VOL. 18, NO. 7, APRIL 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURING LSB STEGANOGRAPHY USING BITE SUBSTITUTION AND IMAGE BLOCKING

Adnan Manasreh[1], Nasser Abdellatif[1] and Ziad A. Alqadi[2]
[1]Department of Electrical Engineering, Applied Science Private University, Amman, Jordan
[2]Department of Computer Engineering, Faculty of Engineering Technology, AL-Balqa Applied University, Amman, Jordan
E-Mail: adnan_m@asu.edu.jo

ABSTRACT

Protecting secret messages is a vital issue, in this paper's research, a simplified, highly secure method of message steganography will be introduced. The proposed method will use a complicated PK, which contains information to select a secret block from the color image to be used as a covering block; also it will contain the values of the chaotic logistic map model to run this model to generate the indices key needed to substitute the message binary matrix. The PK will provide a huge keyspace capable to resist hacking attacks, the extracted message will be very sensitive to any minor changes in the PK, and any changes in this key during the extraction phase will be considered a hacking attempt by producing a damaged extracted message. It will be shown that the proposed method will be always efficient when changing the message length and changing the covering images. The proposed method will be implemented using various messages and various covering images, the obtained results will be analyzed using various types of data analysis methods to prove the improvements provided by the proposed method (quality, security, and efficiency).

Keywords: steganography, PK, CLK, CLMM, IK, MSE, PSNR, CC, NSCR.

Manuscript Received 5 January 2023; Revised 6 May 2023; Published 30 May 2023

ABBREVIATIONS

The following abbreviations are used in this research paper:

PK : private key
CLK : chaotic logistic key
IK : indices key
CLMM : chaotic logistic map model
MBM : message binary matrix
ET : extraction time
HT : hiding time
ETP : extracting throughput
HTP : hiding throughput
MSE : mean square error
PSNR : peak signal-to-noise ratio
CC : correlation coefficient
NSCR : number of samples change ratio

INTRODUCTION

Text messages are widely circulated through various social media, which requires protecting them from the risk of penetration or theft by hackers and data thieves for the following reasons:

- The text message may be personal or private
- The text message may be confidential or contain confidential information
- The means of communication used to transmit the message may not be secure

One of the most popular methods of protecting secret messages is message steganography. Message steganography is the process of hiding a secret message within a covering media in such a way that someone can not know the presence or contents of the hidden message. The purpose of steganography is to maintain secret communication between the message sender and the message receiver. Unlike cryptography, which conceals the contents of a secret message, steganography conceals the very fact that a message is communicated. Although steganography differs from cryptography, there are many analogies between the two, and some authors classify steganography as a form of cryptography since hidden communication is a type of secret message [1-5].

Up to now, cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However, nowadays steganography techniques are used increasingly besides cryptography to add more protective layers to the hidden data. The advantage of using steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal [6-9].

As shown in Figure-1, both the original image file(X) and secret message (M) that needs to be hidden are fed into a steganographic encoder as input. Steganographic Encoder function, f(X, M, and K) embeds the secret message into a cover image file by using techniques like least significant bit encoding. The resulting stego image looks very similar to your cover image file, with no visible changes. This completes encoding. To retrieve the secret message, the stego object is fed into Steganographic Decoder.

Many methods were introduced to apply message steganography; many of these methods were based on the classical LSB method. The LSB method reserves the LSBs (see Figure 2) of the covering image to hold the bits of the

ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

secret message and it can be implemented by applying the following algorithm [10-15]:

1. Select an image and convert it into binary
2. Convert the secret message into binary
3. **while** until all message bits are embedded
4. Chose one pixel of an image and divide it into three channels: red, green and blue
5. Select next three message bits sequence
6. Replace LSB of each red, green and blue channel with these message bits
7. **end while**
8. Set the image to a new value and save it

In the classical LSB technique of message hiding, bits of the message are directly embedded into the LSB of the cover image in a deterministic sequence. This modification does not provide any impact on human perception due to the amplitude of the change being small. In terms of a 24-bit RGB image, each pixel is derived from three primary colors: red, green, and blue, and each primary color is represented by 8 bits. One can store 3 bits in each pixel by changing a bit of each of the red, green, and blue color components. For example, inside the 24-bit image, we have three adjacent pixels (9 bytes), which are shown in Figure-3(a). Assume, we want to hide the letter 'a' (ASCII code of 'a' is 97, which is 01100001 in binary). Superimposing these 8 bits in sequence over the LSB of the 9 bytes above, we get the result as in Figure-3(b), (where bits in bold and underline indicate changes). In this way, message bits can be embedded in the cover image generating the stego-image from which the message bit can be extracted. Figure-2, describes this overall process of LSB strategy [15-20].

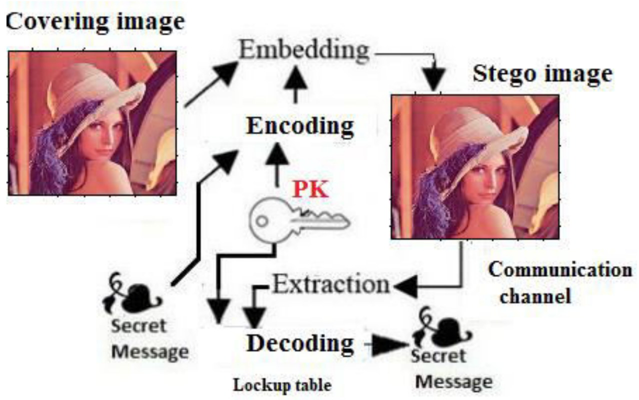

Figure-1. Data steganography model.

Figure-2. LSB of the covering byte.

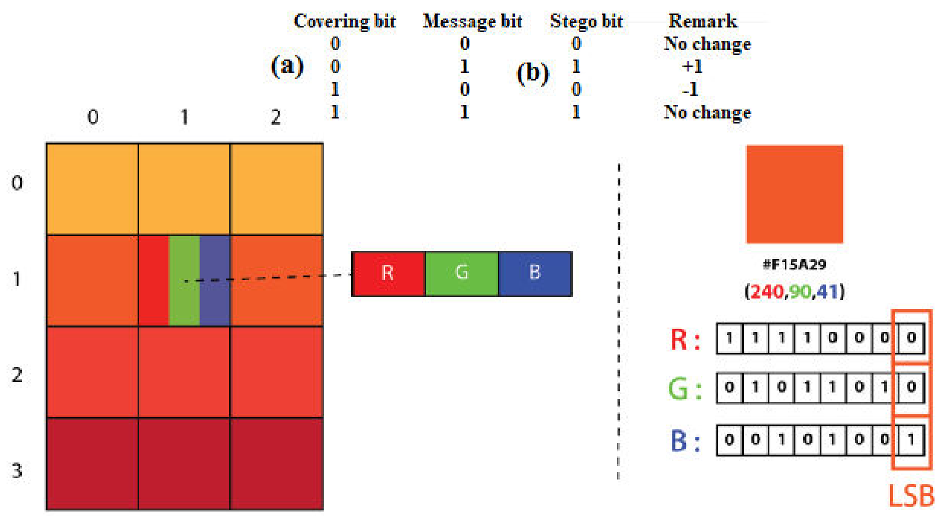

Figure-3. LSB Process of hiding.

