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. 11, November 2022, pg.68 – 88

Using Secret Image Block to Secure LSB Data Steganography

Prof. Ziad Alqadi
Al Balqa Applied University, Faculty of Engineering Technology, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.007

Abstract: Data steganography is one of the most popular methods of data protection, but most introduced methods are not secure. In this paper research a simplified LSB method of data steganography will produced, this method will easily used to hide any message in any covering image, changing the image or/and changing the message will not require any changes in the algorithm. The proposed method will use a complicated key to select a secret block from the covering image to be used to hide the message. The PK will contain 5 components of double data type, thus the PK will provide a huge key space which is capable to resist any hacking attempt, the algorithm of the proposed method will be very sensitive to the PK values, any changes in these values will be considered as a hacking attempt by producing unexpected outputs. The proposed method will be implemented and tested using various messages, various covering images, and various PK; the obtained results will be analyzed applying sensitivity analysis, quality analysis and security analysis to prove the improvements added to LSB method of data steganography.

Keywords: Steganography, stego image, covering image, secret block, PK, MSE, PSNR, CC, NSCR, TP.

Abbreviations

The following abbreviations will be used in this research paper:
PK: private key.
SB: secret block.
SM: secret message
SI: stego image
CI: covering image
HT: hiding time.
ET: extracting time
TP: throughput
MSE: mean square error

© 2022, IJCSMC All Rights Reserved

PSNR: peak signal to noise ratio
CC: correlation coefficient
NSCR: number of samples change ratio
UR: upper row
LR: lower row
UC: upper column
LC: lower column
L: message length

Introduction

Secret message steganography is the process of hiding secret message in a covering digital color image to produce a stego_image as shown in figure 1 [55-64]. Data steganography is required to protect secret data from being used from any other third party who does not have the right to read or deal with the secret data [45-54]. The data sender usually uses one of the existing methods of data steganography to hide secret message, and then the receiver uses the same method to extract secret message from the stego image [21-24].

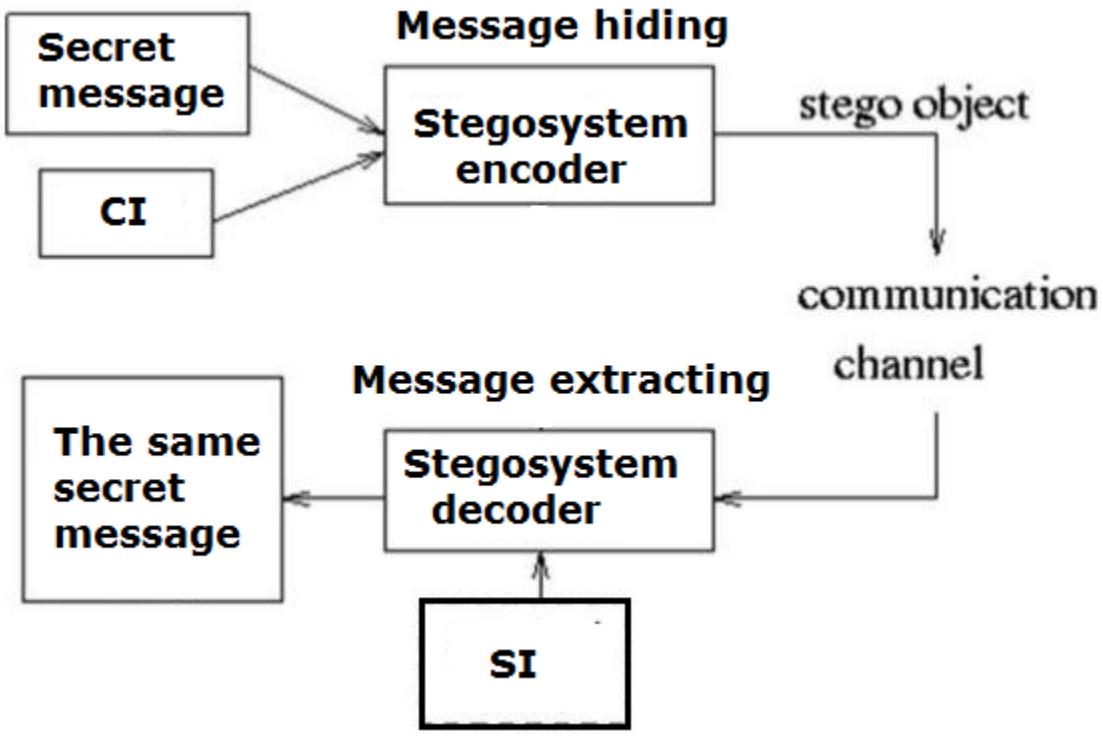

Figure 1: Message steganography model

Mostly Digital color image is the most popular data used as covering media to hide SMs due to following reasons [33-39]:

- Digital image usually has a huge capable to hold short and long secret messages [40-44].
- Digital color images are available everywhere and can be obtained without any cost [10-15].
- Digital images can be easily process, each color image is represented by a 3D matrix and it is very easy to handle this matrix (see figure 2) [15-20].
- Pixels values have the range 0 to 255, which matches the range of characters ASCII values [25-30].
- It is very easy to convert the image matrix from 3D matrix to one row or one column matrix [31-39].

© 2022, IJCSMC All Rights Reserved

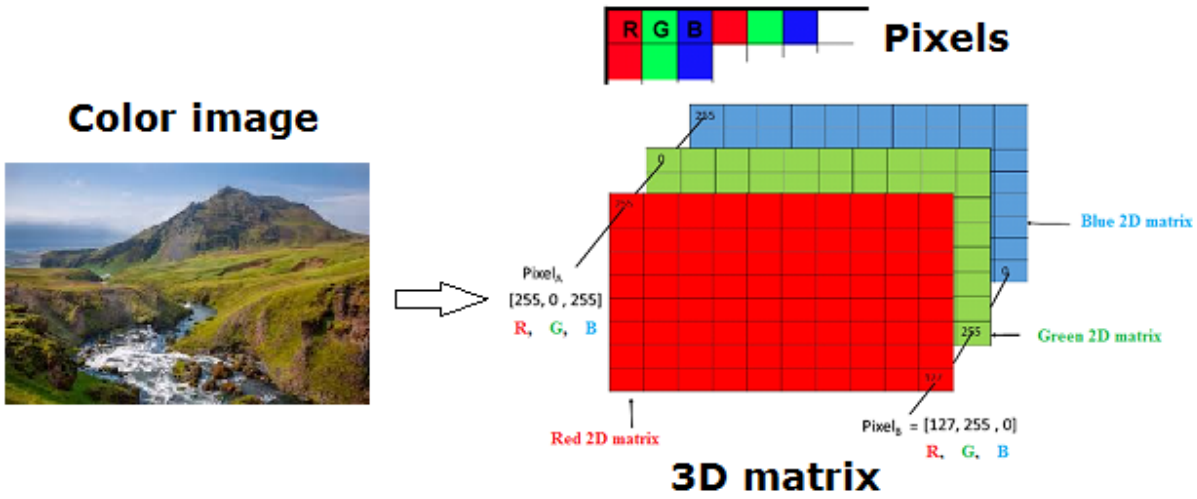

Figure 2: CI representation

One of the most popular methods of SM steganography is least significant bit (LSB) method, this method reserves the LSBs from the CI to hold the SM, and each byte of the SM requires 8 bytes from the CI as shown in figure 3 [25-32], thus the capacity of hiding in bytes (maximum SM length) will be equal CI size divided by 8.

