International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2020.3642

E-ISSN : 2454-6135

Volume.6, Issue 8
August -2020

Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique

Zahraa Salah Dhaief[1], Raniah Ali Mustafa[2] and Amal Abdulbaqi Maryoosh[3]

[1-3]Mustansiriyah University

College of Education, Department of Computer Science

Iraq

ABSTRACT

Today, in this new era of the internet, Information Security is becoming the biggest challenge for the world due to the rapid growth of internet users day by day. Unauthorized access to secret data can have serious repercussions like a financial loss. One of the best techniques for secure communication is Steganography-or covert writing. It is an art of hiding the very existence of communicating the message itself. This research presents a state of dual stenographic technique. Dual Steganography combines two security mechanisms, steganography and cryptography both together. This mechanism has the advantage of providing high security and low time complexity. This research proposes a dual steganography technique with an additional level of security. The proposed algorithm embeds secret text messages in cover image in two phases. The two phases include a chaotic map cipher technique for encrypting text and LSB (Least Significant Bit) image steganography technique for hiding encrypted text in an image. The text containing encrypted data is hidden in an RGB image.

Key Words: *Cryptography, Steganography, Chaotic map, Least Significant Bit, Digital image..*

1. INTRODUCTION

Since the beginnings of human information transfer, the wish to communicate in secrecy has existed. Whether planning a surprise birthday party or overthrowing a government, exchanging information in secret is essential. There has been multi solutions to this problem, the most usually used and investigated being cryptography [1].

Historically, sensitive data has been protected using encryption. Encryption uses powerful mathematics to convert plaintext into an unreadable cipher text that is transmitting over a channel to the recipient. When a message is encrypted it is done so using a secret key. To decrypt a message, the secret key is used to reverse the operation. For an ease dropper to defeat the system he or she must get the secret key. Typically it is supposed that this must be done by searching through the entire key space; a so called “brute-force” attack. As this is a very time consuming endeavor, the “encrypted message” is considered safe [1].

Second method of information transfer, called steganography offers information protection in a somewhat multiple manner. Steganography offers security like to cryptography in that, if an adversary does not know information is being transferred; he cannot intercept and read it. Though protection the inner part of the message secret is required in many cases, steganography have a much more powerful use steganography hides the very fact that a communication is taking place. The difference between cryptography and steganography is an important issue, and is summarized via the following: Encryption prevents an unauthorized party from find out the insides of a communication. Steganography stops finding of the very existence of a communication [2].

2. Cryptography

Cryptography is the science of secret writing with the target of transforming readable information into unreadable form by designing cryptographic systems. Cryptanalysis is the science and sometimes art of breaking ccryptographic systems. Cryptology is a term used to embody the study of both cryptography and cryptanalysis.

A plaintext is an intelligible message, whereas a ciphertext is the unintelligible form of the message. The process of converting plaintext into ciphertext is known as encryption or enciphering, retrieving back the plaintext from ciphertext is called decryption or deciphering. The Cryptography system ingredients are plaintext, cipher key, encryption algorithm that takes a plaintext and

cipher key to be the input and produces ciphertext to be the output and decryption algorithm which is the inverse of the encryption algorithm [3].
Cryptographic systems are classified through the following types:

2.1 Substitution Cipher and Transposition Cipher

All encryption algorithms are based on common principles according to the operation types used to convert plaintext into ciphertext as follows:

a. **Substitution**: A substitution technique changes the characters of a plaintext to produce a ciphertext. A simple example about these ciphers is Caesar cipher. The goal of substitution is the confusion which prevents the cryptanalyst from discovering any relationship between the key and the ciphertext. [4]

b. **Transposition**: A transposition technique rearranges the places where the plaintext letters sit, where the letters do not change, but rather move them around without introducing any new letters. Using transposition, the cryptography targets to achieve diffusion, widely spread the information of the message or the key across the ciphertext. Since a transposition rearranges the symbols of a message, it is also called a permutation. An example about these ciphers is columnar transposition [4].

2.2 Symmetric Cryptography

In symmetric cryptography, only a single key is employed for encryption and decryption operation. As displayed in Figure (1.1), the sender uses an algorithm and a key for encrypting the plaintext and sends the ciphertext to the recipient. The recipient employs the same algorithm and key for decrypting the message and recovers the plaintext. By this kind of cryptography, it is observable that the key should be known to the sender and receiver. An example about this cryptography is DES [5].

