Available Online at www.ijcsmc.com

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. 5, May 2023, pg.71 – 82

Simplified and Improved LSB2 (SILSB2) Method of Secret Message Steganography

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

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i05.008

Abstract:
A simplified and improved method based on LSB2 (SILSB2) method of secret message steganography will be introduced. The method will simplify the message hiding and extracting functions by reducing the set of operations used to hide and extract the secret message. The proposed method will work on inserting and retrieving the secret message in one go instead of inserting or retrieving it byte by byte as used in the classical methods. The introduced method will add a security issues to LSB2 method by using a special private key. This key will be used to divide the secret message into blocks, and each block will be hidden/extracted alone. The private key will be used also to define the staring locations in the covering-stego images, where to start hiding or extracting the message block. The private key will provide a good key space to protect the message from being hacked, the extracted message will be very sensitive to the private key values, any changes in these values will lead to extract a corrupted damaged message, and these changes will be considered as a hacking attempt. The introduced method will be tested and implemented using various messages and various covering images, the obtained results will be analyzed to prove the quality, security, sensitivity and the efficiency provided by the proposed method.

Keywords: Steganography, covering image, stego image, PK, patching, LSB, LSB2, SILSB2.

Introduction
Data steganography [1-10] is one of the easiest techniques used to protect secret data, and it means hiding confidential data in a medium of data media so that the concealment process does not affect the medium with no change in the medium being noticed using the naked eye in order to remove any doubt that the medium carries confidential data [11-15].

The sego process as shown in figure 1 contains two parts, the sending part and the receiving part. The sending part includes: secret message, covering image, stego image, private key (PK) (optional), and hiding function, while the receiving part includes: stego image, PK (optional), secret message, and extracting function [45-49].

It is recommended to use colored digital images [40-49]as a carrier medium for confidential data for the following reasons:

- Large image size, this size will increase the capacity of data hiding (maximum number of characters which can be hidden in the image) [18-25].

- Ease of processing, the color image can be represented by a 3D matrix (see figure 2), and the matrix manipulation can be applied very easy, the matrix can be easily reshaped to 1D matrix and vice versa, also any part of the image can be extracted and deployed for any application [12-17].
-

