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. 12, Issue. 1, January 2023, pg.59 – 69

Long Messages Segmentation for Efficient Message Cryptography

Dr. Hatim Zaini*; Prof. Ziad Alqadi**
*Taif University, KSA
**Albalqa Applied University, Jordan

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i01.008

Abstract: Protecting LSB method of data steganography is a vital issue. In this paper research a secure LSB method will be introduced. The method will use a private key to divide a covering image into block and a secret block will be selected to apply message hiding and message extracting. The extracted message will be very sensitive the selected block size and the selected block number. The proposed method will simplify the hiding and extraction functions by using patch method, this simplification will increase the method efficiency. The proposed method will be tested for sensitivity, several images and several messages will be selected and the quality of the stego images will be examined.

Keywords: Steganography, covering image, stego image, PK, block, quality, sensitivity.

Introduction

Due to the increasing use of the global information network, the Internet, it has become difficult to protect this information, especially since it is in a form that arouses suspicion in the intruder [1-10]. As a result of imposing many restrictions to prevent the use of encryption across the network, this led to the emergence of another method in the field of data security development, which is the science of hiding information. Not only to prevent intruders from knowing the hidden information, but also to remove doubt about the existence of this information. The distinctive thing about the concealment technology is that it keeps pace with modern technologies and can be used in all computer media such as images, texts, audio, video and network packets [31-35].

The masking technique is one of the data security techniques, as it works to include information in a specific medium in a way that does not raise suspicion of the existence of a correspondence between two parties. In this research, an algorithm is proposed to secure the process of message steganography using a complicated private key (PK) [36-40].

The system of message steganography as shown in figure 1 contains: Secret message, covering color image, stego image, PK, hiding function and extracting function [55-59].

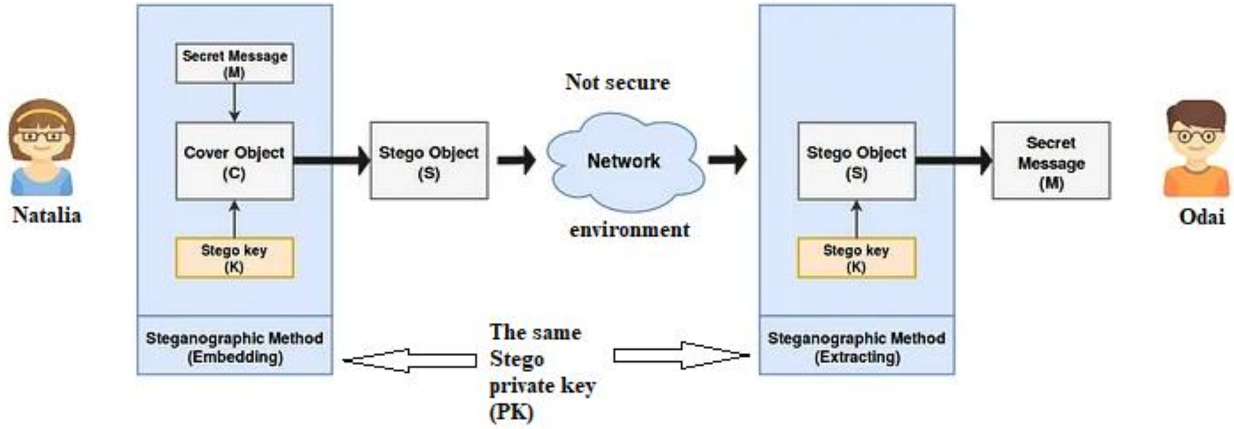


Figure 1: Steganography system

Many methods were introduced for message steganography, and many of these methods were based on least significant bit (LSB) method [12-20].

LSB method of data steganography is a simple method and it reserve the LSBs (see figure 2) of the covering bytes to hold a message, the stego byte will be very closed to the covering byte and the changes are within the range -1 to +1, these changes cannot be noticed by human eyes (see figure 3) [21-28].