The LSB method has the following features:

- LSB reserves 8 bytes from the covering image to hide one character from the secret message.
- The charterers are to be hidden in order, the first 8 bits of the covering image for the first character, the second 8 bits for the second character, and so on [21-25].
- LSB has a good stego image quality, it adds minor changes to the covering image, the covering byte change is within the range -1 to +1 (see Figure-4), this will keep the stego image closed to the covering image and the changes cannot be noticed by human eyes.
- Dealing with the hiding process character by character will require more time, this process will be simplified in the proposed here method [25-30].
- LSB method of steganography is not secure; anyone with good programming skills can easily extract the message from the stego image, knowing that this image is holding a message. The proposed method will solve this disadvantage by using a complicated PK to handle the process of message hiding and extracting

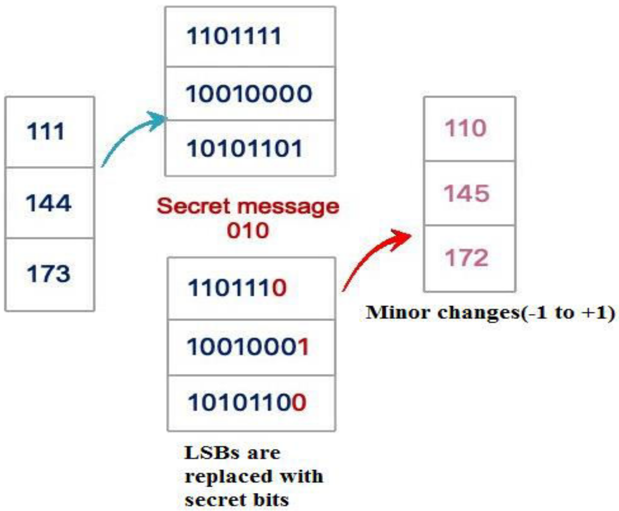

Figure-4. The LSB method adds minor changes to the covering image.

Digital color images are used most of the time as a covering media for the following reasons [28-30]:

- The digital color image has a very high resolution, thus the size of the digital color image is very huge, which enables us to hide large messages [35-40].
- The possibility of obtaining a digital color image at no cost due to the diversity of sources and the availability of various equipment that generates the digital image [15-20].
- Ease of processing color digital image because it is represented by a three-dimensional matrix (one dimension of a 2D matrix for each color channel (red, green, blue)) as shown in Figure-5.
- Ease of reshaping the three-dimensional matrix and converting it to a vertical or linear matrix with one dimension [25-30].
- The possibility of separating the matrix of each color and dealing with it separately and independently.
- Ease of checking the quality of a digital color image by looking at the image itself with the naked eye or using the color distribution scheme in the digital image (image histogram), see Figure-6.
- The pixel values in the digital image are true and positive numeric values, confined between 0 and 255, and are easy to convert into binary values; these values match the ASCII values of the message characters [31-40].

ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

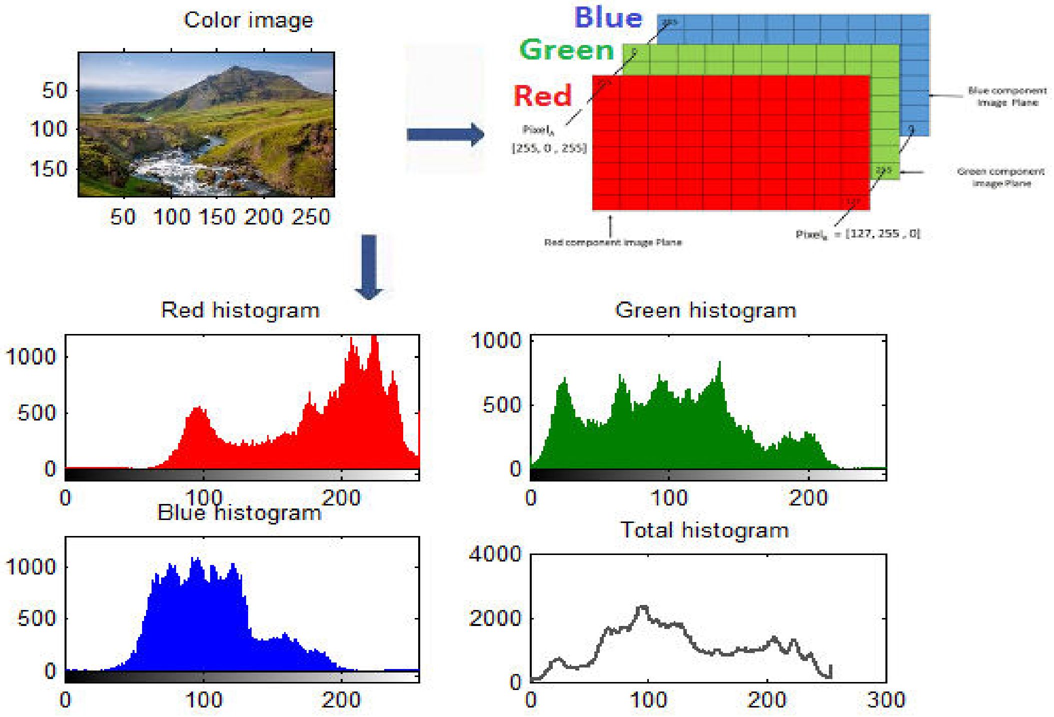

Figure-5. Color image and color channels.

There are currently several ways to hide any text message in a color image; most of these methods are based on the least significant bit (LSB) [16]. A complete survey of the most known steganography methods can be found in [17, 1 LSB-dependent approach is popular because it is easy to implement, despite its several disadvantages. To hide a secret message inside an image, a proper cover image is needed. LSB methods use bits of each pixel in the image, accordingly if we want to compress the cover.

Image it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformation of a lossy compression algorithm. Using Gray images each pixel has one value which means that we can hide just one bit. On the other hand with a 24-bit color image each pixel has three values Red, Green, and Blue color components which can be used, so a total of 3 bits can be stored in each pixel. The main disadvantage of standard LSB methods it is easy to detect the hidden message since it is simply the least significant bit in each pixel. To overcome this disadvantage many algorithms have been proposed to enhance LSB and make it less detectable and more secure [19, 20]. Other methods [21, 22], try to increase the amount of data that can be hidden in the cover image and pre-encrypt the message before hiding it in the cover image. The next two subsections discuss in detail the basic operation of two LSB standard methods. Each method has been implemented using messages with different lengths. The implementations record four values (mean square error, peak signal-to-noise ratio, hiding time, and retrieving time) that we will use to compare with our algorithm.

