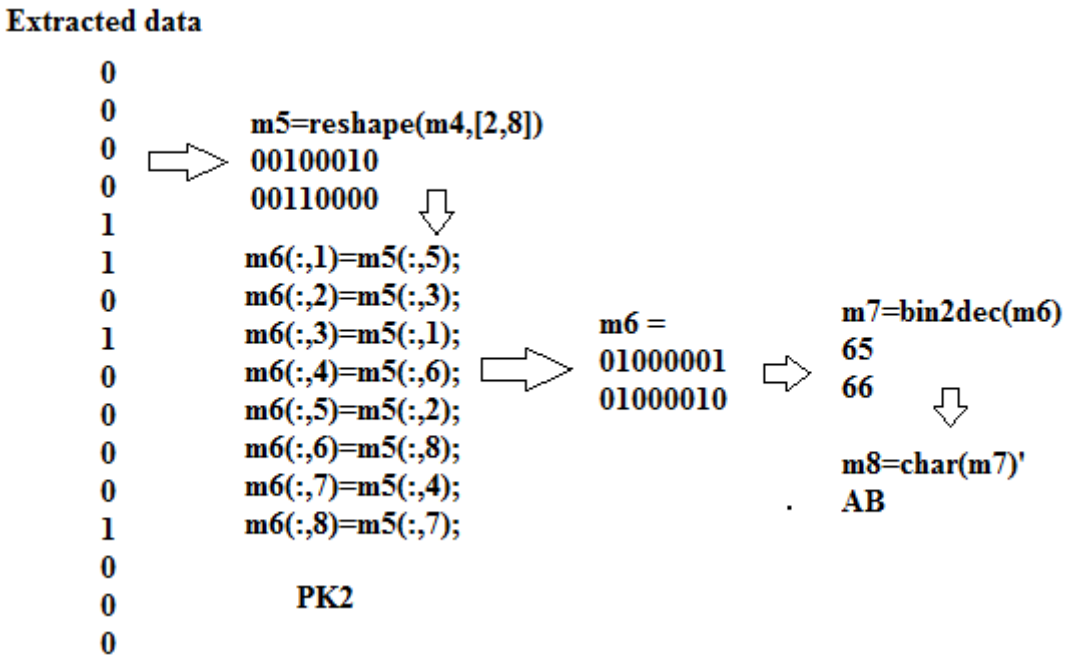

Figure 9: Using PK2 to rearrange CBM in the extracting phase

© 2022, IJCSMC All Rights Reserved

Implementation and Results Analysis

The proposed method was implemented using various secret messages and various covering color images, the obtained results were analyzed using different types of data analysis method (quality, security, sensitivity, and speed analysis's) to prove the efficiency of the proposed method, below we will describe these types of analysis [36-40]:

a) Quality analysis

The requirements of good cryptography is to produce a damaged encrypted data, this data must have a low quality, while the decryption must produce a high quality data that identical to the original data [[40-48].

The steganography must produce a high quality stego image, which is much closed to the covering image, so the changes in the stego image must not be noticed by eyes.

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) MSE and PSNR analysis

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.

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.

© 2022, IJCSMC All Rights Reserved

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

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 10 and 11 show the covering and the stego images:

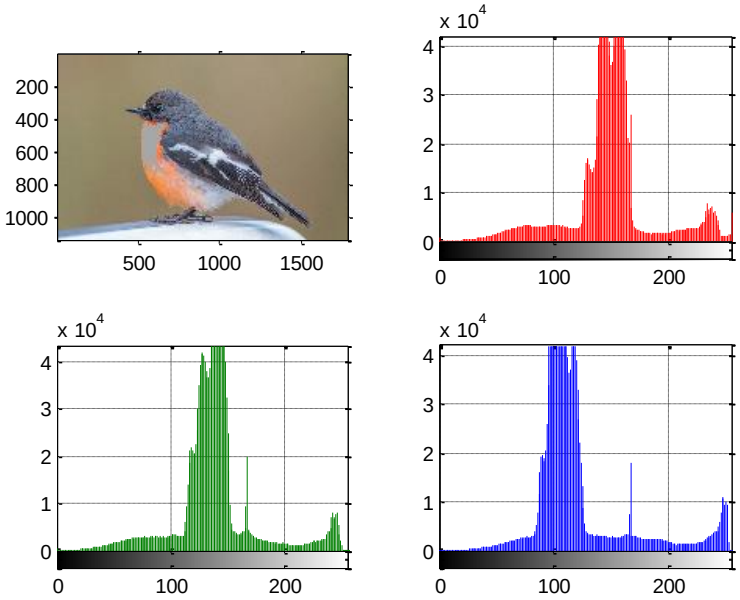

Figure 10: Big covering image

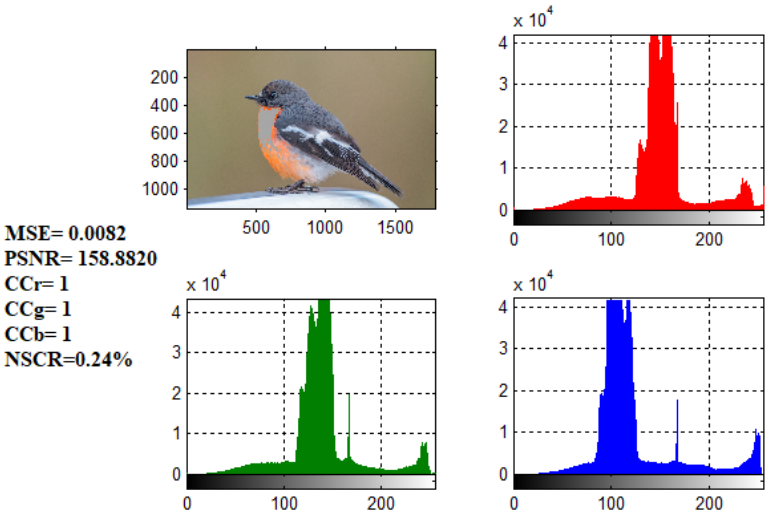

Figure 11: Big stego image

© 2022, IJCSMC All Rights Reserved

The same message was hidden in a smaller covering image with size = 150975, figure 12 and 13 show the covering and stego images:

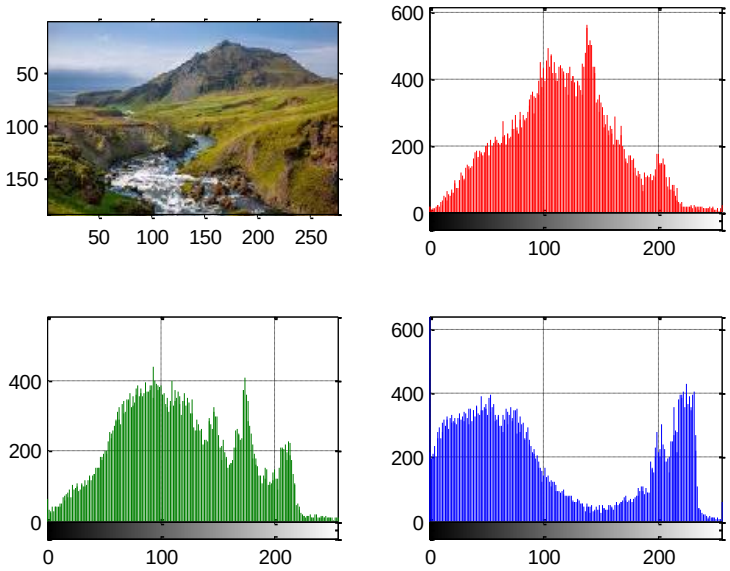

Figure 12: Smaller covering image

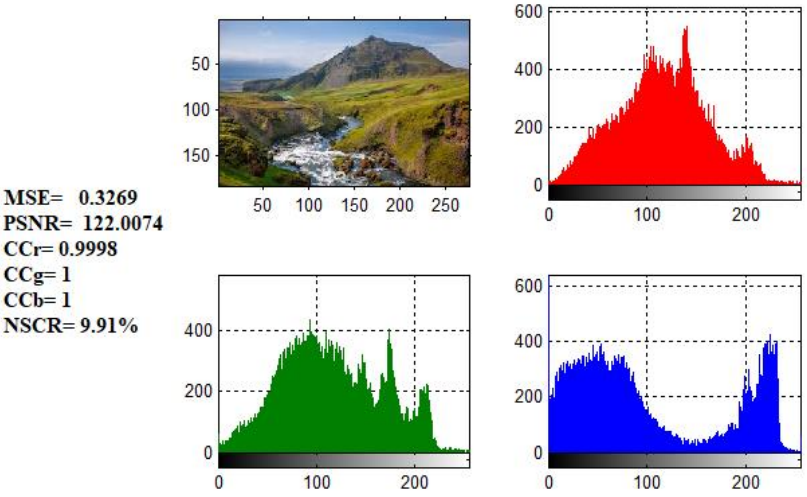

Figure 13: Smaller stego image

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

To optimize the quality of stego image, a big in size covering image was selected (size=6119256 bytes, around 6 M bytes), various messages were treated using this image and using the same PK1 and PK2 (PK1=3.95; 0.325 and PK2=35271486), tables 2 and 3 show the obtained stego quality parameters.