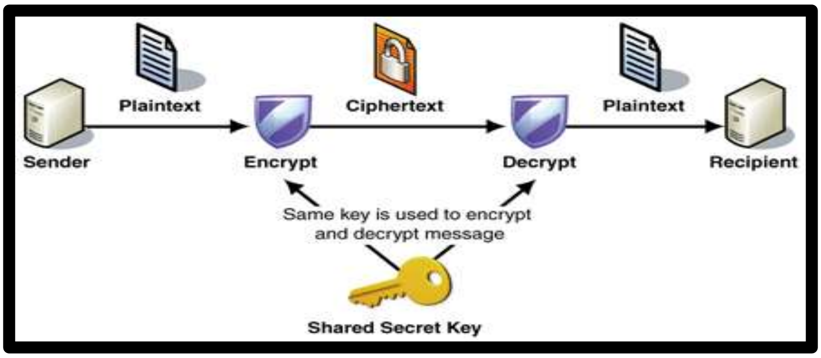


Figure 1.1: single key is employed for encryption and decryption operation.

Symmetric Cryptography can be classified according to the treating way of encrypting a plaintext into the following two types:

a. Stream cipher: A stream cipher shown in Figure (1.2) encrypts bits independently. This is done by encrypting a bit of a key stream with a bit of a plaintext. RC4 is a popular stream cipher [6].

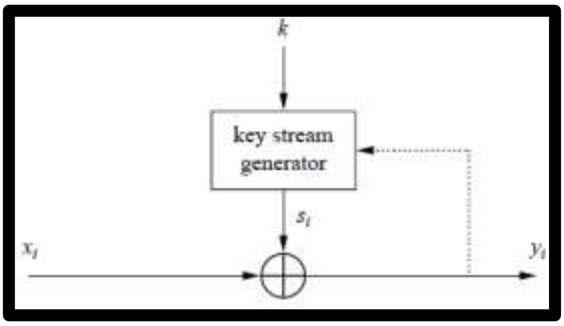


Figure 1.2: Synchronous and Asynchronous Stream Cipher

b. Block cipher: In a block cipher shown in Figure (1.3), a message is split into a number of blocks, for example a block length of 128-bits in AES algorithm or a block length of 64-bits in DES algorithm and after that each block of plaintext bits is transformed into an encrypted block of cipher bits by an algorithm and a key [7].

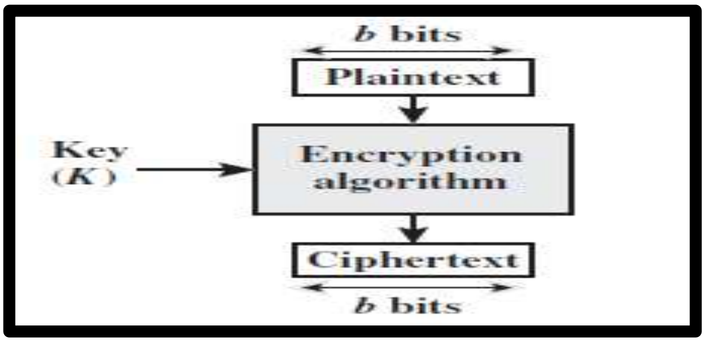


Figure 1.3: Block Cipher

2.3 Asymmetric Cryptography

In 1976, a totally different type of encryption was produced by Whitfield Diffiee, Ralph Merkle and Martin Hellman. Asymmetric cipher is also called a public key cryptography. In asymmetric cryptography shown in Figure (2.4), the encryption and decryption will be done by two different keys, where just the data that is encrypted by a public key could be decrypted by the identical algorithm and the data that is encrypted by a private key could be decrypted by only the same public key. The most known public key encryption algorithm is RSA algorithm [8].

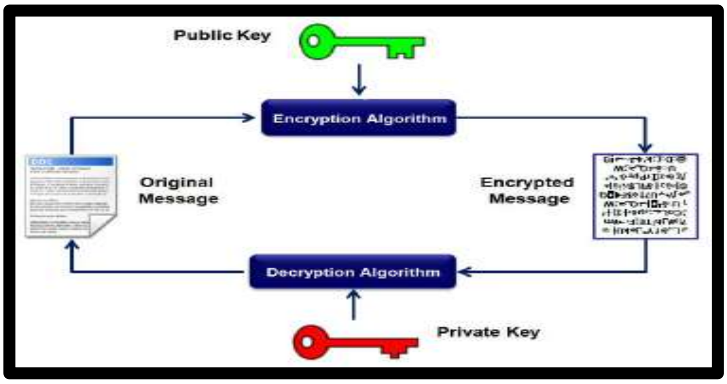


Figure 1.4: Asymmetric Cryptography

3. STEGANOGRAPHY

Steganography (literally, covered writing) is the art of data concealment in ways that prevent the detection of hidden messages. It includes a vast array of secret communication methods that conceal the very existence message.