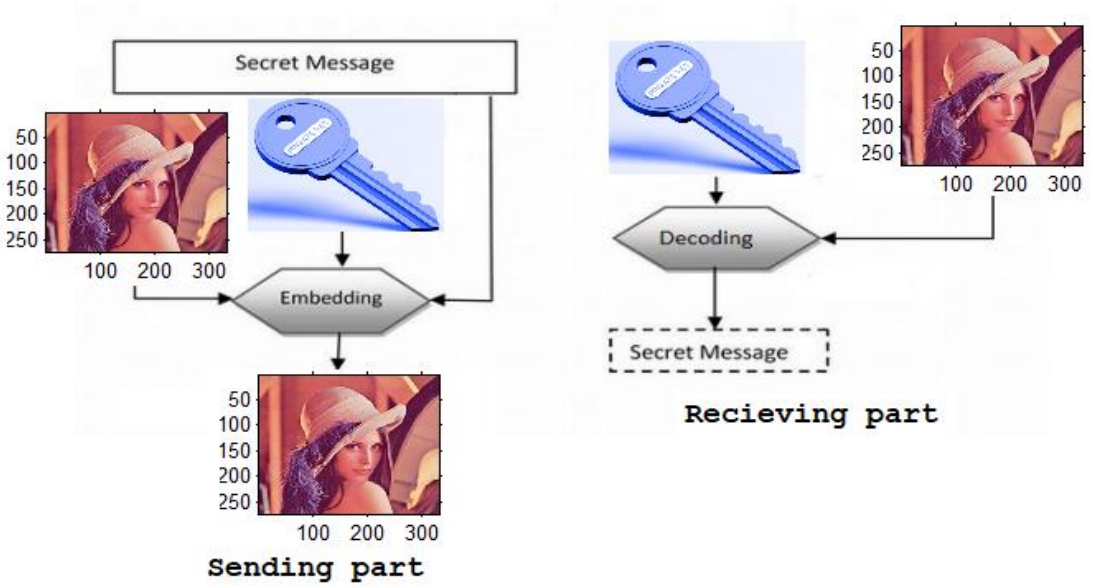


Figure 1: Stego system

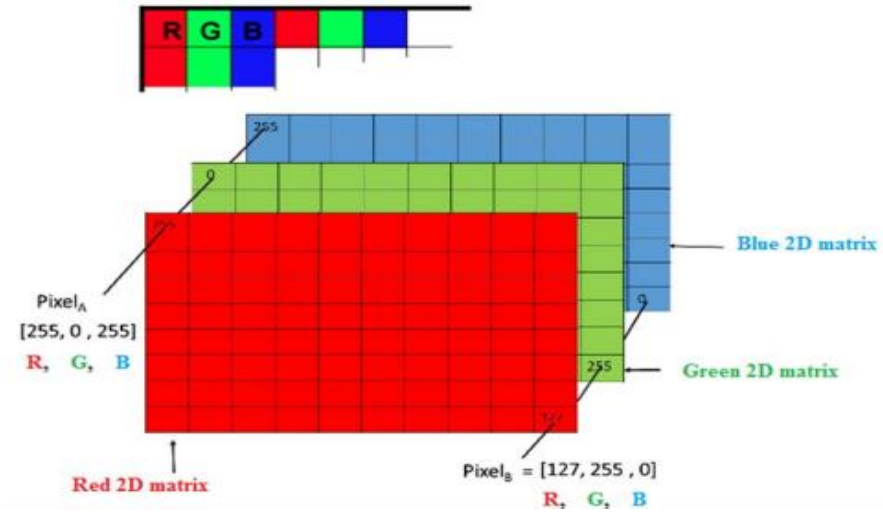


Figure 2: Color image 3D matrix

- The pixel's values have the same range (from 0 to 255) as for characters ASCII value, these values are unsigned inter 8 values (see figure 3), and it is very easy to convert them from decimal to binary and vice versa.
- Ease of obtaining a digital image due to the multiplicity of sources it provides and the multiplicity of equipment it generates.

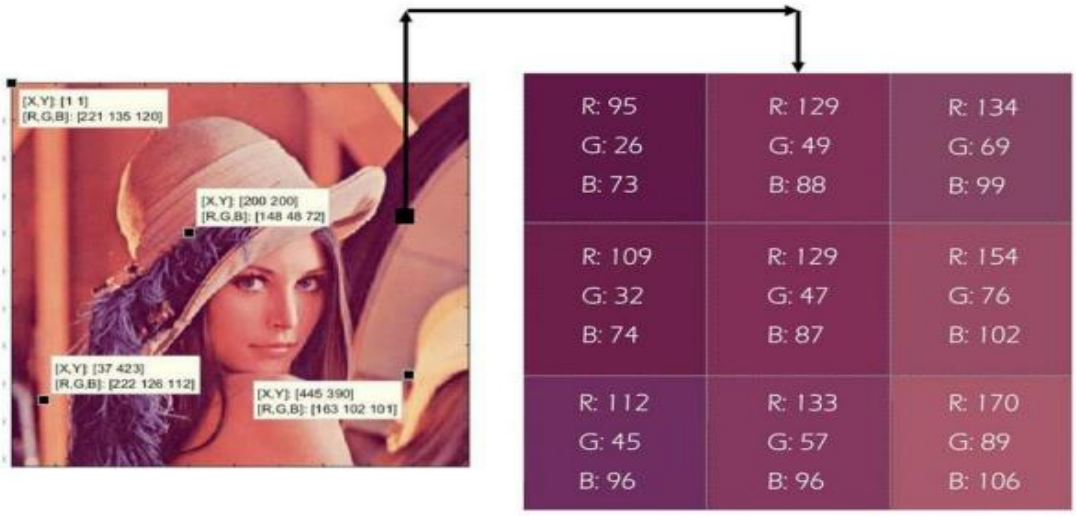
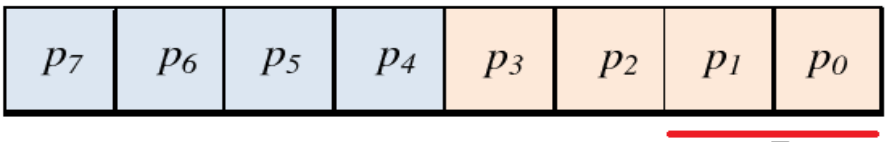