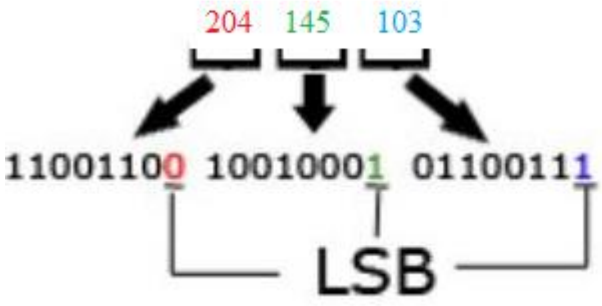
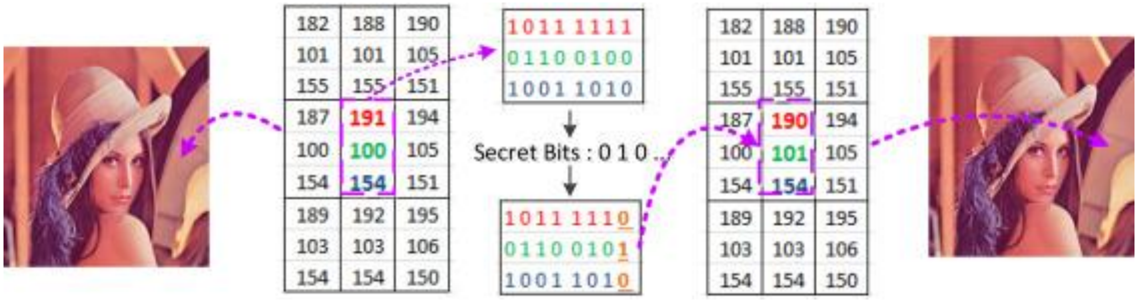


Figure 2: LSBs of the covering/stego bytes



182	188	190
101	101	105
155	155	151
187	191	194
100	100	105
154	154	151
189	192	195
103	103	106
154	154	150

182	188	190
101	101	105
155	155	151
187	190	194
100	101	105
154	154	151
189	192	195
103	103	106
154	154	150

Figure 3: Changes in the stego bytes

LSB method of data steganography has the following features (some of these features can be considered as disadvantages) [1-11]:

- Each message byte requires 8 bytes from the covering image, so the hiding capacity will equal the image size divided by 8 (max byte which can be hidden in the image), increasing the image size, and using a high resolution image will increase the hiding capacity.
- Message hiding/extracting stars from the first byte in the image, the hiding message can be easily hacked applying LSB extracting [40-48].
- The covering-stego bytes must be consecutive, first 8 bytes for the first character, second 8 bytes for the second character and so on (see figure 4), doing this will add extra operations which will increase the complicity of method programming [50-55].
- LSB method of data steganography is not secure, it is easy to hack the hidden message.
- The quality of the stego image is high, mean square error (MSE) between the covering and stego images is always low, while the PSNR (peak signal to noise ratio) between them is always high, so by eyes it is difficult to notice that the stego image is holding a secret message [49-59].

Digital color image (DCI) [21-30] is usually used as a covering image because of the following reasons:

- DCI is available and we can get it without any cost, and it is easy to store and retrieve it.
- DCI has a huge size, which allow us to hide long messages.
- Easy to process, DCI is represented by a 3D matrix as shown in figure 5, this matrix can be divided easily into blocks, and one or more blocks can be used to hide the secret message [11-20].