Steganography has its position in security. It is not intentional to exchange cryptography, but accomplish it. Concealments a message with steganography ways decrease the chance of a message being discovered. If the message is also encrypted then it supply other layer of protection.

Consequently, various stenographic approaches combine traditional cryptography with steganography; the sender encrypts the secret message prior to the overall communication procedure, as it is extra hard for an attacker to notice embedded cipher text in a cover [9].

3.1 Steganography in Various Media

Old steganography includes a vast array of techniqucs for hiding message in a variety of media, for example: the methods are invisible inks and microdots digital signature. Today, thanks to modern technology, steganography is used on text, images, sound and more, and it is expected that a great expansion of stenographical techniques will occur in the coming years [10].

a. Steganography in Texts

Steganography can be used in text documents by adding white spaces in the end of lines of a document. This type of Steganography is effective because the white space occurs naturally and it's not visible to the human eye at all in most of text document editors. When using this Steganography technique there is no way to suspected if there is any hidden data [10].

b. Image Steganography

Usually the Least Significant Byte (LSB) is used when hiding information inside images. Image file simply is a file that shows different colours and intensities of light on different areas of an image. The best type of image file to hide information

DOI : 10.31695/IJERAT.2020.3642

inside of is images have a high quality, resolution and their size such as 24 Bit BMP (Bitmap) image which is the largest type of file. So, this type is easier to hide and mask information inside it. It is important to remember that the hidden information will be lost if the stego-file then converted to another image format [10].

c. Audio Steganography

There are many techniques used in audio steganography when we need to hide information inside audio file; the technique usually used in hiding information inside Audio files is low bit encoding which is similar to LSB in image files. Using the low bit encoding is a risky method because it is usually noticeable to the human ear. Another method used to hide information inside of an audio file is Spread Spectrum, this method works by adding random noises to the signal, the information spread across the frequency spectrum of the audio file. Another method of hiding information inside an audio file is Echo data hiding. This method hides information by simply adding extra sound to an echo inside an audio file, this method better than other methods of hiding information audio files because it can actually improve the sound of the audio inside an audio file[10].

d. Video Steganography

Usually when hide information inside the video the DCT (Discrete Cosine Transform) method used. DCT works by make inconsiderable changing on each of the images in the video, so it’s not noticeable by the human eye. The DTC change the values in certain parts in the picture, where the number of rounds the greatest integer, for example, if the value is 4.578 become 5. Steganography in Videos is similar to that of Steganography in Images, a part of information is hidden in each frame of video, while a small amount of information is hidden inside of video, the hidden information not noticeable, as known whenever the information that is hidden increased, the change will be become more noticeable [10].

3.2 Steganography Process

Steganography process as shown in figure (1.5) has the following components [11]:

1. Secret message: The data to be hidden which can be in the format of text, audio, video, or image.
2. Cover –Media: It refers to the object used as the carrier to embed the secret message inside it.
3. Embedding Algorithm: Known as hiding message procedure.
4. Extracting Algorithm: Known as unhide/uncover the message procedure.
5. Stego-media (image): Refers to the generated object, which is carrying a hidden message.

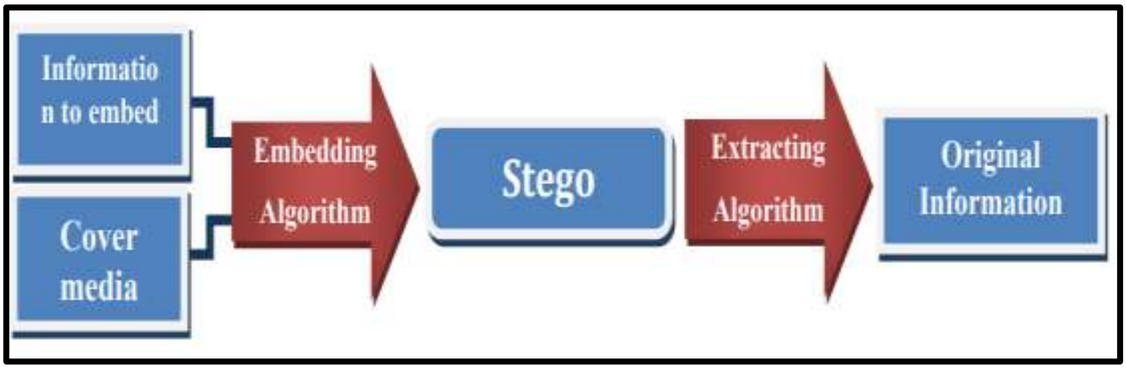


Figure 1.5: The Steganography Process.