In [22] the author showed that the classic LSB method and introduced a method to enhance the LSB efficiency by increasing the PSNR and decreasing the hiding/extracting time.

A method of data steganography will be considered as a good method if it satisfies the requirements of quality, this means that the quality of the stego image must be high. The process of hiding the secret message in the digital image should not affect the image much, so that the stego image remains very close to the covering image, and the changes should not be noticed with the naked eye (see Figure-6). Therefore, the good method of the hiding process must meet the quality conditions shown in Table-1.

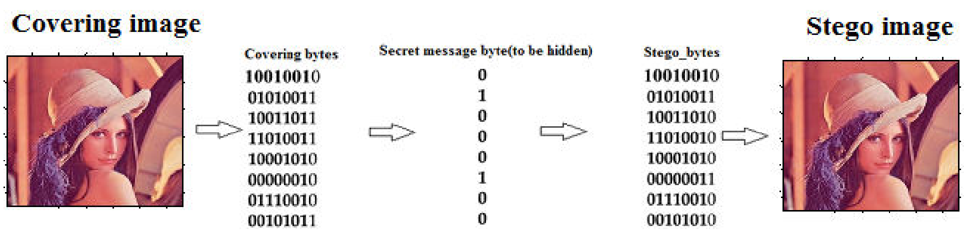

Figure-6. The Stego image is close to the covering image.

Table-1. Quality requirements.

Quality parameter	**Measured between the covering and stego images**
MSE	Very low
PSNR	Very high
CC	Closed to 1
NSCR	Closed to 0

PROPOSED PK

The proposed method uses a complicated PK which will be used with a simplified LSB method to apply message hiding and message extracting. The PK contains the needed information to process the following tasks:

- Selecting a block from the covering image to be used as a covering block.
- Apply message binary matrix substitution based on the generated indices key.

The PK contains the parameters shown in Table-2:

Table-2. PK structure.

PK	
Blocking information	
Lower rows percentage (rp1)	Upper rows percentage(rp2)
Lower columns percentage (cp1)	Upper columns percentage(*cp2*)
CLMM information	
R1	X1
Example	
0.17	0.35
0.2	0.45
3.77	0.125

The blocking information are used to get a block from the covering image, this block will hold a secret message, the information will be used to calculate the lower left and the upper right corners of the required block as shown in Figure-7.

The selected covering block is very sensitive to the blocking information, any minor changes in this information will change the block, changing the covering image will also change the block size, because the block size is a percentage of the selected covering image (see Figures 8, 9 and 10).

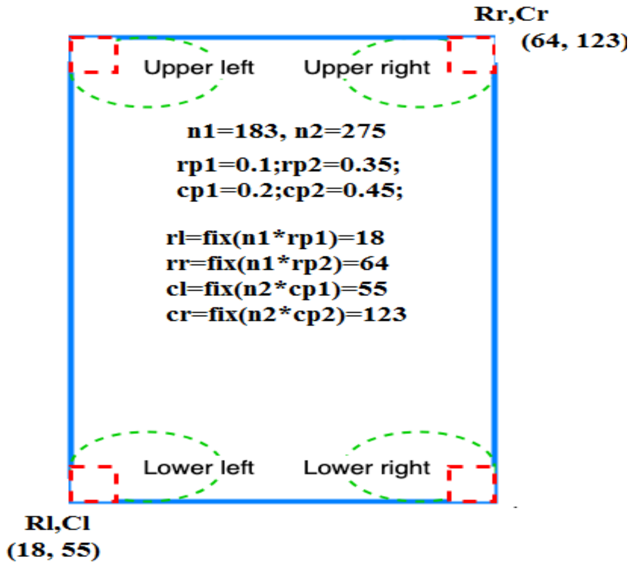

Figure-7. Block calculations.

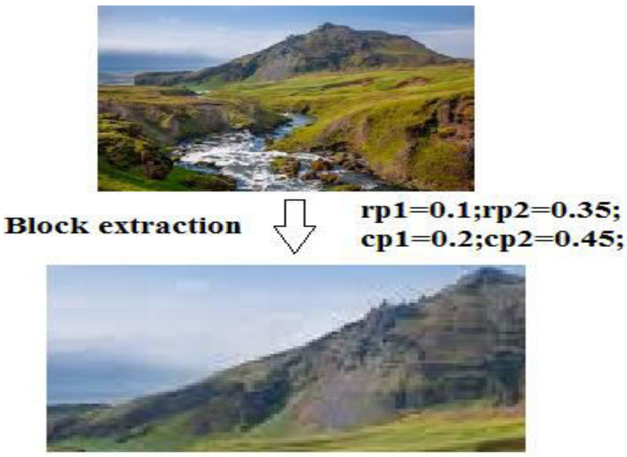

Figure-8. Block example.

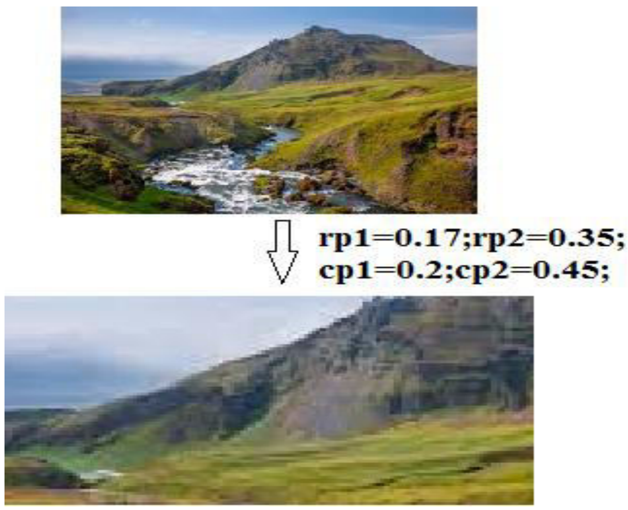

Figure-9. Changing blocking information changes the block.

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

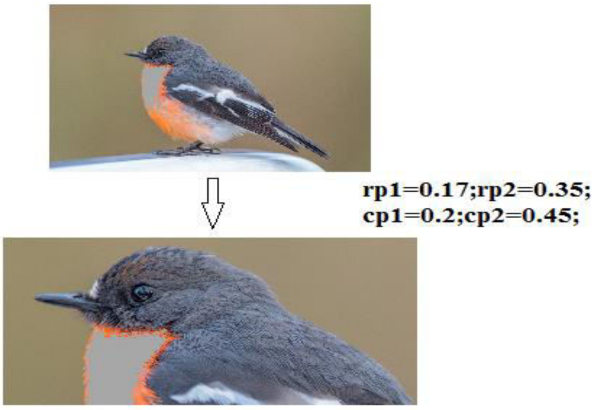

Figure-10. Changing the covering image changes the block.