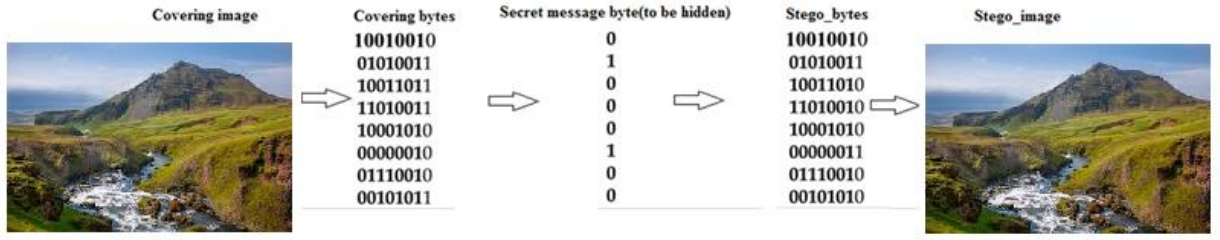

Figure 3: LSM SM hiding

The process of hiding the SM in the CI should not affect the CI negatively so that no change is observed on the stego_image with the naked eye, and accordingly, the quality of the stego_image must be very high so that the mean square error (MSE) between the covering and the stego images must be very low, at the same time peak signal to noise ratio (PSNR) between them must very high [20-30]. A good method of SM steganography must satisfy the quality requirements listed in table 1:

Table 1: Steganography quality requirements

Quality parameter	Measured between CI and SI
MSE	Low
PSNR	High
CC	Closed to 1
PSNR	Closed to zero

© 2022, IJCSMC All Rights Reserved

LSB method of SM steganography adds minor changes to the image bytes, the changes will vary from -1 to +1 (see table 2 and figure 4), these changes cannot be noticed by human eyes, and this will be reflected on the values of MSE and PSNR, making the SI closed to the CI [31-40].

Table 2: LSB method changes in the stego byte

SM bit	CI LSB	SI LSB	Remarks(SI byte with CI byte)
0	0	0	SI=CI
0	1	0	SI=CI-1
1	0	1	SI=CI+1
1	1	1	SI=CI