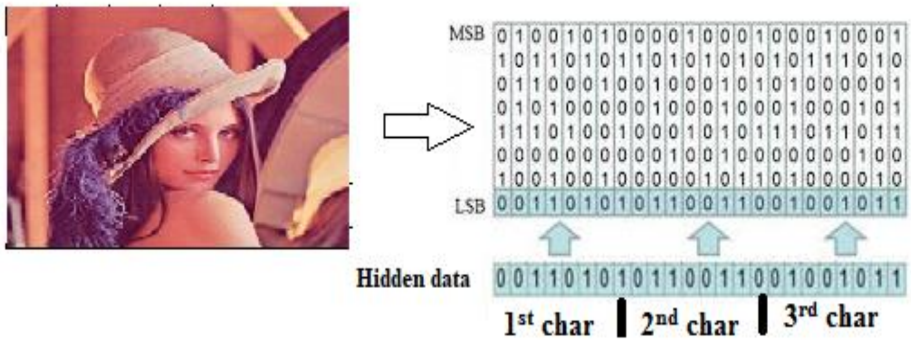


Figure 4: Consecutive bytes to hide a message

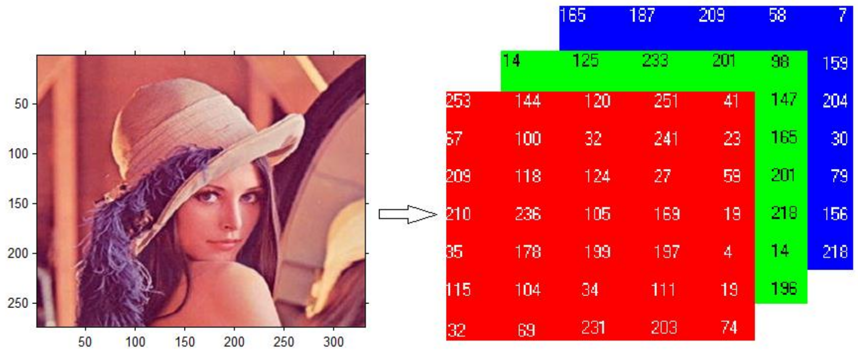


Figure 5: DCI 3D matrix

Proposed Method

The proposed method is based on LSB method of data steganography with an added feature. These features add a security to the LSB method and simplify the process of message hiding and extracting.

The proposed method uses a private key (PK), which contains two parameters p1 and p2, these parameters point to the fractions from the image rows and columns. Figures 6 and 7 show the source image and obtained blocks when p1=0.25 and p2=0.25.

The same private key must be used in the hiding and extracting phases, any changes in the PK in the extraction phase will lead to extract a damaged message.

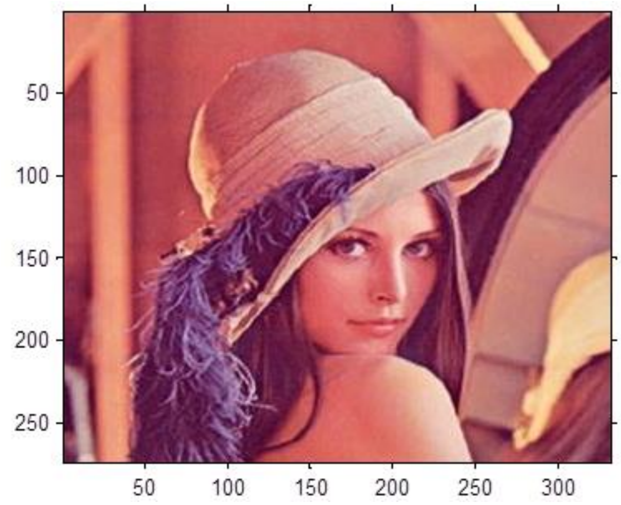


Figure 6: Source DCI

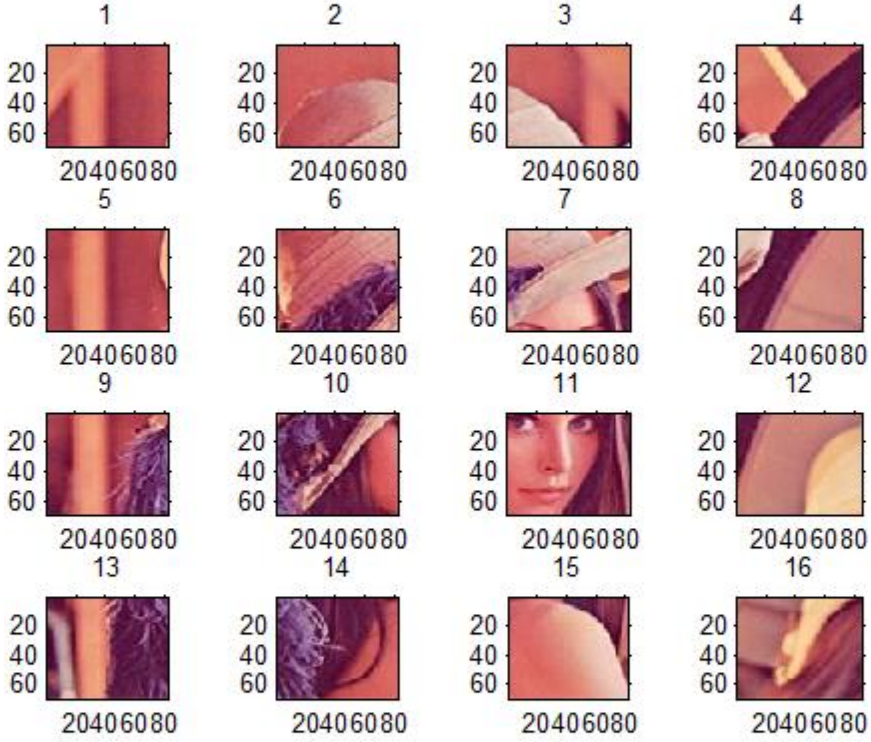


Figure 7: DCI blocks

The proposed method uses a patch method of data hiding/extracting. Instead of using consecutive bytes to hold a message byte the message is to be converted to decimal, the decimal version is to be converted to binary. The message binary matrix is to be reshaped to one column matrix and inserted into the LSBs of the covering bytes as shown in figure 8.