The CLMM information is used to generate the indices key to be used for message binary matrix; this key can be obtained by sorting the CLK obtained as a result of running the CLMM with the selected chaotic parameters values.

The logistic map is defined by equation 1:

$$x_{n+1} = \mathbf{r}\, x_n(1 - x_n) \quad \text{with} \quad n = 0, 1, 2, 3... \qquad \textbf{(1)}$$

Given the starting value $0 \leq x_0 \leq 1$ and a positive parameter $0 < \mathbf{r} < 4$ the map produces a sequence of values:

$$x_0, x_1, x_2, \ldots$$

that we get by iterating it, e.g.

$$x_1 = \mathbf{r}\, x_0(1 - x_0)$$

$$x_2 = \mathbf{r}\, x_1(1 - x_1)$$

$$\ldots$$

The IK will contain 8 elements with values within the range 1 to 8 without repeating the same value. The generated IK will be very sensitive to the values of chaotic logistic parameters R1 and X1; any changes in these values will change the generated IK, Table-3 shows various IK generated as a result of using different values for R1 and X1.

Table-3. IK sensitivity.

R1, X1	CLK	IK
3.77; 0.125	0.4123 0.9135 0.2978 0.7884 0.6290 0.8797 0.3989 0.9039	3 7 1 5 4 6 8 2
3.91; 0.125	0.4277 0.9570 0.1608 0.5275 0.9745 0.0970 0.3426 0.8806	6 3 7 1 4 8 2 5
3.77; 0.2	0.6032 0.9023 0.3322 0.8363 0.5160 0.9415 0.2075 0.6200	7 3 5 1 8 4 2 6
3.95; 0. 25	0.7406 0.7588 0.7230 0.7912 0.6527 0.8955 0.3698 0.9205	7 5 3 1 2 4 6 8

THE PROPOSED METHOD

The proposed method uses the PK shown in Table-1; the process of message hiding will be implemented in three phases:

Phase 1: Image blocking

This phase can be implemented applying the following steps:

Step 1: Get the covering color image.
Step 2: Get the covering image size (rows and columns)
Step 3: From the PK get the blocking information.
Step 4: Use the blocking information to find the required block.

The following sequence of operations can be used to implement this phase:

```
aa=imread('E:\my_images\a12.jpg');
[n1 n2 n3]=size(aa);ss=n1*n2*n3;
a=aa;
%PK:
%Blocking information
rp1=0.17;rp2=0.35;
cp1=0.2;cp2=0.45;
%Chaotic logistic parameters
R1=3.95;X1=0.25;
r1=fix(n1*rp1);
r2=fix(n1*rp2);
c1=fix(n2*cp1);
c2=fix(n2*cp2);
%The required block
b=a(r1:r1+r2,c1:c1+c2,:);[nn1 nn2 nn3]=size(b);
```

Phase 2: MBM substitution

This phase can be implemented using the generated IK, and it can be implemented by applying the following steps:

Step 1: From the PK get the CLMM parameters value.
Step 2: Run the CLMM to get an 8 elements CLK
Step 3: Convert CLK to IK using sort function
Step 4: Get the message and retrieve the message size (L)
Step 5: Convert the message to decimal (ASCII values)
Step 6: Convert the decimal message to binary to get a message binary matrix (MBM)
Step 7: Use IK to substitute MBM

The following sequence of operations can be used to implement this phase:

```
%IK generation
for i=1:8
    X1=R1*X1*(1-X1);
    CLK1(i)=X1;
end
[d key1]=sort(CLK1);
m='The art of data steganography';
m1=uint8(m);
L=length(m1);
%MBM
m22=dec2bin(m1,8);
%MBM substitution
for i=1:8
  m2(:,i)=m22(:,key1(i));
end
```

Phase 3: Message hiding

This phase hide the message in the selected block, the process of hiding will be implemented by inserting the message in the block in a burst way (one operation), this will increase the efficiency of data hiding, and the message bits will be inserted in the block by inserting the first bits of all characters, then the second bits of the second characters and so on (see Figure-11).

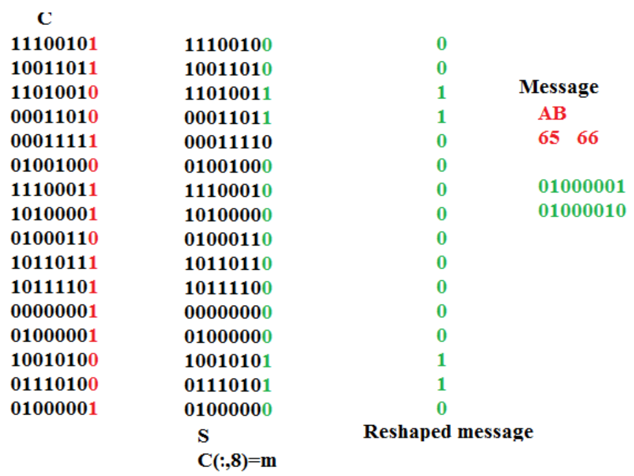

Figure-11. Character bits hiding.

The message-hiding phase will be implemented by applying the following steps:

Step 1: Get the block
Step 2: Reshape the block to a one-row matrix
Step 3: From the one-row matrix get a part equal to L*8
Step 4: Convert the part to binary
Step 5: Reshape the substituted MBM to one column matrix
Step 6: Let all the LSBs in the binary part equal the one-column matrix
Step 7: Convert the results in Step 6 to decimals
Step 8: Return the results to block part
Step 9: Reshape back the block to the 3D matrix
Step 10: Return the block to the covering image to get a stego image

This phase can be implemented by applying the following sequence of operations:

```
[nn1 nn2 nn3]=size(b);
b1=reshape(b,[1,nn1*nn2*nn3]);
a1=b1(1,1:L*8);
a2=dec2bin(a1,8);
m3=reshape(m2,[L*8,1]);
a2(:,8)=m3;
a3=bin2dec(a2)';
b1(1,1:L*8)=a3;
b2=reshape(b1,[nn1 nn2 nn3]);
a(r1:r1+r2,c1:c1+c2,:)=b2;
```

Figure-12. Shows an example of the hiding process.

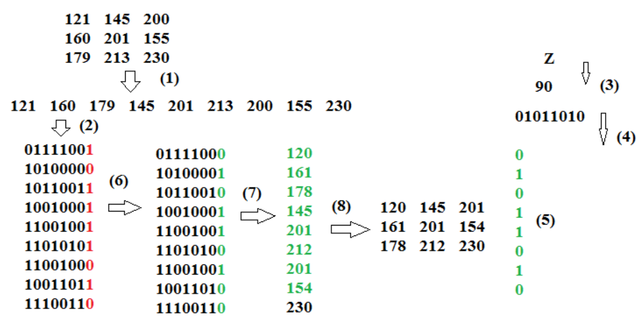

Figure-13. Hiding process example.