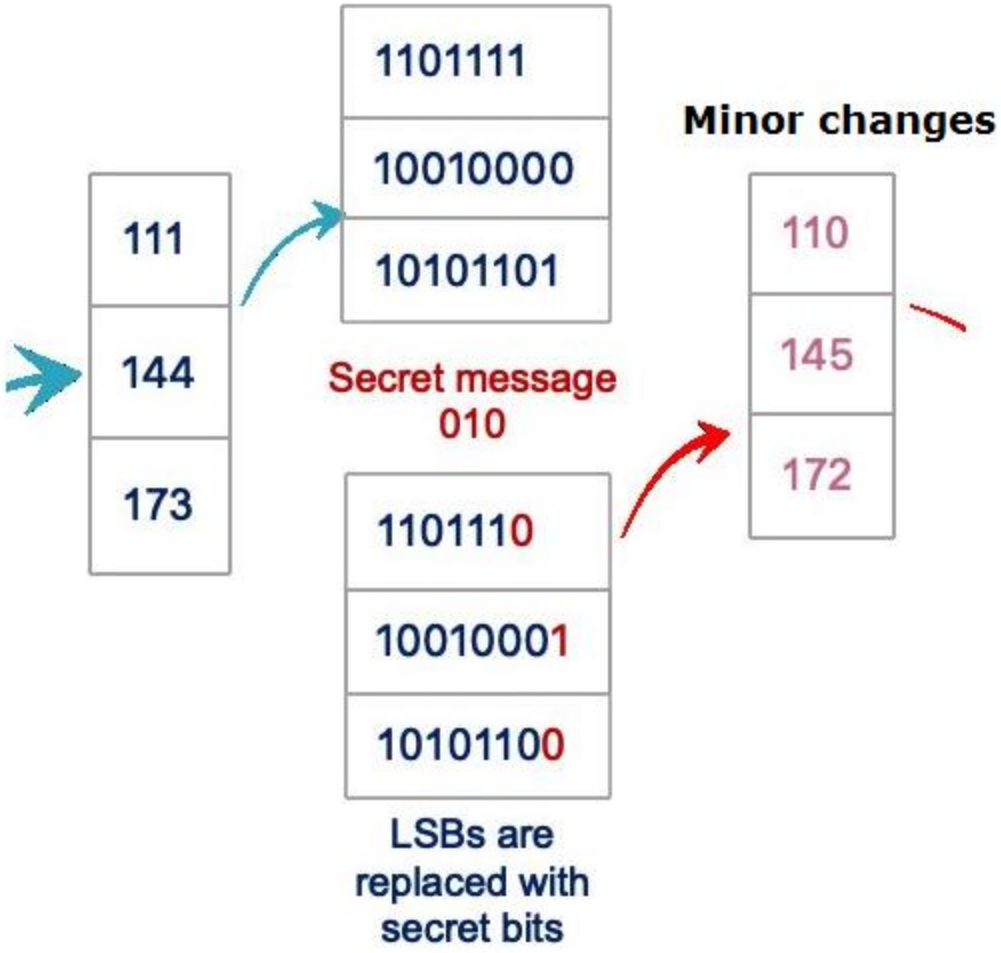

Figure 4: LSB method adds minor changes to CI

© 2022, IJCSMC All Rights Reserved

LSB method of SM steganography has been widely used to hide secret private information within digital color image due to its simplicity and more imperceptible method. Different Authors used the simple LSB techniques to hide data by replacing the pixels with secret data bits according to Authors in [10]. The authors in [6], worked on hiding the secret image into cover image, where both images should have the same size. Their technique first compresses the secret message using Set Partitioning in Hierarchical Trees (SPIHT) algorithm, then the output of this compression is embed into the cover image using default LSB technique. The compression is made by wavelet transform and then by using the SPIHT coding. Image quality is retained with high PSNR values. Authors in [7], hided the secret message file into the covered image, the image should be colored and transformed into 3 matrices (R, G, and B). The message convert to binary, depending on the secret message bit using (OR) or (AND) operation, sequentially (RGB, BGR, RGB, BGR…). Their results showed better performance in terms of quality of the stego image obtained. On the other hand, authors in [5], used two different techniques LSB and DCT to perform steganography. It gave a good result according to the PSNR values comparing with previous works and the security was increased by using DCT. Authors in [4], hided text message by embedding the byte of the message in three pixels only. They found that their method achieved a very high Maximum Hiding Capacity and Higher visual quality as indicated by PSNR. Authors in [12], tried to overcome the disadvantage of the LSB method by appending encrypted data in image in place of plain textual data. To encrypt the data RSA and Diffie Hellman algorithms were used. To check the efficacy of the proposal, they calculated the number of instructions executed at sender and receiver site since the number of instructions executed is a measure of time complexity of the process. The result showed that the use of encryption in Steganalysis does not affect the time complexity if Diffie Hellman algorithm is used instead of RSA algorithm. Authors in [11], used a methodology that hide the secret message based on searching for the identical bits between the secret messages and image pixels' values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hides the secret message directly in the least two significant bits of the image pixels. This paper concludes that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it searches for the identical bits then starts hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. Authors in [13], used Pixel-Value Differencing (PVD) method as image steganography scheme; the pixel values in the stego image may exceed the range 0 … 255. Therefore, they have eliminated this overflow problem of each component pixel. Moreover, for providing more security, they have used different number of bits in different pixel components. It was very difficult to trace how many bits are embedded in a pixel of the stego image. The results obtained in the introduced proposed method provide better visual quality of stego_image compared to the PVD method.

In [1] an Image Steganography Algorithm using LSB Replacement through XOR Substitution was proposed, this method is not secure and gave good values for quality parameters (PSNR=70.08 for long messages and 91.6 for short messages, and 91.6) the authors make a comparison with [2] and showed the achieved enhancements in the obtained MSE and PSNR values. In [3] a New Image Steganography Depending On Reference & LSB was proposed this method is not secure and provided a good quality by moving the PSNR value to 92. In [14], the authors made comparisons between several of methods used for data steganography; it was shown that LSB method provided a good quality and throughput measures.

© 2022, IJCSMC All Rights Reserved

The Proposed Method

The objective of this research paper is to provide an LSB-based method to hide any SM in any CI; this method will improve the security of LSB method by using a complicated private key as shown in figure 5:

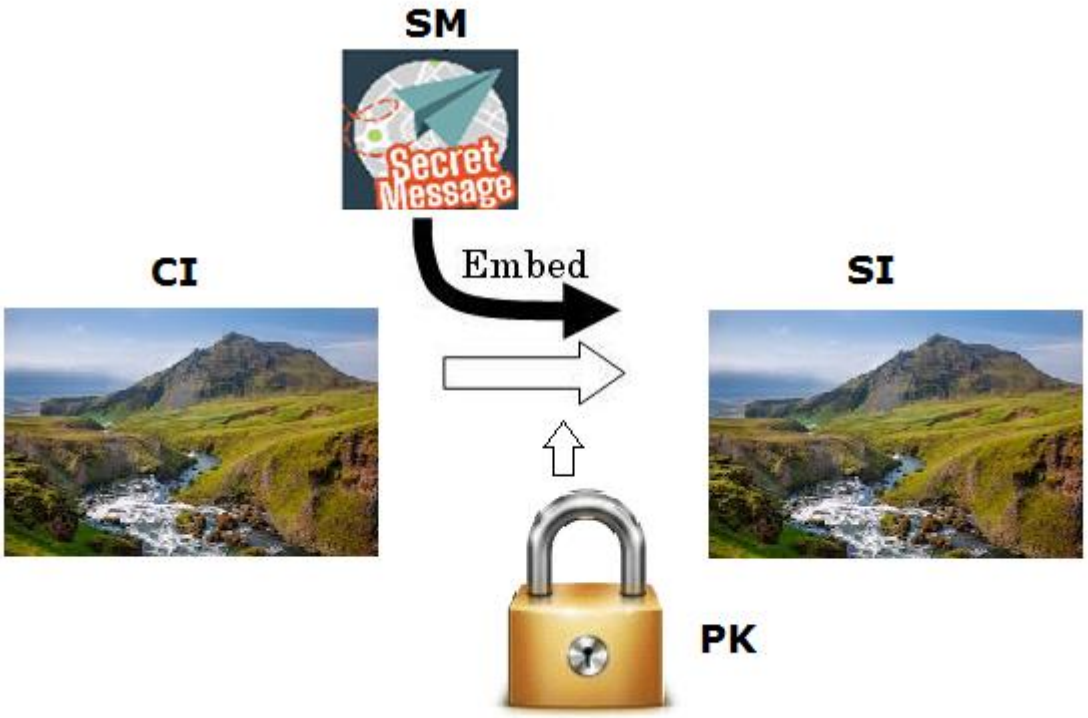

Figure 5: Proposed method diagram

The PK as shown in figure 6 has a complicated structure, which contains the following components:

- L: SM length in characters.
- UR: upper row fraction, which is used to find the upper row of the secret block, by multiplying its value with the covering image row length and taking the integer value.
- LR: lower row fraction, which is used to find the lower row of the secret block, by multiplying its value with the covering image row length and taking the integer value, here UR must be greater than LR.
- UC: upper column fraction, which is used to find the upper column of the secret block, by multiplying its value with the covering image column length and taking the integer value.
- LC: lower column fraction, which is used to find the lower column of the secret block, by multiplying its value with the covering image column length and taking the integer value, here UC must be greater than LC.

It must be noticed here that the SB size must be greater than the SM length multiplied by 8, the size of the selected SB depends on the selected values of the PK and on the selected size of the CI, the secret block is very sensitive to the PK selected values, changing one or more value will change the SB size and the starting points of the selected SB.