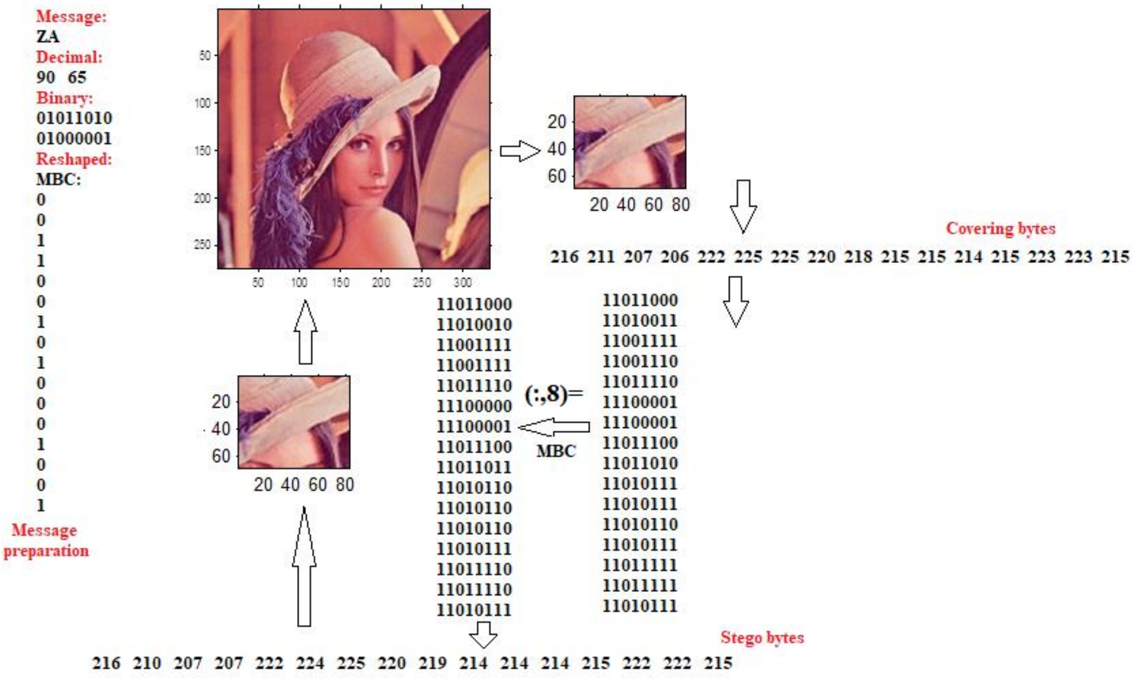


Figure 8: Proposed method data hiding example

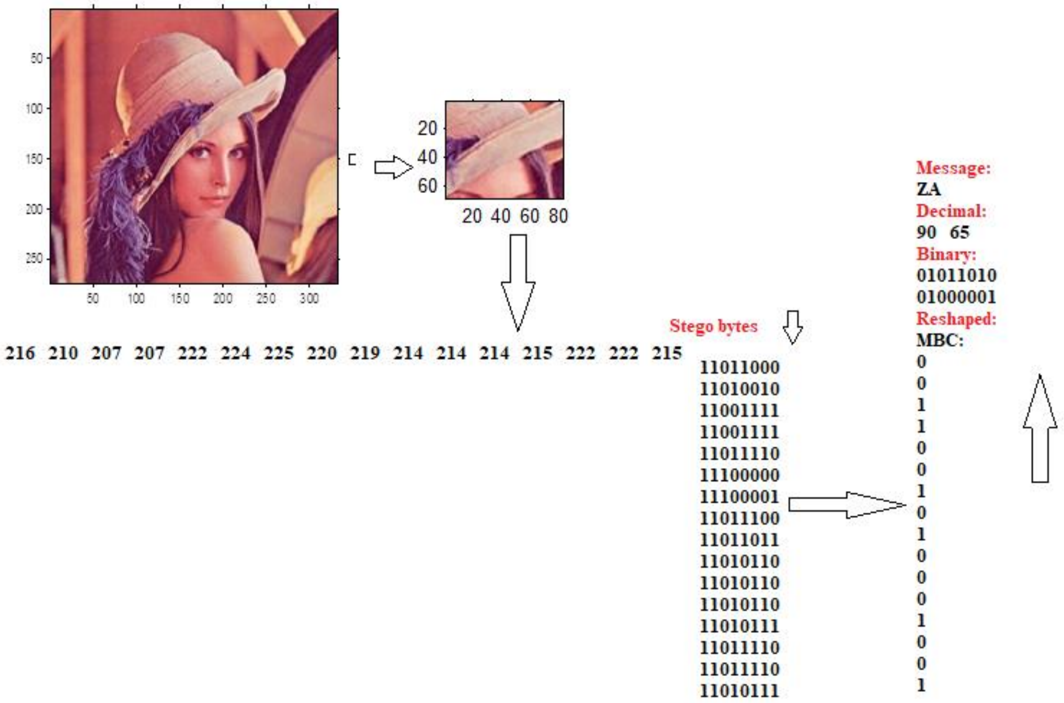
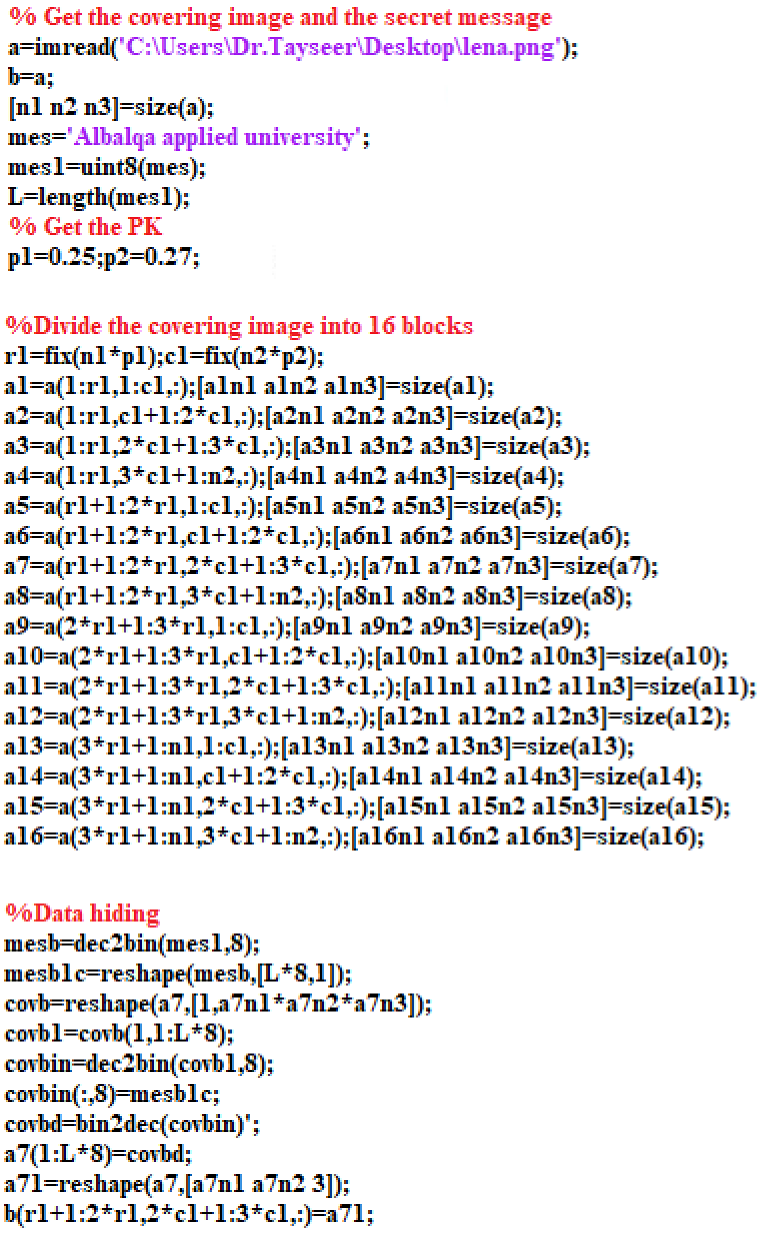


Figure 9: Proposed method data extracting example

The extracting process is to be implemented using patch method, this method can be implemented applying the following:

The covering bytes must be converted to binary, the LSBs must be extracted and the obtained one column matrix must be reshaped to 8 columns matrix to get the message binary matrix, this matrix must be converted to decimal then to characters to get the secret message. Figure 9 shows an example of data extracting.