The message-extracting process can be implemented by applying the following phases

Phase 1: Image blocking

The same as in the hiding process, but using a stego image instead of a covering image, the following sequence of operations can be used to apply this phase (the same PK must be used):

VOL. 18, NO. 7, APRIL 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

```
rp1=0.17;rp2=0.35;
cp1=0.2;cp2=0.45;
R1=3.77;X1=0.125;
bb=a(r1:r1+r2,c1:c1+c2,:);
[nn1 nn2 nn3]=size(bb);
```

Phase 2: Message extracting

This phase can be implemented by applying the following steps:

Step1: Reshape the selected block into the one-row matrix
Step 2: Get a part equal to L*8
Step 3: Convert a part to binary
Step 4: From the binary results get the least significant column
Step 5: reshape the column to 8 column matrix to get MBM

The following sequence of operation can be used to apply this phase:

```
a5=reshape(bb,[1,nn1*nn2*nn3]);
a6=a5(1,1:L*8);
a7=dec2bin(a6,8);
m45=a7(:,8);
m5=reshape(m45,[L,8]);
```

Phase 3: MBM substitution

This phase requires an IK to apply MBM substitution, and it can be implemented by applying the following steps:

Step 1: Run CLMM to generate CLK
Step 2: Convert CLK to IK using the sort function
Step 3: Use IK to apply MBM substitution
Step 4: Convert MBM to decimal
Step 5: Convert decimal values to characters to get the secret message

The following sequence of operations can be used to implement this phase:

```
for i=1:8

    X1=R1*X1*(1-X1);
    CLK2(i)=X1;
end
[d key2]=sort(CLK2);

bb=a(r1:r1+r2,c1:c1+c2,:);[nn1 nn2 nn3]=size(bb);
a5=reshape(bb,[1,nn1*nn2*nn3]);
a6=a5(1,1:L*8);
a7=dec2bin(a6,8);
m45=a7(:,8);
m5=reshape(m45,[L,8]);
for i=1:8
  ss=find(key2==i);
  m6(:,i)=m5(:,ss);
end
m7=bin2dec(m6)';
```

Figure-14. Shows an example of extracting phase implementation:

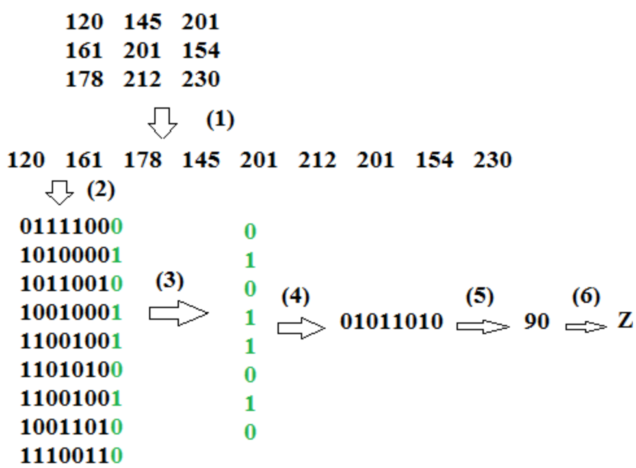

Figure-15. Extracting phase example.

IMPLEMENTATION AND RESULTS ANALYSIS

The proposed method was implemented using various messages and various covering images, the obtained results were analyzed using various methods of data analysis, and the analysis of the results will be described.

a. Visual analysis

Inserting the secret message in the covering image must not affect the image, the stego image must be close to the covering image, changes in the stego image must not be noticed by human eyes, and this will eliminate the suspicion that a color digital image may contain a secret message. Here we can visually prove this by locking to the images and their histogram, the stego image must be closed to the covering image, also the stego image histograms must be closed to the covering image histograms, this is shown in the method produced outputs shown in Figures 16 and 17.

VOL. 18, NO. 7, APRIL 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

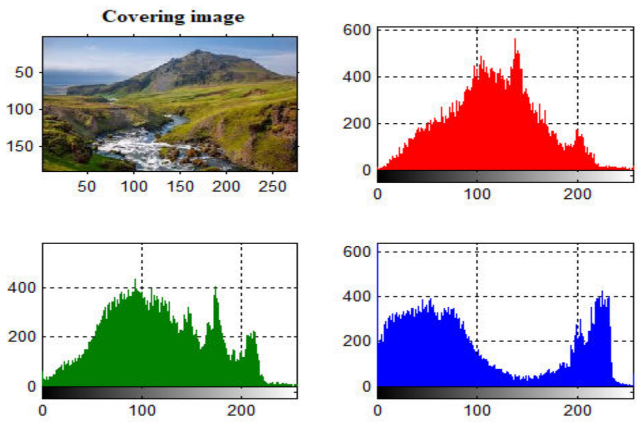

Figure-16. Sample of covering image and its histograms.

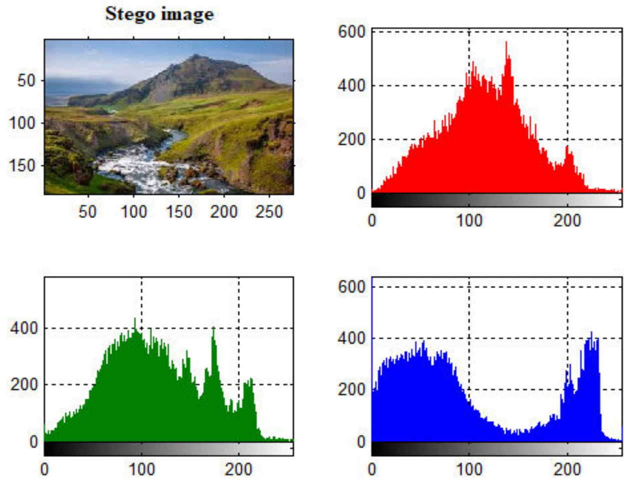

Figure-17. Sample of stego (holding the message: 'Data steganography using indices key') image and its histograms.

b. Sensitivity analysis

The extracted secret message is very sensitive to the selected values in the PK, any changes in the PK during the extraction phase will produce and extract a damaged secret message, doing these changes will be considered a hacking attempt. To show this the message 'Message steganography' was hidden in a covering image using PK1, Table-4 shows the results of message extraction using other PKs in the extraction phase

PK1:
rp1=0.17; rp2=0.35;
cp1=0.2; cp2=0.45;
R1=3.95; X1=0.25;

PK2:
rp1=0.17; rp2=0.35;
cp1=0.2; cp2=0.45;
R1=3.71; X1=0.25;

PK3:
rp1=0.17; rp2=0.35;
cp1=0.2; cp2=0.45;
R1=3.95; **X1=0.15;**

PK4:
rp1=0.17; rp2=0.35;
cp1=0.2; cp2=0.45;
R1=3.71; X1=0.15;

PK5:
rp1=0.27; rp2=0.44;
cp1=0.2; cp2=0.45;
R1=3.95; X1=0.25;

Table-4. Key sensitivity.