Figure 3: Color pixels' values

Many methods were introduced for message steganography, most of these methods were based on least significant bit (LSB) and LSB2 methods, these methods are not secure and they are very simple and easy to implement.
LSB and LSB2 methods use the same procedures for secret message hiding and extracting, LSB method uses the LSB bits of the covering bytes to hold the bits of the message, while LSB2 method uses the two LSB bits of the covering bytes to hold the message bits [26-30].
LSB2 method doubles the covering image capacity of hiding, and reserves 4 bytes from the covering image to hold one character from the secret message, the two LSBs of each covering byte are to be used to hold two bits from the message character (see figure 4). LSB2 method adds minor changes to the covering bytes and these changes are within the range -3 to +3 as shown in figure 4.
The LSB2 method allocates 4 consecutive bytes to be used to carry one character of the secret message (see figure 5), and this procedure needs to perform a series of logical operations, which will increase the number of instructions used in each of the hiding and extracting functions (see figure 6).



Covering bits	Message bits			
	00	01	10	11
	Stego bits			
00	00(no change)	01(+1)	10(+2)	11(+3)
01	00(-1)	01(no change)	10(+1)	11(+2)
10	00(-2)	01(-1)	10(no change)	11(+1)
11	00(-3)	01(-2)	10(-1)	11(no change)

Figure 4: Using two LSBs

Covering bytes	120	133	142	155
Binary	01111000	10000101	10001110	10011011
Holding byte (binary)	01111001	10000100	10001100	10011001
Holding bytes	121	132	140	153

Hiding A: D=65; B=01000001

Figure 5: LSB2 hiding example

```
s=[120 133 142 155]
 a1=65; %ASCII of A letter
 i=1;
s(i) = uint8(bitor(bitand(s(i),bitcmp(2^n-1,8)),bitshift(a1,-6)));
a=bitand(a1,48);
a=bitshift(a,2);
s(i+1)=uint8(bitor(bitand(s(i+1),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,12);
a=bitshift(a,4);
s(i+2)=uint8(bitor(bitand(s(i+2),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,3);
a=bitshift(a,6);
s(i+3)=uint8(bitor(bitand(s(i+3),bitcmp(2^n-1,8)),bitshift(a,-6)));
s
    s =
       121   132   140   153
```

LSB2 hiding procedures

```
i=1
d1=bitand(s(i),3);
d1=bitshift(d1,6)        d1 = 64
d2=bitand(s(i+1),3);
d2=bitshift(d2,4)        d2 = 0
d3=bitand(s(i+2),3);
d3=bitshift(d3,2)        d3 = 0
d4=bitand(s(i+3),3)      d4 = 1
d=d1+d2+d3+d4            d = 65
```

LSB2 extracting procedures

Figure 6: LSB2 procedures

The first objective of the proposed SILSB2 method is to reduce the hiding and extracting functions by reducing and simplifying the procedures needed to apply message hiding and message extracting.
The process of concealing the message in the digital image, as well as the process of retrieving the message from the carrier image, is not affected by the process of distributing the characters of the secret message in the image, and from this point of view, we suggest in the presented method to use the one-act operation in the concealment process and the retrieval process, by converting The binary values of the secret message into a two-column array and insert or retrieve them once as shown in the figures 7 and 8, these procedures will simplify the hiding and extracting functions used in the proposed method as shown in figure 9.