Table 2: MSE, PSNR and NSCR for stego image

Message length (byte)	Between covering and stego images		
	MSE	PSNR	NSCR
100	0.000065204	207.2052	0.0065
500	0.00032422	191.1661	0.0324
1000	0.00065024	184.2069	0.0650
2500	0.0016	174.9824	0.1636
50000	0.0033	168.0285	0.3279
10000	0.0065	161.1322	0.6534
25000	0.0163	151.9606	1.6350
50000	0.0326	145.0496	3.2633
100000	0.0654	138.0935	6.5427
700000	0.4574	118.6468	45.7419

Table 3: CC between covering image colors and stego image colors

Message length (byte)	Between covering and stego images		
	CCr	CCg	CCb
100	1	1	1
500	1	1	1
1000	1	1	1
2500	1	1	1
50000	1	1	1
10000	1	1	1
25000	1	1	1
50000	1	1	1

© 2022, IJCSMC All Rights Reserved

100000	0.9999	1	1
700000	0.9998	0.9998	0.9999

From tables 2 and 3 we can see that the quality parameters values were good and they point to the fact that the stego image is very closed to the covering image, thus the proposed method satisfies the quality requirement of data steganography.

The encryption phase of the secret message must destroy the message by producing a damaged encrypted message, and must recover the original message in the decryption phase; the obtained results shown in tables 4 and 5 prove this fact.

Table 4: MSE and PSNR for message cryptography

Message length(byte)	Between source and encrypted messages		Between source and decrypted messages	
	MSE	PSNR	MSE	PSNR
100	10848	17.9079	0	Infinite
500	10967	17.7987	0	Infinite
1000	10847	17.9086	0	Infinite
2500	10534	18.2012	0	Infinite
50000	10455	18.2766	0	Infinite
10000	10451	18.2807	0	Infinite
25000	10572	18.1653	0	Infinite
50000	10484	18.2490	0	Infinite
100000	10502	18.2317	0	Infinite
700000	10561	18.1760	0	Infinite

Table 5: CC and NSCR for message cryptography

Message length(byte)	Between source and encrypted messages		Between source and decrypted messages	
	CC	NSCR	CC	NSCR
100	0.0920	100	1	0
500	0.0142	99.6000	1	0
1000	0.0110	99.7000	1	0
2500	0.0299	99.7600	1	0

© 2022, IJCSMC All Rights Reserved

50000	0.0302	99.6400	1	0
10000	0.0332	99.5900	1	0
25000	0.0249	99.7000	1	0
50000	0.0336	99.6400	1	0
100000	0.0334	99.6200	1	0
700000	0.0299	99.5994	1	0

b) Sensitivity Analysis

The outputs results of the proposed method are very sensitive the selected values of PK1 and PK2, any changes in one of them or both will lead to produce a damaged and destructed message, these changes in the data retrieving phase will be considered as a hacking attempt by producing a damaged message, table 6 shows the obtained messages when using changed PKs in the retrieving phase, the used keys in the embedding phase where:
Embedding keys:
PK1: r=3.95; x1=0.325
PK2=35271468

Table 6: Retrieving damaged messages when changing the PKs

Retrieving key	Source message	Extracted message
PK1: r=3.95; x1=0.325 PK2=35271468	Data steganography	Data steganography
PK1: r=3.85; x1=0.325 PK2=35271468	Data steganography	Só äÿ¨·ÿV O
PK1: r=3.95; x1=0.125 PK2=35271468	Data steganography	©Õ]ÕÐø]Ñ@Õ< @-Õ³ • l
PK1: r=3.95; x1=0.325 PK2=85271463	Data steganography	Î¥]¥Ð»]ÑÇ¥< Çî¥³ë

c) Security Analysis

PK1 contains two chaotic parameters values, each value has a double data type(8 bytes for representation), thus PK1 will provide a key space with size equal 2^128. PK2 contains 8 components, each of them ranges from 1 to 8, so the key space provided by this key is equal 8^8=2^24, and here the total key space will equal 2^152, this key space can resist any hacking attack.