Used key in the extraction phase	Extracted message	Remarks
PK1	Message steganography	Ok
PK2	\tggdvt gqtvdz~vcdahm	Damaged message
PK3	GUyyQuU□y□UuQ7wu9Q□□[	Damaged message
PK4	□SyyQsS□y□SsQ³□s9Q□□□	Damaged message
PK5	Ké=□□<ù□¥□□6□□)-□*z□ù	Damaged message

c. Security analysis

The hacker must know the following in order

- The data hiding process was performed using the LSB method; here if the extraction phase was implemented using only the LSB extraction phase the extracted message will be damaged. Table-5 shows the results of extracted messages using the LSB method, the message embedding was performed using the proposed phase of data hiding:

Table-5. Extraction using the LSB method.

Embedded message	Extracted message using the LSB method
Data steganography	*r*>rjn*gon6*2#;
Securing LSB method	<j.z6+gna<$kjr#ob
Hacking process	!*./+gn26o.j>>
Message substitution	ij>>*nj>z&>r+rzr+og
Security analysis	<j.z6+r;*g*c;>+>

- The key was generated using CLMM

- Chaotic logistic parameters values, the PK contains 6 components, and thus, the PK provides a huge keyspace capable to resist hacking attacks (see equation 2).

$$\text{Key space} = 2^{64x6} = 2^{384} \quad (2)$$

- The IK was used for MBM substitution.

d. MSE and PSNR analysis

The quality between two images can be measured by Mean square error (MSE) and peak signal-to-noise ratio (PSNR), high value of MSE and low value of PSNR points to low quality, while low MSE and high PSNR points to high quality. A good method of data steganography must provide a high quality (low MSE and high PSNR) of the stego image, MSE and PSNR can be calculated using equations 2 and 3:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \text{dB}, \quad (3)$$

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2, \quad (4)$$

Where: MAX is the maximum possible value of sample values, N is the total number of samples, and xi and yi are the corresponding sample values of the source and encrypted/decrypted images.

A secret message of length 100 characters was treated using various covering images, MSE and PSNR was calculated between the covering and the stego images, and Table-6 shows the obtained results. The following PK was used:

PK:
rp1=0.17; rp2=0.35;
cp1=0.2; cp2=0.45;
R1=3.95; X1=0.25;

Table-6. Obtained MSEs and PSNRs results.

Image number	Size(byte)	MSE	PSNR	NSCR (%)
1	150849	0.0026	170.2263	0.2632
2	518400	0.00072917	183.0614	0.0729
3	5140800	0.000074697	205.8460	0.0075
4	4326210	0.000089455	204.0430	0.0089
5	122265	0.0030	168.7758	0.3043
6	518400	0.00075039	182.7745	0.0750
7	150975	0.0027	170.1344	0.2656
8	150975	0.0025	170.6198	0.2530
9	1890000	0.00022063	195.0153	0.0221
10	6119256	0.000062916	207.5623	0.0063

From Table-6 we can see the following:

- The obtained values of MSE and PSNR are acceptable and the obtained stego images have good quality.
- Increasing the covering image size will increase the hiding capacity and will improve the quality of the stego image by decreasing the value of MSEs and increasing the values of PSNRs.
- It is recommended to use a covering image with a big size, this will increase the hiding capacity and will decrease MSE, and will increase PSNR between the covering and stego images.

Table-7 shows the quality parameter values of hiding various messages in a covering image with a size equal to 6119256 bytes.

Table-7. MSE, PSNR, and NSCR using big images.

Message size (K bytes)	MSE	PSNR	NSCR
0.25	0.00016456	197.9475	0.0165
0.50	0.00032847	191.0359	0.0328
1	0.00067214	183.8757	0.0672
2	0.0013	177.0542	0.1330
3	0.0020	172.9066	0.2013
5	0.0033	167.8218	0.3347
10	0.0067	160.8589	0.6715
20	0.0134	153.9861	1.3352
25	0.0167	151.7289	1.6733
50	0.0335	144.7845	3.3509

VOL. 18, NO. 7, APRIL 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

Increasing the message size will increase MSE and decrease PSNR (see Figure-18), but the values of MSE and PSNR for hiding long messages will remain acceptable and the stego image quality will be high, Figures 19 and 20 show the covering image and a stego image holding 50 K bytes message.

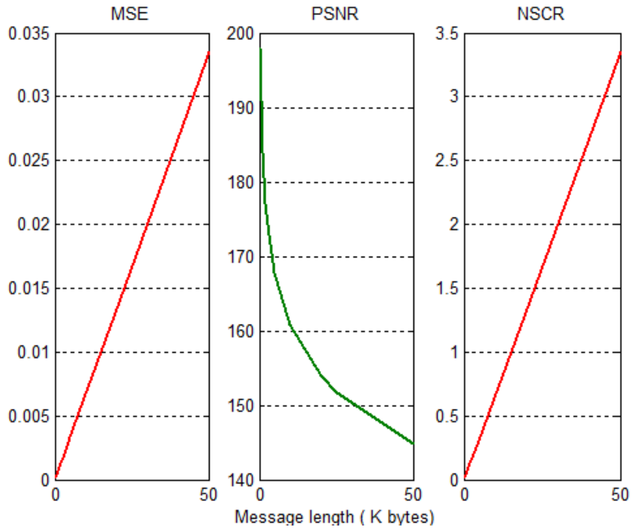

Figure-18. MSE, PSNR and NSCR using various lengths of messages.

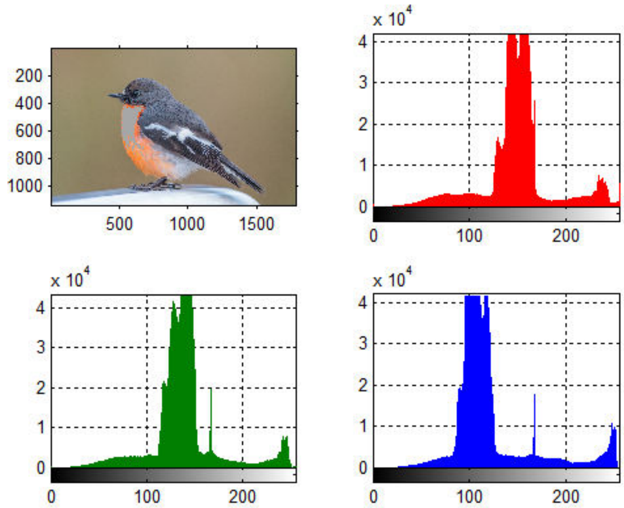

Figure-19. Covering images and histograms.