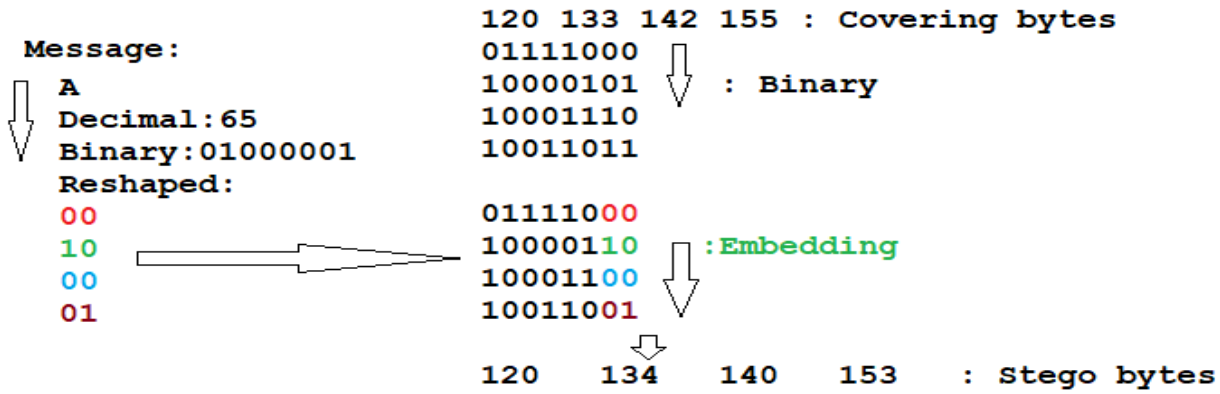


Figure 7: Proposed data hiding procedures

Figure 8: Proposed data extracting procedures

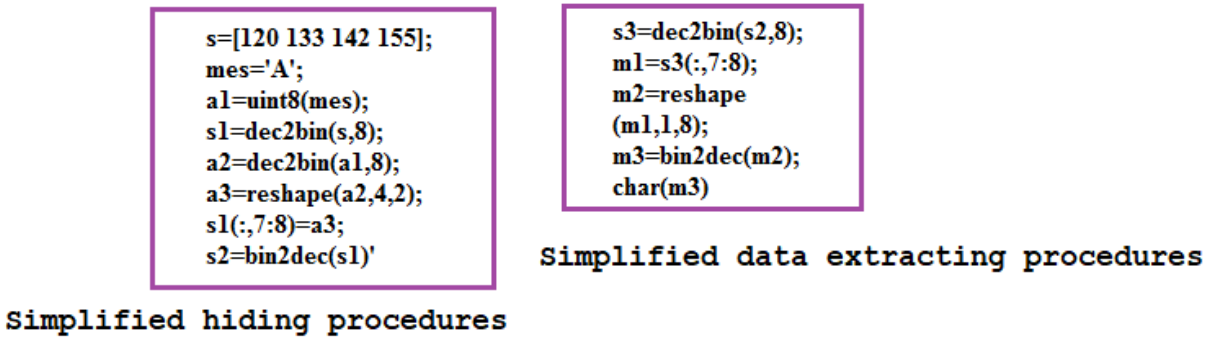


Figure 9: Simplified SILSB2 functions

In addition to hiding and extracting functions simplification the proposed method will aim to achieve the following requirements:

- Speed, the hiding time and the extracting time will be reduced, thus the throughput of the method will be increased.
- Security, the method will use a PK, this key must be used in both the hiding and extracting phases, and the PK will provide a key space capable to resist hacking attacks.
- Sensitivity, the extracting phase must use the same PK as in the hiding phase, any minor changes in the PK in the extracting phase will be considered as a hacking attempt by extracting a corrupted damaged message.
- High quality of the stego image, the stego image will be closed to covering image and the quality factors measured between the two images must be as follows: low MSE (mean square error) [35-41], High PSNR (peak signal to noise ratio), High CC (correlation coefficient) and low NPCR (number of pixels change rate) [30-34].

The Proposed Method

The proposed method provides a high level protection for the secret message by using a special PK, this PK contains three values a two fractional values to find the starting of the covering image block and the third one is to be used to determine the number of message blocks. The secret message is to be divided into blocks and each block is to embedded-extracted from the image separately, and table 1 shows the structure of the PK:

Table 1: PK structure

PK	
SS1	SS2
NB	L
Example	
0.0179	0.246
8	46

Each message block is to be hidden-extracted sing patching method as shown in figures 7 and 8 and the hiding phase of SILSB2 method can be implemented applying the following steps:

Step 1:

Data preparation: Get the covering image, retrieve the image size, reshape the image matrix from 3d to one row matrix, get the message, retrieve the message length, convert the message to decimal, this step can be implemented applying the following sequence of mat lab instructions:


```
CI1=imread('C:\Users\Dr.Tayseer\Desktop\stimages\house.tiff');
[n1 n2 n3]=size(CI1);s=n1*n2*n3;
CI=reshape(CI1,1,s);
mes='Secret message cryptography';
m1=uint8(mes);
L=length(m1);
```

Step 2:

Get the PK; Assign values for the PK components, calculate the starting location, find the block length, find the length of the last message block, this step can be implemented applying the following sequence of mat lab instructions:

```
SS1=0.012;SS2=0.0179;
POS=fix(SS1*s)+fix(SS2*s);
NB=4;
P=fix(L/NB);
LST=L-P*NB;
```

Step 3:

Message hiding: For each message block do the following:

a) Get the message block.
b) Convert the message block to binary.
c) Reshape the resulting binary matrix into two columns matrix.
d) Get the image block.
e) Convert the image block to binary.
f) Let the two LSBs of the binary block equal the two column matrix.
g) Convert the image block back to decimal