© 2022, IJCSMC All Rights Reserved

d) Speed Analysis

The covering image with size equal 6119256 bytes was selected, various in sizes messages were treated using the proposed method, and table 7 shows the obtained speed parameters:

Table 7: Obtained speed parameters results

Message length(byte)	Embedding		Retrieving	
	Time(second)	Throughput(K byte per second)	Time(second)	Throughput(K byte per second)
100	0.0234	4.1684	0.0013	77.1864
500	0.0358	13.6420	0.0022	221.0818
1000	0.0498	19.6095	0.0036	270.6359
2500	0.0963	25.3446	0.0073	335.5839
5000	0.1714	28.4854	0.0128	380.3584
10000	0.3202	30.4955	0.0249	391.9765
25000	0.7776	31.3968	0.0624	390.9910
50000	1.5245	32.0290	0.1553	314.4414
100000	3.0860	31.6445	0.2469	395.5619
700000	22.0862	30.9512	1.7051	400.9228
Average		24.7767		317.8740

From table 7 we can see that the proposed method provides good average throughputs in the embedding and retrieving phases, the embedding and retrieving times depend on the message length and there is a linear relationship between each of them and the message length as shown in figure 14.

© 2022, IJCSMC All Rights Reserved

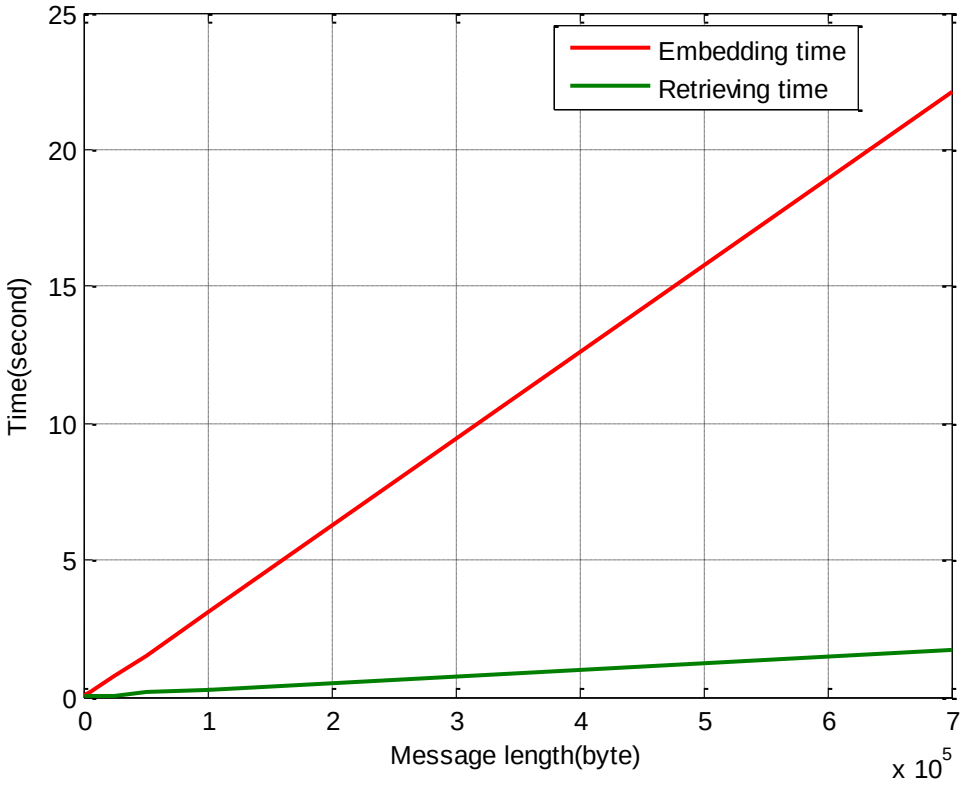

Figure 14: Embedding and retrieving times vs message length

Conclusion

A simple and efficient method of data steganography was introduced. The method was based on LSB of data steganography with simple modifications. The data hiding and retrieving were organized on characters' bit's sequence instead of characters' sequence used in the LSB method. The method used two private keys to provide message protection; these two keys provided the necessary key space to resist hacking attacks. The process of message data embedding was performed using two phases: message encryption using PK1 and message hiding using PK2. The process of message retrieving was performed using two phases: message extracting using PK2, and message decryption using PK1. CLMM was used to generate the first secret key which was converted to lockup table to apply message encryption-decryption. The second key was used to apply bits' substitutions of the message binary matrix.

The proposed method was implemented, and it was recommended to use a big in size covering image to optimize the efficiency of the proposed method. The obtained results of data analyses proved that the proposed method satisfied the quality requirements of data cryptography and data steganography. The outputs of the proposed method are very sensitive to PK1 and PK2 any changes in them in the retrieving phase will be considered as a hacking attempt. It was shown that the proposed method has a good speed parameters values by providing a good throughput in the embedding and retrieving phases.

© 2022, IJCSMC All Rights Reserved

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.

[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.

© 2022, IJCSMC All Rights Reserved

[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.

[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.

© 2022, IJCSMC All Rights Reserved

[44] 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