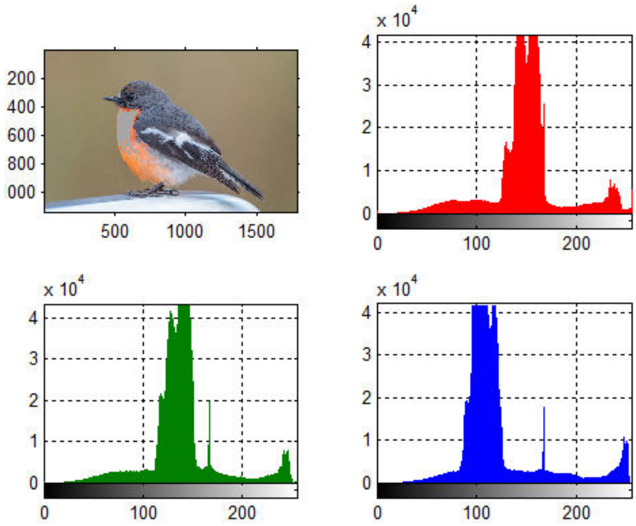

Figure-20. Stego image holding 50 K bytes' message.

e. Correlation analysis

The value of CC between two images expresses the dependency between their corresponding gray values. This is another statistical evaluation for testing the quality of the algorithm of data steganography. Calculating the correlation coefficient determines the level of correlation between two images and the correlation coefficient is always in the range [−1, 1]. Values between |1–0.7| are considered a strong correlation (samples from the source files are similar to samples from the encrypted file), a correlation between |0.7–0.3| is considered a medium correlation and values between |0.3–0| is considered as weak correlation. The correlation coefficient can be calculated using Equation 4:

$$\mathbf{CC}_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad \mathbf{(5)}$$

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 the covering and stego files, x⁻ and y⁻ are the mean values of samples, and finally cov (x, y) is the covariance between both files.

The selected message was treated using the proposed method, CCs (Between the red channels, the green, and the blue), were calculated between the covering and the stego images and Table-8 shows the obtained results.

VOL. 18, NO. 7, APRIL 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

Table-8. Correlation coefficients results.

Image number	CCr	CCg	CCb
1	1	1	1
2	1	1	1
3	1	1	1
4	1	1	1
5	1	1	1
6	1	1	1
7	1	1	1
8	1	1	1
9	1	1	1
10	1	1	1
Remarks	Always 1	Always 1	Always 1

From Table-8 we can see that the obtained values of CCs are excellent and this proves the good quality provided by the proposed method.

f. NSCR analysis

The number of sample change rates (NSCR) is a robustness test for establishing the quality of data steganography algorithms. The purpose of the test is to compare the corresponding sample values of the covering and stego images and to show the difference in percent. NSCR can be calculated using equation 5.

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \qquad \textbf{(6)}$$

where

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

The selected message was treated using the proposed method, and NSCRs were calculated between the covering images and the stego ones, the results of NSCRs are shown in Table-7, and they show that the proposed method satisfies the quality requirements.

g. Efficiency analysis

The message with 100 characters' length was treated using various covering images; Table-9 shows the obtained calculated efficiency parameter values.

Table-9. Efficiency parameters results.

Image number	HT(second)	ET(second)	HTP (K bytes per second)	ETP (K bytes per second)
1	0.0210	0.0040	4.6503	24.4141
2	0.0230	0.0040	4.2459	24.4141
3	0.0250	0.0050	3.9062	19.5313
4	0.0250	0.0050	3.9063	19.5312
5	0.0220	0.0040	4.4389	24.4141
6	0.0220	0.0040	4.4389	24.4141
7	0.0250	0.0050	3.9063	19.5312
8	0.0300	0.0050	3.2552	19.5312
9	0.0230	0.0050	4.2459	19.5313
10	0.0240	0.0060	4.0690	16.2760
	0.0240	0.0047	4.1063	21.1589

From Table-9 we can see that changing the covering image will keep the efficiency parameters without changes, thus it is better to use a covering image with a big size, this will increase the hiding capacity, and PSNR also will increase, while MSE will decrease.

Table-10 shows the efficiency parameters values when changing the message length and fixing the covering image (image 10: with big size):

Table-10. Efficiency parameters results in various messages.

Message length (K byte)	HT(second)	ET(second)	HTP (K bytes per second)	ETP (K bytes per second)
0.25	0.0310	0.0070	8.0645	35.7143
0.50	0.0410	0.0080	12.1951	62.5000
1	**0.0610**	**0.0140**	**16.3934**	**71.4286**
2	0.0990	0.0230	20.2020	86.9565
3	0.1380	0.0310	21.7391	96.7742
5	0.2900	0.0510	17.2414	98.0392
10	0.4120	0.0950	24.2718	105.2632
20	0.8150	0.1880	24.5399	106.3830
25	1.0220	0.2440	24.4618	102.4590
50	1.9910	0.4700	25.1130	106.3830
Average	0.4900	0.1131	19.4222	87.1901

From Table-10 we can see that the proposed method is very efficient by providing a hiding throughput of around 19.4222K bytes per second and extracting throughput of around 87.1901K bytes per second, these parameters are better than the results obtained in [22], the proposed method has a speedup comparing with classical LSB method and the method proposed in [22], see Table-11.

Table-11. Efficiency parameters of hiding a message of I K bytes.

Method	ET	Speedup of the proposed method	DT	Speedup of the proposed method
Classical LSB	0.14	2.2951	0.125	8.9286
Ref. [22]	7.005	114.8361	0.124	8.8571
Proposed	0.0610	1	0.0140	1

CONCLUSIONS

A simple efficient and highly secure and quality method of message steganography was proposed. The proposed method simplified the procedures used in the classical LSB method of message hiding and extracting, thus the HT and ET were minimized. The proposed method used a complicated PK, which provided a huge keyspace capable to resist any hacking attack, the method was very sensitive to any changes in the PK, and any changes in the PK used in the extracting phase were considered as a hacking attempt by producing a damaged decrypted message. The PK contained information to select a secret block from the image to be used as a covering block and information to run CLMM to generate the IK used to substitute the message binary matrix.

The proposed method provided an excellent quality of the stego image; this was proved by the obtained Low MSE, High PSNR, low NSCR, and CC equal 1. The proposed method decreased both the ET and DT and increased the throughput of message steganography; the proposed method provided a significant speedup compared with other existing methods.

The proposed method was implemented using various messages and various covering images, the obtained results were analyzed using various methods of data analysis, the results of the analysis proved the enhancements provided by the proposed method in the security, quality, and efficiency issues.

ACKNOWLEDGMENT

The researchers are grateful to the Applied Science Private University, Amman, Jordan, for the full financial support grated to this research project.

REFERENCES

[1] Mekha Jose. Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[2] Reena M. Patel, D. J. Shah. 2013. Conceal gram: Digital image in image using LSB insertion method. International Journal of electronics and communication engineering & technology (IJECET).

[3] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan. 2013. Enhancing the security and quality of LSB based image steganography. 2013 5th International Conference on Computational Intelligence and Communication Networks.

[4] Mamta. Juneja, Parvinder S. Sandhu. 2013. Animproved LSB based Steganography with enhanced Security and Embedding/Extraction. 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, Hong Kong (China) J.