Do the same steps for the last block and reshape back the image to 3D matrix to get the stego image, this step can be implemented applying the following sequence of mat lab instructions:

```
for i=1:NB
    b1=CI(1,POS+(i-1)*P*4+1:POS+i*P*4);
    b2=dec2bin(b1,8);
    m2=m1(1,(i-1)*P+1:i*P,:);
    m3=dec2bin(m2,8);
    m4=reshape(m3,P*4,2);
    b2(:,7:8)=m4;
    b3=bin2dec(b2)';
    CI(1,POS+(i-1)*P*4+1: POS+i*P*4)=b3;
end
if(LST>0)
       b4=CI(1,POS+NB*P*4+1:POS+NB*P*4+LST*4);
    b5=dec2bin(b4,8);
    m5=m1(1,NB*P+1:NB*P+LST,:);
    m6=dec2bin(m5,8);
    m7=reshape(m6,LST*4,2);
    b5(:,7:8)=m7;
    b6=bin2dec(b5)';
    CI(1,POS+NB*P*4+1: POS+NB*P*4+LST*4)=b6;
end
SI=reshape(CI,n1,n2,n3);
```

The message extraction phase can be implemented applying the following steps:

Use the same steps as for message hiding (step1 and step2).

Step3:

Message extraction: create an empty message, for each message block do the following:

a) Get the stego block.
b) Convert the stego block to binary.

c) Extract the last two columns from the binary matrix.
d) Reshape the two column matrix to 8 columns matrix.
e) Convert the resulting matrix to decimal.
f) Append the decimals to the message.

Convert the decimal matrix to characters to get the secret message, this step can be implemented applying the following sequence of mat lab instructions:

```
dmes=[];
for i=1:NB1
        b11=SI1(1,POS+(i-1)*P1*4+1:POS+i*P1*4);
    b22=dec2bin(b11,8);
    m333(1:P1*4,:)=b22(:,7:8);
    m444=reshape(m333,P1,8);
    m555=bin2dec(m444)';
    dmes=[dmes m555];
end
if(LST>0)
       b44=SI1(1,POS+NB1*P1*4+1:POS+NB1*P1*4+LST1*4);
    b55=dec2bin(b44,8);
    m666(1:LST1*4,:)=b55(:,7:8);
    m777=reshape(m666,LST1,8);
    m888=bin2dec(m777)';
    dmes=[dmes m888];
end
      char(dmes)
```

Implementation and Results Discussion

The proposed SILLSB2 method was implemented using various messages, and various covering images, the images were selected from the data base: USC-SIPI: http:// sipi.usc.edu/database/. A set of results analysis approaches were performed, below these approaches will be discussed.

a) Security and sensitivity analysis

The proposed method uses 4 values in the PK to apply message hiding and message extracting, these values will give as shown in equation1 a good key space capable to resist hacking attacks:

$$\text{Key space} = 2^{4*64} = 2^{256} \quad (1)$$

The extracted message is very sensitive to the selected PK, the hiding and extracting phase must use the same PK, any minor changes in the PK during the extracting phase will be considered as a hacking attempt by producing a damaged corrupted message. To prove this fact, the message 'Secret message steganography using SILSB2 method' Was hidden using the following PK, the hidden message was extracted once for each of the following changes shown in table 2, as we can see from the obtained messages (image house.tiff was selected as a covering image),
any changes in the PK will damage the message, also using CLSB or CLLSB2 method will lead to extract a damaged message.

```
PK:
SS1=0.012;SS2=0.0179;
NB=4; L=49
```


Table 2: SILSB2 method sensitivity

Used method	Changes in the PK	Extracted message
SILSB2	No changes	Secret message steganography using SILSB2 method
SILSB2	SS1=0.013	Ç□(£0□nÕ□¸ìÛÀÔéÒ¤Édv}Ý□NOb2Ô□ÈÈôè ?~éù□ ï^T¸|VFå:
SILSB2	SS2=0.0178	@â□à9Lbî□qß□¢Haî Ì□□ÐÝP□Õè@ÊÊççÅ]□□È□èÊÎÃÍÎÎ□□□□Þt
SILSB2	NB=3	df"dfBBh□aEFÓûâÅÐÌÝÞ□□□□ßÒ□□¼°´½°□□³³+ 7□□□□Krlad
SILSB2	NB=5	□22ptpS}vÌ\□□□□3;□ÏÇÆ□□□□ÌÀä÷ ÷óaèÃà□/?rpvRX□□y□□
CLSB	No PK	.□□□o¸□□è□□£§ëî□□{e□×î-□h□>l\`□□ŠY□□m&N>□8X¸<□`±□
CLSB2	No PK	□□Yl□{ _>(I□ □□Yè□¶□□^□□f□36e¦{(¥)1□¢□s□□¥□S□¦{□