© 2022, IJCSMC All Rights Reserved

PK			
L			
UR	LR	UC	LC
Example (CI size=183x275)			
100			
0.3	0.2	0.45	0.17

Figure 6: PK structure

Figure 7 shows an example of determining the secret block:

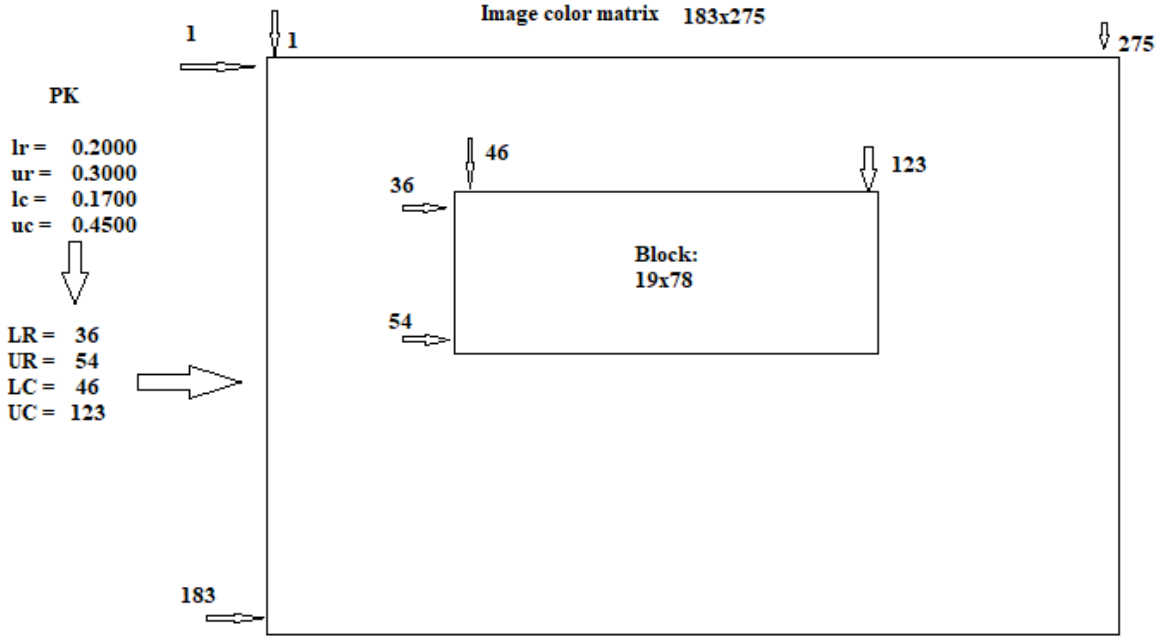

Figure 7: Determining the SB example

© 2022, IJCSMC All Rights Reserved

Figures 8 and 9 show a samples of the selected SB using various PKs and various images:

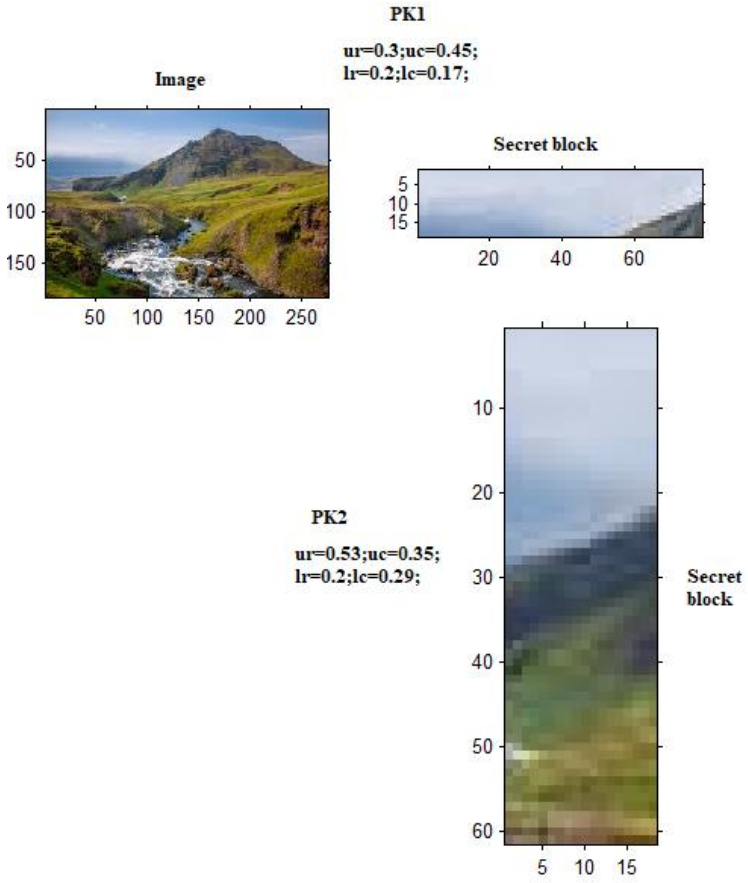

Figure 8: Samples of SBs using the same CI

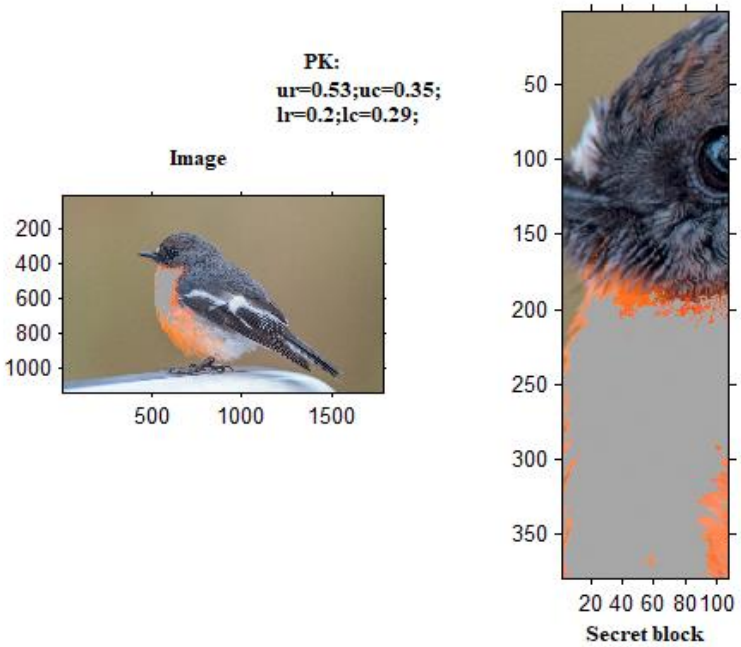

Figure 9: SB using another CI

© 2022, IJCSMC All Rights Reserved

The proposed method is based on LSB method, but the processes of hiding and extraction SK are simplified by minimizing the number of operations required to apply SM hiding and extracting.

The process of hiding in the proposed method can be implemented applying the following phases (see figure 10):

Phase 1: Selecting the SB, this phase can be implemented applying the following steps:

Step 1: Select the PK.

Step 2: Get the CI and retrieve the image size.

Step 3: Apply the necessary calculations to find the SB size and location.

Phase 2: SM hiding, this phase can be implemented applying the following steps:

Step 1: Get the SM

Step 2: Convert the SM from characters to decimals.

Step 3: Convert the decimal SM to binary.

Step 4: Reshape the binary message to one column.

Step 5: Reshape the SB to one row matrix.

Step 6: From the obtained row select a part with size equal SM length multiplied by 8.