[5] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain. 2001. A New Approach for LSB Based Image Steganography using Secret Key. Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, I, Dhaka, Bangladesh.

[6] Morkel T., Eloff J. H. P., and Olivier M. S., 2005. An Overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, South Africa, 2005.

[7] Ms. Nidhi Bux, Prof. K. J. Satao. 2015. Implementation of Watermarking Technique for Secured Transmission, International Journal of Advanced Research in Computer and Communication Engineering. 4(8).

[8] Jihad Nadir, Ziad Alqadi and Ashraf Abu Ein. 2016. Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image, International Journal of Computerand Information Technology (ISSN: 2279 -0764). 05(05).

[9] Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A. Abu Jazar and Rushdi Abu Zneit. Optimized True-Color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, 2010 ISSN 1818-4952.

[10] Gaurav Bhatnagar, Balasubramanian Raman. A new robust reference watermarking scheme based on DWT -SVD. 0920-5489/$–see front matter © 2008 Elsevier B.V.. doi:10.1016/j.csi.2008.09.031.

[11] C. De Vleeschouwer, J. F. Delaigle, a nd B.Macq. 2002. Invisibility and application functionalities in perceptual watermarking anoverview. Proceedings of the IEEE. 90: 64-77.

[12] Prof. Ziad A. A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti. 2016. Comparative Analysis of Color Image Steganography, IJCSMC. 5(11): 37-43.

[13] Dr. Ashraf Abu-Ein, Prof. Ziad A.A Alqadi, Dr. Jihad Nader. 2016. A Technique of hiding Secrete Text in Wave File. International Journal of Computer Applications ·. DOI: 10.5120/ijca2016911732.

[14] K. Matrouk, A. A. Hasanat and H.Alashalary, Prof. Ziad Al-Qadi and Prof. Hasan Al-Shalabi. 2014. Speech fingerprint toidentify isolated word person. World Appl. Sci. J. 31(10): 1767-1771.

[15] Rafael C. Gonzalez and Richard E. 2002. Woods, Digital Image Processing, Prentice Hall, second edition.

[16] Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. 2008. Digital watermarking and steganography (2nd. ed.). New York: Morgan Kaufmann.

[17] Cheddad A., Condell J., Curran K. & Kevitt P. Mc. 2010. Digital image steganography: survey and analyses of current methods signal processing. 90(3): 727-752).

[18] Katzenbeisser S. & Petitcolas F. A. 2000. Information hiding techniques forsteganography and digital watermarking. (pp. 43-78). London: Artech House.

[19] Roque J. J. & Minguet J. M. 2009. SLSB: Improving the steganographic algorithm LSB. Proceedings the Ibero-American Congress on Information Security (CIBSI). pp. 398-408.

[20] Cvejic N., Seppanen T. 2004. Increasing robustness of LSB audio steganography by reduced distortion LSB coding. Proceedings ITCC 2004 International Conference on Information Technology: Coding and Computing.

[21] Mazen Abu Zaher. 2011. Modified Least Significant Bit (MLSB), Computer and Information Science. 4(1).

[22] Swati Balbhadra, Jageshwar Shrivas, Rohit Miri. 2015. A Novel Technique for Secure, Lossless Steganography with Unlimited Payload, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, 02(03).

[23] Rashad J. Rasras1, Mutaz Rasmi Abu Sara, Ziad A. 2019. Al Qadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data

Steganography. International Journal of Advanced Trends in Computer Science and Engineering, 8(3), https://doi.org/10.30534/ijatcse/2019/64832019

[24] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazarand Rushdi Abu Zneit. 2010. Optimized True-RGBcolor Image Processing, World Applied Sciences Journal8 (10): 1175-1182, ISSN 1818-4952.

[25] Waheeb A. and Ziad Al Qadi. 2009. Gray image reconstruction, Eur. J. Sci. Res. 27: 167-173.

[26] Akram A. Moustafa and Ziad A. Alqadi. 2009. Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254

[27] Musbah J. Aqel, Ziad Al Qadi, Ammar Ahmed Abdullah. 2018. RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication. International Journal of Engineering & Technology, 7(3.13): 104-107. https://doi.org/10.14419/ijet.v7i3.13.16334

[28] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein. 2016. A Comparison between Parallel and segmentation Methods Used for Image Encryption-Decryption International Journal of Computer Science & Information Technology (IJCSIT). 8(5).

[29] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi. 2014. Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X 121(3): 258-266.

[30] Ziad A. A. Alqadi, Musbah Aqel, and Ibrahiem M. M. El Emary, Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.

[31] Z. Alqadi, A. Abu-Jazzar. 2005. Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering.

[32] Musbah J. Aqel, Ziad A. Alqadi, Ibraheim M. El Emary. 2007. Analysis of Stream Cipher Security Algorithm. Journal of Information and Computing Science. 2(4): 288-298.

[33] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher. 2018. A Novel zero-error method to create a secret tag for an image. Journal of Theoretical and Applied Information Technology. 96(13): 4081-4091.

[34] Prof. Ziad A. A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti. 2016. Comparative Analysis of Color Image Steganography, JCSMC. 5(11): 37-43.

[35] M. Jose. 2014. Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality. International Journal of Science and Research. 3(9): 2281-2284.

[36] Emam M. M., Aly A. A. & Omara F. A. 2016. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications, 1(7): 361-366. https://doi.org/10.14569/IJACSA.2016.070350

[37] Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber. 2019. Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC. 8(2): 93-103.

[38] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi. 2019. Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research. 9(1): 3681-3684.

[39] Zhou X., Gong W., Fu W., Jin L. 2016. An 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

[40] 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

[41] Das R., Das I. 2016. 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, https://doi.org/10.1109/ICRCICN.2016.7813674

[42] M. Abu-Faraj and Z. Alqadi. 2022. Image Encryption using Variable Length Blocks and Variable Length Private Key. International Journal of Computer

ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

Science and Mobile Computing (IJCSMC). 11(3): 138-151.

[43] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi. 2022. A Dual Approach for Audio Cryptography. Journal of Southwest Jiaotong University. 57(1): 24-33.

[44] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi. 2022. Complex Matrix Private Key to Enhance the Security Level of Image Cryptography. Symmetry. 14(4): 664-678.

[45] M. Abu-Faraj, K. Aldebei and Z. Alqadi. 2022. Simple, Efficient, Highly Secure, and Multiple Pur-posed Method on Data Cryptography. Traitement du Signal. 39(1): 173-178.

[46] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi. 2021. Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study. Journal of Southwest Jiaotong University. 56(6): 685-694.

[47] M. Abu-Faraj, Z. Alqadi and K. Aldebei. 2021. Comparative Analysis of Fingerprint Features Ex-Traction Methods. Journal of Hunan University Natural Sciences. 48(12): 177-182.

[48] M. Abu-Faraj and Z. Alqadi. 2021. Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography. International Journal of Computer Science and Network Security (IJCSNS). 21(12): 451-458.

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