b) Quality analysis

The stego image must be closed to the covering image, the proposed method provides a good quality of the stego image, to show this, the method was implemented using various messages (short and long), image 2.2.01.tiff was selected as a covering image, the quality parameters between the covering and stego image were calculated, table 3 shows the obtained results:

Table 3: Quality of the stego images

Message length (character)	MSE	PSNR	CCr, CCg, CCb	NPCR %
100	0.00030422	190.2542	1, 1, 1	0.0089
200	0.00063578	182.8832	1, 1, 1	0.0190
400	0.0012	176.4017	1, 1, 1	0.0376
500	0.0016	173.8958	1, 1, 1	0.0477
1000	0.0033	166.4477	1, 1, 1	0.0970
2000	0.0064	159.7613	1, 1, 1	0.1912
4000	0.0127	152.9241	1, 1, 1	0.3834
5000	0.0161	150.5536	1, 1, 1	0.4807
10000	0.0317	143.7845	1, 1, 1	0.9506
50000	0.1583	127.7093	0.999, 1, 1	4.7632
100000	0.3168	120.7729	0.99, 1, 1	9.5261
Remarks	Low	high	Closed to 1	Low

From table 3 we can see that the proposed method satisfies the quality requirements even for long messages, the quality of the stego image can be examined visually, figure 10 shows a stego image holding 10000 charters message, the stego image is close to the covering image and the stego image histograms are also closed to the covering image histograms.

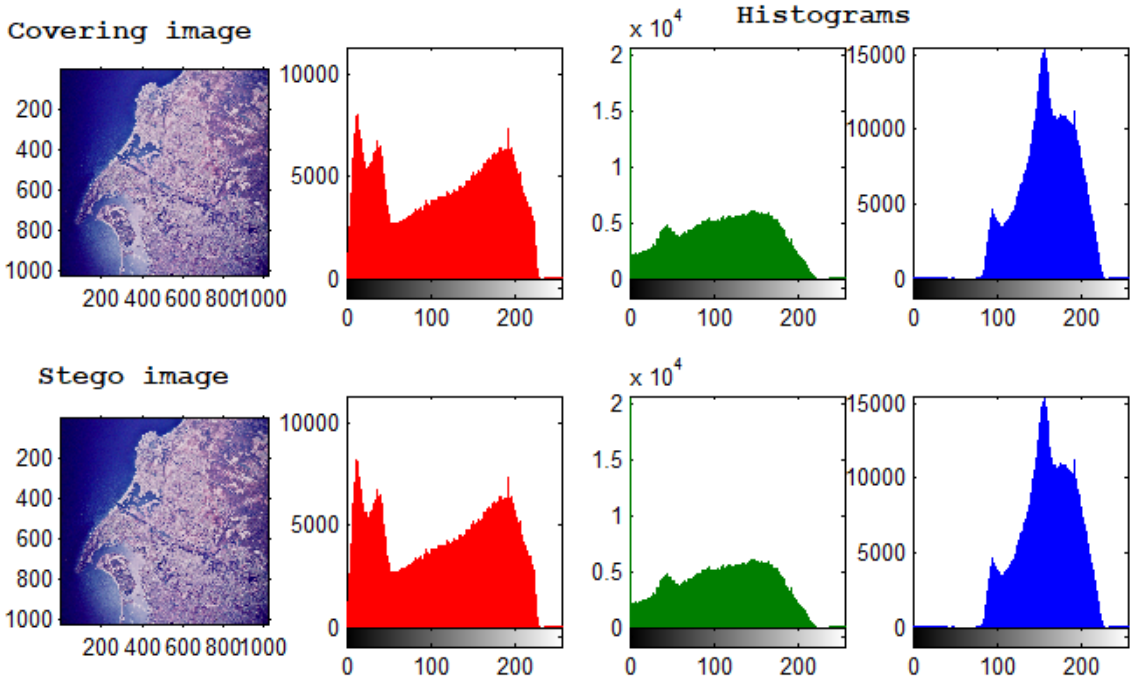


Figure 10: Stego image holding 10000 characters' message

c) Speed analysis

For the selected messages the hiding time (HT), extracting time (ET), hiding throughput (HTP) and extracting throughput (ETP) were calculated, table 4 shows the obtained results:

Table 4:Speed parameters of SILSB2 method

Message length (character)	HT(seconds)	ET(seconds)	HTP(K bytes per second)	ETP(K bytes per second)
100	0.0157	0.0021	6.2113	46.3573
200	0.0173	0.0027	11.2663	72.9595
400	0.0204	0.0034	19.1611	115.2354
500	0.0219	0.0038	22.3310	127.0507
1000	0.0297	0.0062	32.9161	158.1657
2000	0.0457	0.0104	42.7503	187.2172
4000	0.0742	0.0175	52.6433	223.1097
5000	0.0896	0.0224	54.4667	218.3541
10000	0.1777	0.0405	54.9666	241.1843
50000	0.8080	0.2158	60.4334	226.3164
100000	1.5212	0.4203	64.1950	232.3552

From table 4 we can see the following facts:

- The proposed method provided a good speed parameters, even for long message with 100 K bytes required 1.5 seconds for hiding and 0.4 seconds for extracting, and these are high speed parameters (see figure 11).
- Increasing the message length will slowly increase the hiding time and fast increasing the hiding throughput.
- Extracting phase required less extraction time, the extraction throughput rapidly increases when increasing the message length.

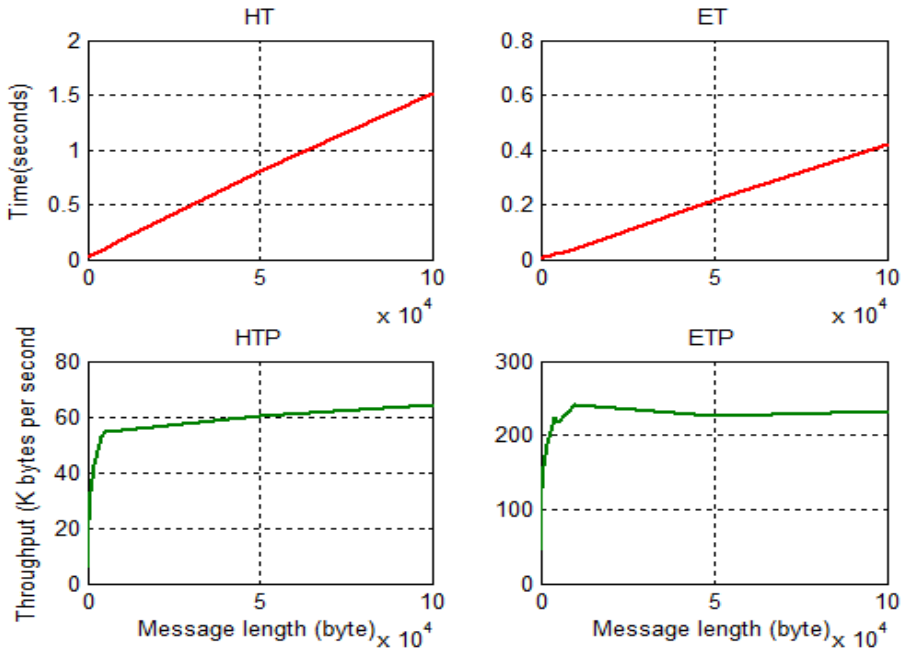


Figure 11: Speed parameters vs message length

Conclusion

A simplified method of message steganography was proposed, the method simplified the processes of message hiding and message extracting by replacing a set of used in other method logical operations by a simple patch way for message bits hiding and message bits extracting. The proposed SILSB2 method was based on LSB2 method and it used a PK to protect the hidden message from being hacked. The PK provided a good key space and the obtained extracted message was very sensitive to the selected values of the PK, any minor changes in the PK in the extraction phase produced a damaged corrupted secret message. The PK was used to divide the message into blocks and to determine the starting location of the covering block, each message block was treated separately.

The proposed method was tested using short and long messages and it was shown that for any message, with any length the proposed method operated efficiently.

The obtained results were analyzed and the results analysis were used to prove the enhancement provided by the proposed method in: security, speed, quality and sensitivity.

References

[1]. Kaur, R. Dhir, & G. Sikka,"A new image steganography based on first component alteration technique", International Journal of Computer Science and Information Security (IJCSIS), 6, pp.53-56, 2009.http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf.