Below is the mat lab code which can be used to hide/extract a secret message:



```
% Get the covering image and the secret message
a=imread('C:\Users\Dr.Tayseer\Desktop\lena.png');
b=a;
[n1 n2 n3]=size(a);
mes='Albalqa applied university';
mes1=uint8(mes);
L=length(mes1);
% Get the PK
p1=0.25;p2=0.27;

%Divide the covering image into 16 blocks
r1=fix(n1*p1);c1=fix(n2*p2);
a1=a(1:r1,1:c1,:);[a1n1 a1n2 a1n3]=size(a1);
a2=a(1:r1,c1+1:2*c1,:);[a2n1 a2n2 a2n3]=size(a2);
a3=a(1:r1,2*c1+1:3*c1,:);[a3n1 a3n2 a3n3]=size(a3);
a4=a(1:r1,3*c1+1:n2,:);[a4n1 a4n2 a4n3]=size(a4);
a5=a(r1+1:2*r1,1:c1,:);[a5n1 a5n2 a5n3]=size(a5);
a6=a(r1+1:2*r1,c1+1:2*c1,:);[a6n1 a6n2 a6n3]=size(a6);
a7=a(r1+1:2*r1,2*c1+1:3*c1,:);[a7n1 a7n2 a7n3]=size(a7);
a8=a(r1+1:2*r1,3*c1+1:n2,:);[a8n1 a8n2 a8n3]=size(a8);
a9=a(2*r1+1:3*r1,1:c1,:);[a9n1 a9n2 a9n3]=size(a9);
a10=a(2*r1+1:3*r1,c1+1:2*c1,:);[a10n1 a10n2 a10n3]=size(a10);
a11=a(2*r1+1:3*r1,2*c1+1:3*c1,:);[a11n1 a11n2 a11n3]=size(a11);
a12=a(2*r1+1:3*r1,3*c1+1:n2,:);[a12n1 a12n2 a12n3]=size(a12);
a13=a(3*r1+1:n1,1:c1,:);[a13n1 a13n2 a13n3]=size(a13);
a14=a(3*r1+1:n1,c1+1:2*c1,:);[a14n1 a14n2 a14n3]=size(a14);
a15=a(3*r1+1:n1,2*c1+1:3*c1,:);[a15n1 a15n2 a15n3]=size(a15);
a16=a(3*r1+1:n1,3*c1+1:n2,:);[a16n1 a16n2 a16n3]=size(a16);

%Data hiding
mesb=dec2bin(mes1,8);
mesb1c=reshape(mesb,[L*8,1]);
covb=reshape(a7,[1,a7n1*a7n2*a7n3]);
covb1=covb(1,1:L*8);
covbin=dec2bin(covb1,8);
covbin(:,8)=mesb1c;
covbd=bin2dec(covbin)';
a7(1:L*8)=covbd;
a71=reshape(a7,[a7n1 a7n2 3]);
b(r1+1:2*r1,2*c1+1:3*c1,:)=a71;
```

```
%Data extracting
a7r=reshape(a7,[1,a7n1*a7n2*a7n3]);
a7rs=a7r(1,1:L*8);
a7rsb=dec2bin(a7rs,8);
a72=a7rsb(:,8);
a74=reshape(a72,[L,8]);
a75=bin2dec(a74);
em=char(a75')
```

Implementation and Results Discussion

The proposed method was implemented using various images and various messages, figure 10 shows the selected images:

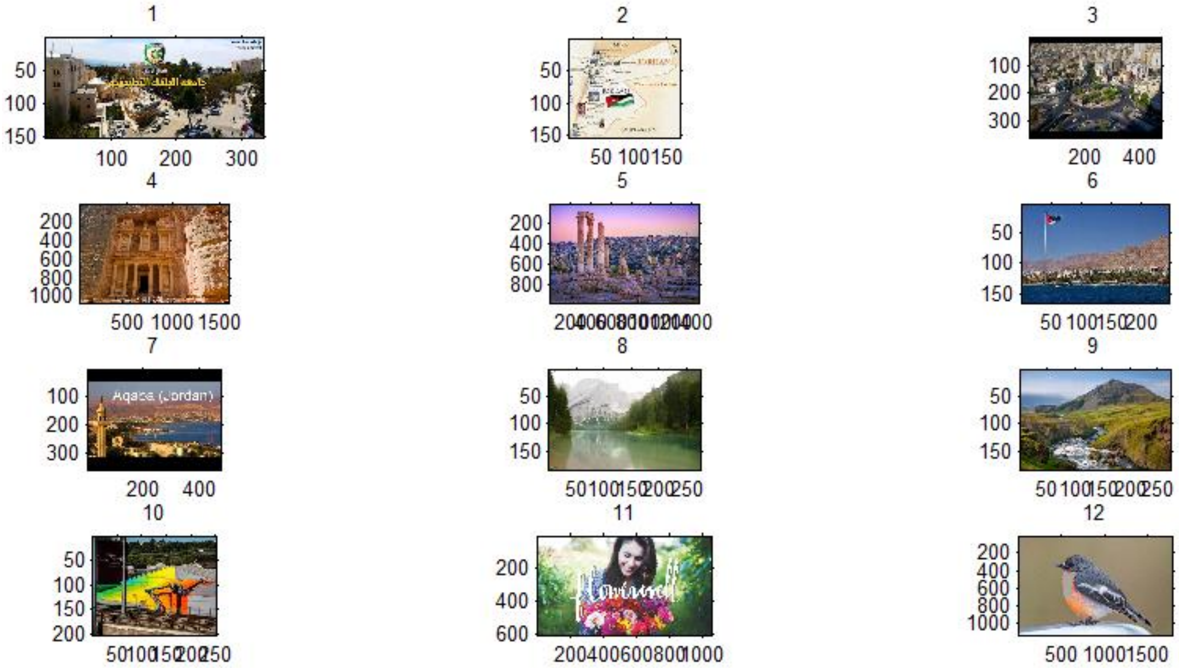
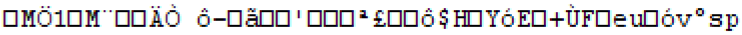


Figure 10: Selected covering DCI

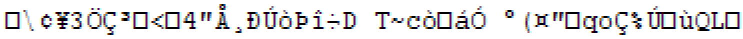
The proposed method is sensitive the selected PK, any changes in the PK during the extraction phase will lead to extract a damaged secret message, the message “Secure data steganography using image blocking’ was hidden using the PK: p1=0.25, p2=0.27 and extracted using p1=.03, p2=0.19.

The following rubbish was extracted:



```
□MÖ1□M¨□□ÄÒ ô-□ã□□'□□□ª£□□ô$H□YóE□+ÙF□eu□óv°sp
```

The extracting phase was implemented using the same PK but the block was changed to block 9, here also we obtained a damaged message:



```
□\¢¥3ÖÇ³□<□4"Å¸ĐŰòÞî÷D T~cò□áÓ °(¤"□qoÇ‰Ű□ùQL□
```

The quality of the stego image was tested, table 1 shows the obtained values of MSE and PSNR calculated between the covering and stego images after hiding a message of 46 characters:

Table 1: Quality parameters

Covering image	Size (byte)	MSE	PSNR
1	150849	0.0012	177.9163
2	77976	0.0024	171.0494
3	518400	0.00036073	190.0992
4	5140800	0.000036376	213.0414
5	4326210	0.000043225	211.3162
6	122265	0.0015	175.7612
7	518400	0.00034336	190.5925
8	150975	0.0012	177.7629
9	150975	0.0012	177.8704
10	151353	0.0012	177.8415
11	1890000	0.000095767	203.3612
12	6119256	0.000028598	215.4469

From table 1 it is shown that the quality for all stego images is acceptable, MSE decreased when increasing the image size and PSNR increased when increasing the image size.

Conclusion

A simple method of data steganography was introduced, the method simplified the process of message hiding and message extracting by using patch method, the binary message was hidden using one operation, and also the binary data extracting was also implemented using one operation. The proposed method protect the hidden message based on using a private key, the message was hidden in a selected secret block, which increased the security level of message protection. The hiding and extracting phases must use the same private key, any changes in the private key during the extraction phase was considered as a hacking attempt by producing a damaged message. The quality of the stego images was tested and it was shown that the proposed method provided a good quality image.

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).

[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 & 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.

[34]. Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.

[35]. Ziad A, Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, vol. 15, issue 1, 2005.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. 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.

[40]. 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.