Step 7: Convert the part to binary.

Step 8: Let the LSBs of the binary part equal the SM binary column.

Step 9: Convert the part back to decimal.

Step 10: Return the modified SB back to the CI.

The process SM extracting can be implemented applying the following phases (see figure 11):

Phase 1: Getting the SB, this phase can be implemented applying the following steps:

Step 1: Get the PK.

Step 2: Get the CI and retrieve the image size.

Step 3: Apply the necessary calculations to find the SB size and location.

Phase 2: SM extracting, this phase can be implemented applying the following steps:

Step 1: Get the SB.

Step 2: Reshape the SB to one row matrix.

Step 3: From the obtained row get a part equal SM length multiplied by 8.

Step 4: Convert the part to binary.

© 2022, IJCSMC All Rights Reserved

Step 5: Retrieve the LSBs from the part (column 8).

Step 6: reshape the obtained column to 8 column matrix.

Step 7: Convert the obtained matrix to decimal.

Step 8: Convert the decimal matrix to character to get the SM.

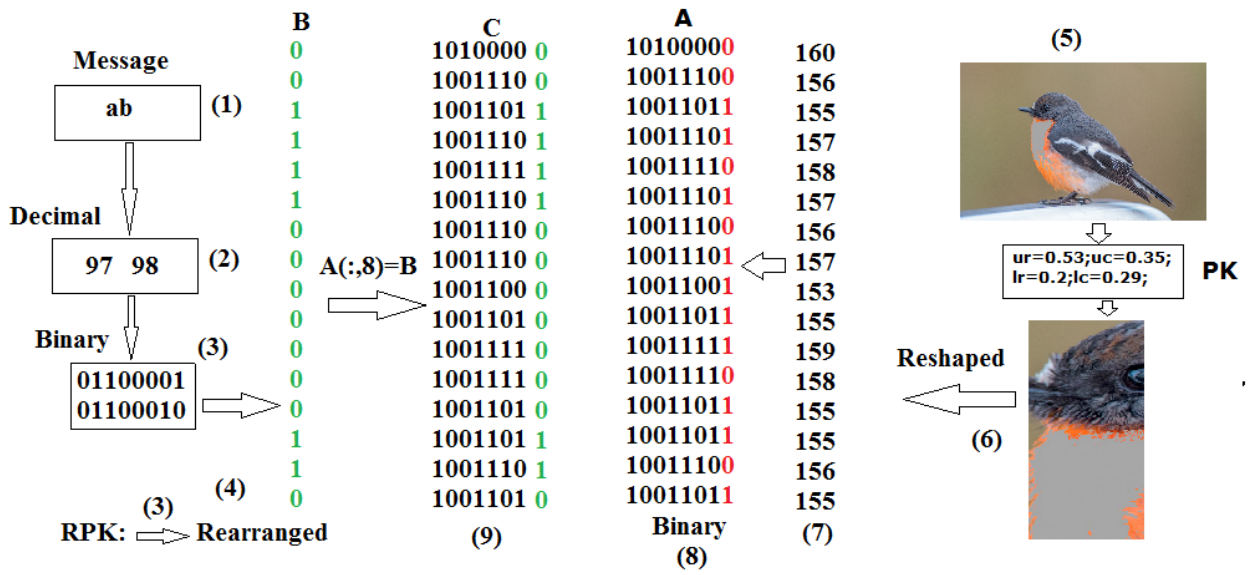

Figure 10: Data hiding process example

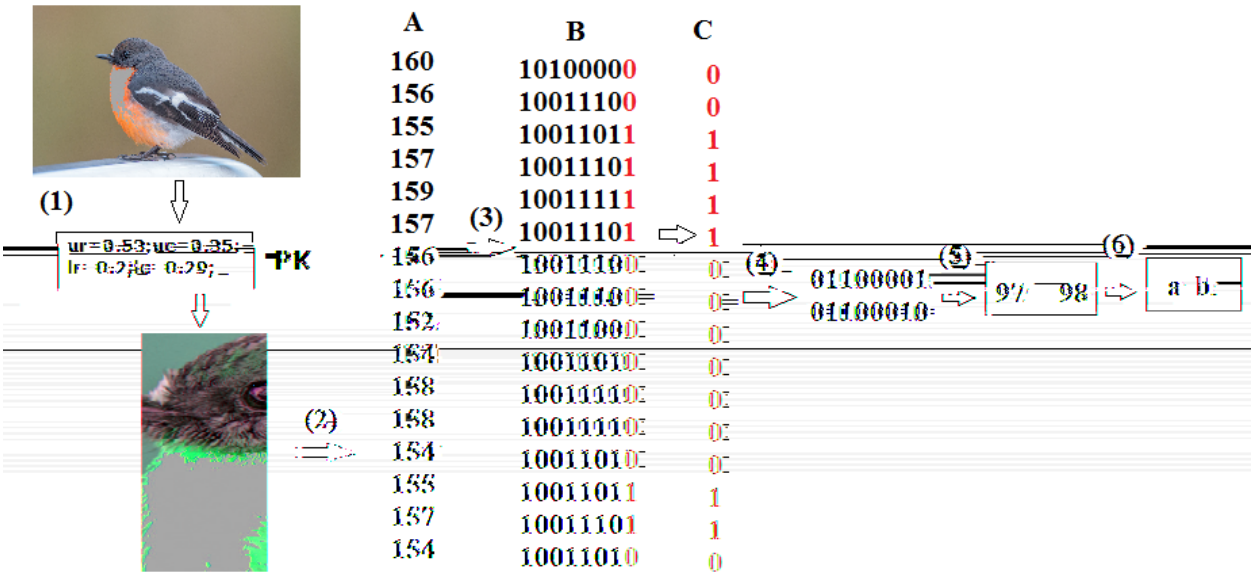

Figure 11: Data extracting process example

© 2022, IJCSMC All Rights Reserved

Implementation and Results Analysis

The proposed method was implemented using various SMs and various Cis, the obtained results were analyzed, below the analysis results will be discussed.

- **Visual Analysis**

The obtained SI after SM hiding must be closed to the CI, the changes in the SI must not be noticed by human eyes, also the extracted SM must be identical to the source SM. The following SM 'Data steganography using secret block' was hidden in a CI using Following PK:

PK:

L=37;

ur=0.53; uc=0.35;

lr=0.2; lc=0.29;

The same PK was used in the extraction phase, figures 12 and 13 show the obtained outputs, the same source SM was extracted after performing the extraction phase.