[2]. Alvaro Martin, Guillermo Sapiro, &GadielSeroussi,"Is Steganography Natural", IEEE Transactions on Image Processing, 14(12), pp.2040-2050, 2005.doi: 10.1109/TIP.2005.859370 .

[3]. Bhattacharyya, A. Roy, P. Roy, & T. Kim,"Receiver compatible data hiding in color image", International Journal of Advanced Science and Technology, 6, pp.15-24, 2009.http://www.sersc.org/journals/IJAST/vol6/2.pdf .

[4]. EE. KisikChang, J. Changho, & L. Sangjin,"High Quality Perceptual Steganographic Techniques", Springer. 2939, pp.518-531, 2004.doi: 10.1007/978-3-540-24624-4_42, http://www.springerlink.com/content/c6guuj5xnyy4wj3c/ .

[5]. C. Kessler,"Steganography: Hiding Data within Data" An edited version of this paper with the title "Hiding Data in Data", Windows & .NET Magazine, 2001. [Online] Available: http://www.garykessler.net/library/steganography.html (October 4,2011).

[6]. Gandharba Swain, &S.K.lenka,"Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking. 2(1), pp.35-39, 2010. ISSN: 0975-7163. http://www.serialspublications.com/journals1.asp?jid=436&jtype.

[7]. Hideki Noda, Michiharu Nimi, & Eiji Kawaguchi, "High- performance JPEG steganography using Quantization index modulation in DCT domain", Pattern Recognition Letters, 27, pp.455-46, 2006.http://ds.lib.kyutech.ac.jp/dspace/bitstream/10228/450/1/repository6.pdf .

[8]. Kathryn,"A Java Steganography Tool", 2005.http://diit.sourceforge.net/files/Proposal.pdf .
[9]. Motameni, M.Norouzi, M.Jahandar, & A. Hatami,"Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, 24, pp.349-354, 2007. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf.
[10]. Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3): 57-62, 2012.http://www.ijacsa.thesai.org.
[11]. Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", International Science and Technology Conference (ISTEC 2012), Dubai, December 13-15, 2012. http://www.iste-c.net
[12]. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKETINFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol.9, issue 2, pp. 2319,2020.
[13]. 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.
[14]. Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.
[15]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, vol. 151, issue 4, pp. 1-4, 2016.
[16]. Musbah Aqel, Ziad Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp. 45-52, 2009.
[17]. 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 .
[18]. 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, pp. 20-33, 2019.
[19]. J Al-Azzeh M Abuzalata, Ziad Alqadi, Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing, vol. 8, issue 2, pp. 93-103, 2019.
[20]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp.288-298, 2007.
[21]. Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology &Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.
[22]. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
[23]. 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, vol. 153, issue 2, pp. 31-34, 2016.
[24]. 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.
[25]. 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.
[26]. Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
[27]. Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, pp. 262-265, 2019.
[28]. 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. 18, issue 3, pp. 76-90, 2019.
[29]. 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, 2019.
[30]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306-319,2019.
[31]. Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, International Journal of Computer Science and Mobile Computing, vol. 8, issue 6, pp. 106-123,2019.
[32]. Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Improving the security of LSB image steganography, JOIV: International Journal on Informatics Visualization, vol. 3, issue 4, pp. 384-387, 2019.

[33]. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, 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, pp. 748-754, 2019.

[34]. ZIAD ALQADI, A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES, Journal of Theoretical and Applied Information Technology, vol. 96, issue 10, pp. 3014-3024,2018.

[35]. 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.

[36]. Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[37]. Jihad Nader 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

[38]. Dr. Mohammad S. Khrisat; Prof. Ziad A. Alqad, Using Logical Operations to SecureLSB2 Data Steganography, IJCSMC, Vol. 9, Issue. 11, PP.70 – 76, November 2020.

[39]. 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.

[40]. 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.

[41]. 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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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.

[46]. Namer Ali Aletawi; Mansour A. Abu Sameha; Prof. Ziad Alqadi**,** Modified LSB2 Steganography Method to Secure the Embedded Secret Message**,** IJCSMC, Vol. 11, Issue. 8, August 2022, pg.22 – 44**,** DOI: https://doi.org/10.47760/ijcsmc.2022.v11i08.003**.**

[47]. 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.

[48]. 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.

[49]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB color image encryption-decryption using image segmentation and matrix multiplication, International Journal of Engineering & Technology, vol. 7, issue 3.13, pp. 104-107, 2018.