[41]. Prof. Ziad Alqadi, Bits and Characters Substitutions to Increase the Security Level of Transmitted Secret Message, International Journal of Computer Science and Mobile Computing, vol. 11, issue 9, pp. 11 – 28, 2022.

[42]. Dr. Mohamad T. Barakat et al, International Journal of Computer Science and Mobile Computing, Vol.11 Issue.10, October- 2022, pg. 24-47.

[43]. Adnan Manasreh, Prof. Ziad Alqadi, COVER IMAGE REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY, Journal of Engineering and Applied Sciences, vol. 17, issue 3, 2022, pp. 294-302.

[44]. Namer Ali Aletawi et al, International Journal of Computer Science and Mobile Computing, Vol.11 Issue.8, August- 2022, pg. 22-44.

[45]. Prof. Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.11 Issue.7, July- 2022, pg. 18-36.

[46]. Ziad Alqadi, Two PKs to Protect LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, Vol.11 Issue.8, August- 2022, pg. 45-66.

[47]. Qazem Jaber Ziad Alqadi, Multiple CLMMs Keys to Secure Message Transmission, International Journal of Computer Science and Mobile Computing, vol. 11, issue 7, 2022, pp. 18-36.

[48]. Dr Rushdi S Abu Zneit, Dr Ziad AlQadi, Dr Mohammad Abu Zalata, A Methodology to Create a Fingerprint for RGB Color Image, IJCSMC, vol. 6, issue 1, pp. 205-212, 2017.

[49]. Abdullah I Alhasanat, Khaled D Matrouk, Haitham A Alasha'ary, Ziad A Al-Qadi, Connectivity-based data gathering with path-constrained mobile sink in wireless sensor networks, Wireless Sensor Network, vol. 6, issue 6, 2014, DOI:10.4236/wsn.2014.66013.

[50]. Sundaram, K.T. (2022) “Digital Transformation with AI/ML & Cybersecurity,” *International Journal of Computer Science and Mobile Computing*, 11(11), pp. 1–3. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i11.001.

[51]. Sundaram, K.T. (2022) *Five key steps to realize the digital transformation value and ensuring a successful SAP HANA transformation in Global Organizations*, *Free Press Journal*. Available at: https://www.freepressjournal.in/business/five-key-steps-to-realize-the-digital-transformation-value-and-ensuring-a-successful-sap-hana-transformation-in-global-organizations.

[52]. Sundaram, K.T. (2022) “Five key steps realize the digital transformation value and ensure a successful SAP HANA transformation in Global Organizations,” *International Journal of Computer Science and Mobile Computing*, 11(10), pp. 116–118. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i10.009.

[53]. 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.

[54]. 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.

[55]. M. Abu-Faraj, A. Al-Hyari, I. Al-taharwa, B. Al-Ahmad, and Z. Alqadi, “CASDC: A Cryptographically Secure Data System Based on Two Private Key Images,” IEEE Access, vol. 10, pp. 126304-126314, 2022, doi:10.1109/ACCESS.2022.32263

[56]. 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.

[57]. 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, https://doi.org/10.3390/sym14040664.

[58]. 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.

[59]. 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.

[60]. M. Abu-Faraj, Z. Alqadi, and M. Zubi, “Creating Color Image Features Based on Morphology Image Processing,” Traitement du Signal, vol. 39, no. 3, pp. 797-803, 2022, doi:10.18280/ts.390304.

[61]. M. Abu-Faraj, Z. Alqadi, B. Al-Ahmad, K. Aldebei, and B. Ali, “A Novel Approach to Extract Color Image Features using Image Thinning,” Applied Mathematics & Information Sciences (AMIS), vol.16, no. 5, pp. 665-672, 2022, doi:10.18576/amis/160501.

[62]. M. Abu-Faraj, A. Al-Hyari, B. Al-Ahmad, Z. Alqadi, B. Ali, and A. Alhaj, “Building a Secure Image Cryptography System using Parallel Processing and Complicated Dynamic Length Private Key,” Applied Mathematics & Information Sciences (AMIS), vol. 16, no. 6, pp. 1017-1026, 2022, doi:10.18576/amis/160619.

[63]. M. Abu-Faraj, A. Al-Hyari, I. Al-taharwa, Z. Alqadi, and B. Ali, “Increasing the Security of Transmitted Text Messages Using Chaotic Key and Image Key Cryptography,” International Journal of Data and Network Science, vol. 7, no. 1, pp. 1-12, 2023, doi:10.5267/j.ijdns.2023.1.008.