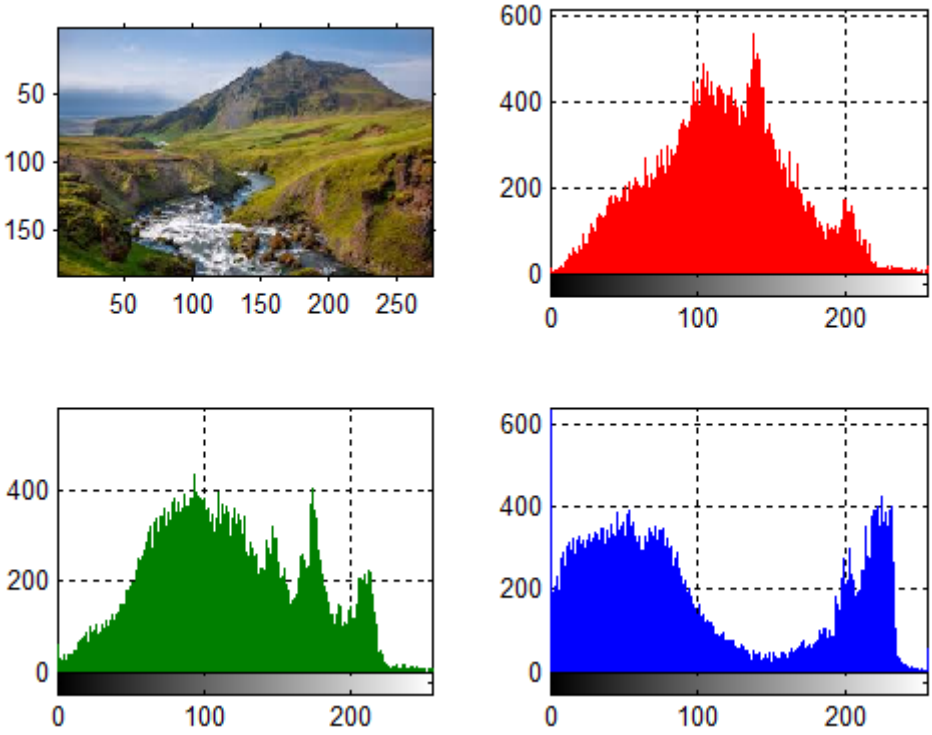

Figure 12: CI and histograms

© 2022, IJCSMC All Rights Reserved

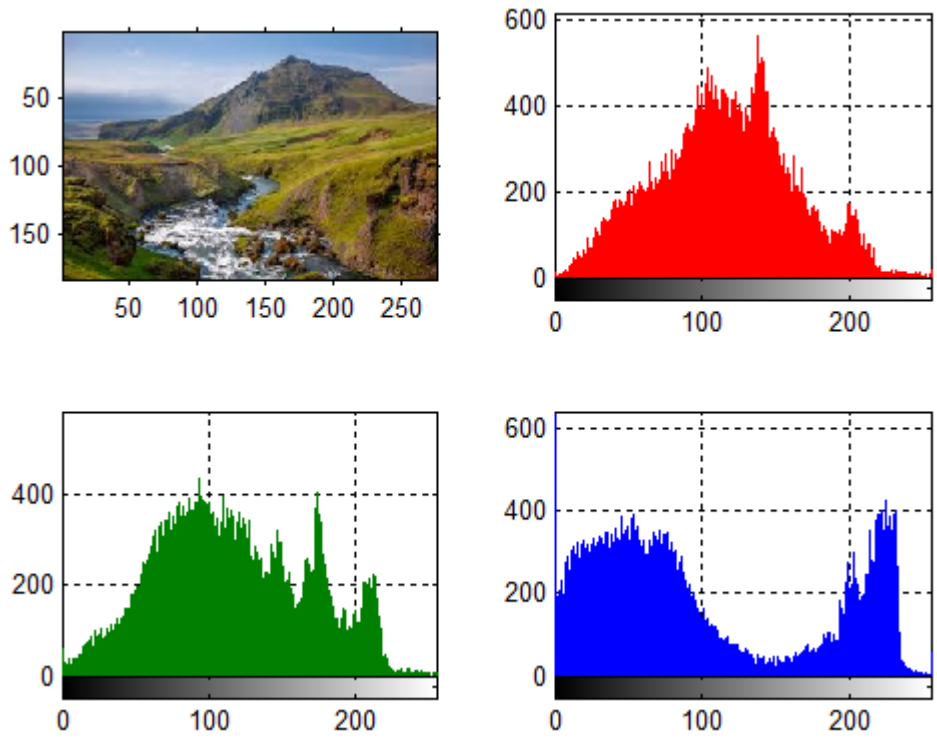

Figure 13: SI and histograms

From figures 12 and 13 it is seen that the SI is very closed to the CI, and the changes in SI cannot be noticed by nicked eyes.

- **Sensitivity Analysis**

The extracted SM from the SI is very sensitive to the used PK, the same PKs must be used in the hiding and extracting phases, any changes in the PK during the extracting phase will produce a damaged and un expected message, also using only LSB method of data extracting will produce un expected SM.

To show this the previous message was hidden using PK1 and extracted using PK2:

PK1:

PK:

L=37;

ur=0.53; uc=0.35;

lr=0.2; lc=0.29;

PK2:

L=37;

ur=0.4; uc=0.62;

© 2022, IJCSMC All Rights Reserved

lr=0.1; lc=0.17;

The extracted message was:

□e□□□m-ç□?ïü□pad□ö>□□`□¶2Ø!Ý□ÿèU°□³%³

Using only LSB method of message extraction (without using the PK) also cause to obtain un expected message, the following message was extracted using LSB method of data extraction:

@k□?Þ¦Ðöl□åx|«□8õ³³Ò|j□M{□ nÀæ4□¨#°□b

- **Quality Analysis**

The quality of the SI must be high and the SI must be very closed to the CI, this fact can be proved by calculating the quality parameters measured between the source CI and the SI (MSE, PSNR, CC, and NSCR).

MSE and PSNR can be calculated using equations 1 and 1:

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

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

Where: MAX is the maximum possible value of samples values, N is the total number of samples, xi and yi are the corresponding sample values of CI and SI.

The value of CC between two images expresses the dependency between their corresponding sample values. This is another statistical evaluation for testing the quality of the algorithm of data cryptography. Calculating correlation coefficient determines the level of correlation between two images and the correlation coefficient is always in range [−1, 1]. Values between |1–0.7| is considered as strong correlation, 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:

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

where

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

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

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

N is the total number of samples, xi and yi are the sample values of two images, $\bar{x}$ and $\bar{y}$ are the mean values of samples, and finally cov (x, y) is covariance between both images.

© 2022, IJCSMC All Rights Reserved

Number of sample change rate (NSCR) is robustness test for establishing the quality of data cryptography algorithms. The purpose of the test is to compare the corresponding sample values of two images to show the difference in percent. NSCR can be calculated using equation 5.

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

where

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

The image shown in figure 14 was selected as a CI, several messages were processed using the proposed method, the quality parameters were calculated, and table 3 shows the obtained results:

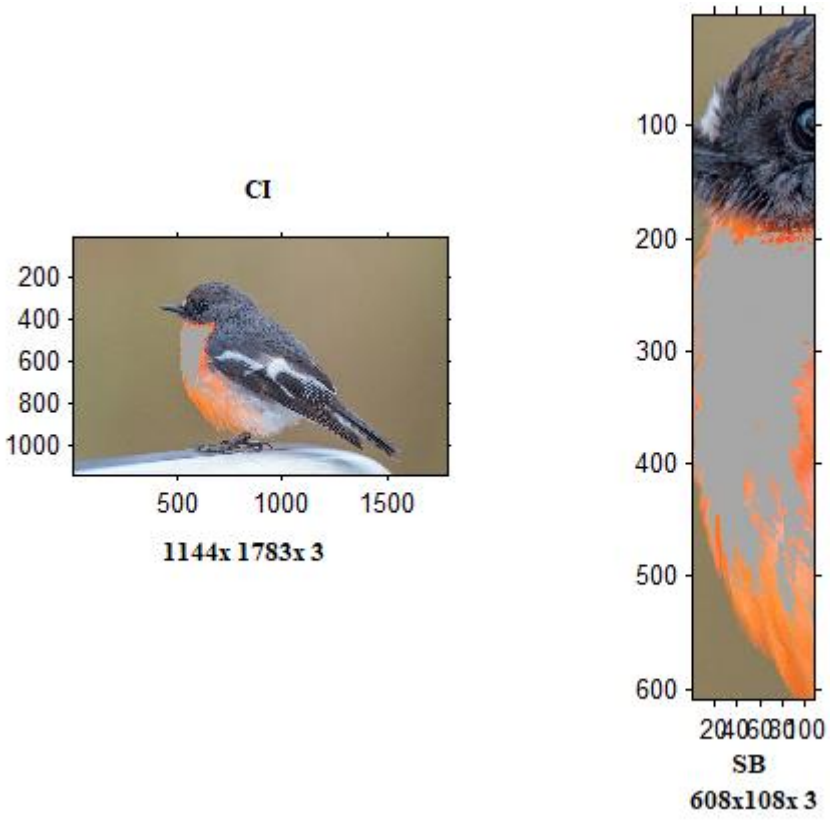

Figure 14: Selected CI

© 2022, IJCSMC All Rights Reserved

Table 3: Quality results (measured between CI and SI)

SM number	L(characters)	MSE	PSNR	CCr	CCg	CCb	NSCR (%)
1	50	0.000030559	214.7837	1	1	1	0.0031
2	100	0.000067492	206.8603	1	1	1	0.0067
3	250	0.00016734	197.7801	1	1	1	0.0167
4	500	0.00032341	191.1913	1	1	1	0.0323
5	750	0.00048159	187.2094	1	1	1	0.0482
6	1000	0.00066135	184.0375	1	1	1	0.0661
7	2000	0.0013	177.1345	1	1	1	0.1319
8	3000	0.0019	173.2267	1	1	1	0.1950
9	4000	0.0026	170.3478	1	1	1	0.2600
10	5000	0.0033	168.0980	1	1	1	0.3256
Remarks		**Low**	**High**	**Excellent**			**Low**

The obtained results shown in table 3 show that the proposed method satisfies the quality requirements, and here the following must be noticed:

- Increasing the CI size will enhance the quality parameters.
- Increasing the SM length will negatively affect the quality parameters (see figure 15, but the SI quality remains acceptable.
- The proposed method can be efficiently used to hide SM with various sizes (short and long SMs), keeping the quality of the SI good and acceptable.

© 2022, IJCSMC All Rights Reserved

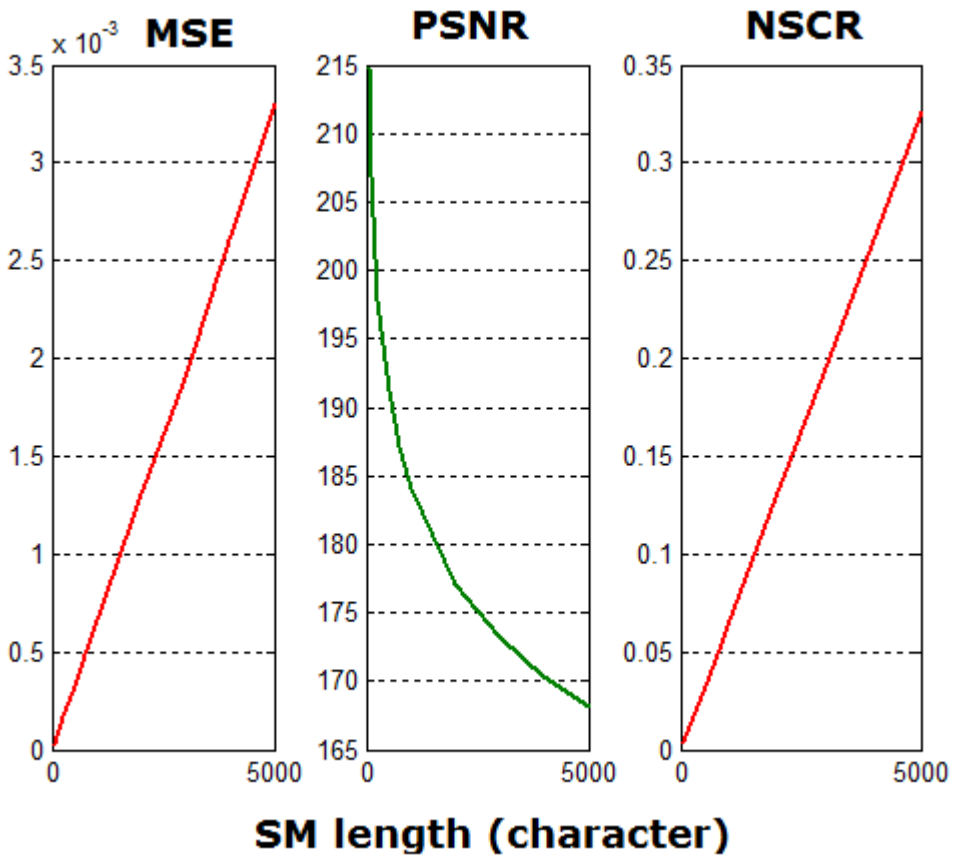

Figure 15: MSE, PSNR and NSCR vs SM length

- **Speed Analysis**

The proposed method was implemented using various SMs, the HTs and ETs were measured and the TPs were calculated, table 4 shows the obtained results.

Table 4: Speed results

SM number	Size (byte)	HT(second)	ET(second)	Hiding TP(K bytes per second)	Extracting TP(K bytes per second)
1	50	0.1840	0.0020	0.2654	24.4141
2	100	0.1880	0.0020	0.5194	48.8281
3	250	0.1960	0.0050	1.2456	48.8281
4	500	0.2430	0.0080	2.0094	61.0352
5	750	0.2110	0.0080	3.4712	91.5527
6	1000	0.2240	0.0100	4.3597	97.6563

© 2022, IJCSMC All Rights Reserved

7	2000	0.2750	0.0190	7.1023	102.7961
8	3000	0.3030	0.0290	9.6689	101.0237
9	4000	0.3320	0.0380	11.7658	102.7961
10	5000	0.3970	0.0450	12.2993	108.5069

From table 5 we can see that increasing the SM length increases the hiding and extracting throughputs, to prove this fact an image with size (3000x4500x3=40500000=39550.78125 K bytes) was selected as a CI, and long SMs were treated, table 5 shows the obtained results:

Table 5: Times and throughputs results (for long messages)

Message size(K byte)	Hiding time(second)	Extraction time(second)	Hiding throughput(byte per second)	Extraction throughput(byte per second)
1	0.0680	0.0150	15059	68267
10	0.4780	0.1080	21423	94815
40	1.6110	0.4040	25425	101390
50	2	0.4980	25600	102810
80	3.4560	0.7730	23704	105980
100	3.9320	1.0730	26043	95433
200	8.1470	1.8740	25138	109280
300	12.1510	3.0500	25282	100720
400	15.8890	3.9200	25779	104490
500	19.9630	4.8300	25647	106000
1000	41.2830	9.4670	24804	108170

From table 5 we can see that the proposed method is very efficient by providing hiding throughput around 25 K bytes per second and extracting throughput around 106 K bytes per second, these parameters are better than the results obtained in [1-5].

- **Simplicity and Security Analysis**

The proposed hiding and extracting phases are too simple, each of them contains a sequence of operations, and the sequences do not require any changes when changing the secret message, covering image and PK.

The proposed method uses a PK with 5 components; each of them has a double data type, so the provided key space will be calculated using equation 5:

© 2022, IJCSMC All Rights Reserved

$$\text{Key space} = 2^{64x5}$$

$$= 2^{320} \qquad (5)$$

This huge key space is capable to resist hacking attacks.

Conclusion

An enhanced LSB method of secret messages steganography method was provided, the LSB method improvements increased the efficiency of SMs steganography. The proposed method was implemented and the obtained results showed various improvements of LSB SM steganography. The method used a complicated PK to create a secret block to be used to hide the SM The corners of the secret block are to be calculated based on the PK contents, the created secret block was very sensitive to the selected values of the PK, any changes in these values in the extraction phase caused to producing un expected SM and it was considered as a hacking attempt. The PK provided a huge key space capable to resist hacking attempts.

The quality analysis showed that the proposed method provided an excellent value for MSE and PSNR and the stego_image was always closed to the covering image. The proposed method is a multipurpose method, it was shown that it suite short and long messages steganography keeping this process efficient, and it was recommended to use big in size covering image to hold a long messages (with hundreds of K bytes sizes). The throughput analysis showed that the proposed method minimized the hiding and extracting time and maximizing the hiding and extracting processes throughputs (up to 25 K byte per second in the hiding process and 106 K bytes per second in the extracting process).

References

[1] Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT), DOI:10.1109/icoiact46704.2019.8938486.

[2] Maya Abood, An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms, Computer Science, Mathematics 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT) 2017.

[3] Saher Manaseer, Asmaa Aljawawdeh and Dua Alsoudi, A New Image Steganography Depending On Reference & LSB, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1950-1955.

[4] Emam, M. M., Aly, A. A., &Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications, 1(7), pp. 361-366, (2016).

[5] Kaur, G., &Kochhar, A. A steganography implementation based on LSB & DCT. International Journal for Science and Emerging Technologies with Latest Trends, 4(1), pp.35-41, (2012).

[6] Thenmozhi, M. J., &Menakadevi, T. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. International Journal of Engineering, 16(17), (2016).

[7] Shabnam, S. & Hemachandran , K. LSB based Steganography using Bit masking method on RGB planes. (IJCSIT) International Journal of Computer Science and Information Technologies, 7 (3) , pp.1169- 1173, (2016) .

[8] Datta, B. , Mukherjee, U. , &Bandyopadhyay, S. LSB Layer Independent Robust Steganography using Binary Addition. International Conference on Computational Modeling and Security (CMS 2016), Elsevier Pub, (2016).

[9] Pandit, A. S., Khope, S. R., & Student, F. Review on Image Steganography. International Journal of Engineering Science, 6115, (2016).

© 2022, IJCSMC All Rights Reserved

[10] Artz, D. Digital steganography: hiding data within data. IEEE Internet computing, 5(3), 75-80, (2001).
[11] Al-Shatnawi, A. M. A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), 3907-3915, (2012).
[12] Gupta, S., Goyal, A., &Bhushan, B. Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 4(6), pp.27, (2012).
[13] Mandal, J. K., & Das, D. Color image steganography based on pixel value differencing in spatial domain. International journal of information sciences and techniques, 2(4), (2012).
[14] Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019
[15] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, 2010, Optimized True-RGB color Image Processing, World Applied Sciences Journal8 (10): 1175-1182, ISSN 1818-4952.
[16] Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.
[17] Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254
[18] Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334
[19] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.
[20] Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.
[21] Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.
[22] Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005.
[23] Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.
[24] 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.
[25] 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.
[26] 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.
[27] Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350
[28] Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue.2, February 2019, pg.93 – 103
[29] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.
[30] Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 .https://doi.org/10.1109/ICIS.2016.7550955
[31] Wu D-C, Tsai W-H. A stenographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003https://doi.org/10.1016/S0167-8655(02)00402-6
[32] Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016.https://doi.org/10.1109/ICRCICN.2016.7813674.
[33] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

© 2022, IJCSMC All Rights Reserved

[34] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[35] 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.

[36] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[37] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[38] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[39] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[40] Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.

[41] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[42] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[43] 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.

[44] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[45] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[46] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[47] J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.

[48] K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal, 31 (10), 1767-1771, 2014.

[49] Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.

[50] 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, issue 1, pp. 86-93, 2019.

[51] Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.

[52] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[53] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.

[54] 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 9, pp. 4092-4098, 2019.

[55] Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.

© 2022, IJCSMC All Rights Reserved

[56] 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.

[57] Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

[58] Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[59] Jihad Nader Ahmad Sharadqh, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.

[60] 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.

[61] Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology &Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[62] Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019.

[63] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TOCREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.

[64] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

© 2022, IJCSMC All Rights Reserved