3.3 Methods of Concealing Data in Digital Image

Information can be hidden in different ways in images. The most common approaches of information hiding in images are [12]:

- Least Significant Bit (LSB) insertion.
- Masking and Filtering Techniques.
- Algorithms and transformations.

3.3.1 Least Significant Bit (LSB)

The idea behind the LSB algorithm is to insert the bits of' the hidden message into the **least significant bits** of the pixels. As a simple example of bits insertion in a 24 bit pixel [12]:

DOI : 10.31695/IJERAT.2020.3642

If the pixel bits: (l l00l0l0 00111010 l0l l00l l)

Red Green Blue

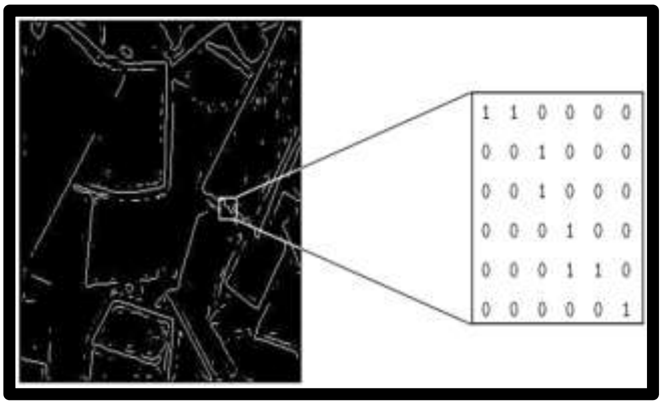
If we insert 110 : (l l00l0l1   00111011   l0l l00l 0)

Red Green Blue

4. DIGITAL IMAGES

A digital image is composed of a finite number of elements, each of which has a specific position and value. Each one of these elements is known as picture element, or simply a pixel [12]. Below, the basic types of digital images:

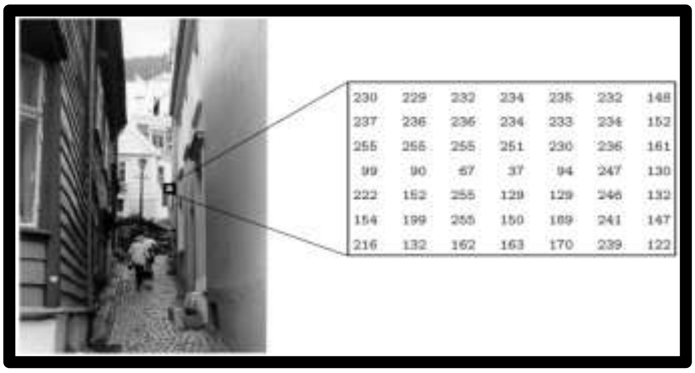
a. Binary Image: A binary image is the simplest type of images. A Binary image is a two dimensional array that assigns one numeric value (0 or 1) to every pixel in an image, black color corresponds to 0 and white color corresponds to 1. Figure (1.6) shows a binary image [12].



1	1	0	0	0	0
0	0	1	0	0	0
0	0	1	0	0	0
0	0	0	1	0	0
0	0	0	1	1	0
0	0	0	0	0	1

Figure 1.6: Binary Image

c. **Gray scale Image**: Gray scale image has 256 different gray levels from 0 which represents black color to 255 which represents white color. Such range denotes that every pixel is represented by eight bits, or precisely one byte [14]. Figure (1.7) shows a gray scale image.



230	229	232	234	235	232	148
237	236	236	234	233	234	152
255	255	255	251	230	236	161
99	90	67	37	94	247	130
222	152	255	129	129	246	132
154	199	255	150	169	241	147
216	132	162	163	170	239	122

Figure 1.7: Gray scale Image

d. **Color Image**: Color image is also known as RGB image, since such an image contains three matrices represent red (R), green (G) and blue (B) values for every pixel. Hence, for every pixel there are three corresponding values. Each of R, G and B components has a range of values from (0-255), the whole number of bits needed for every pixel is 24 (bits/pixel), 8-bits to each of R, G and B color components [15]. Figure (1.8) shows a color image.

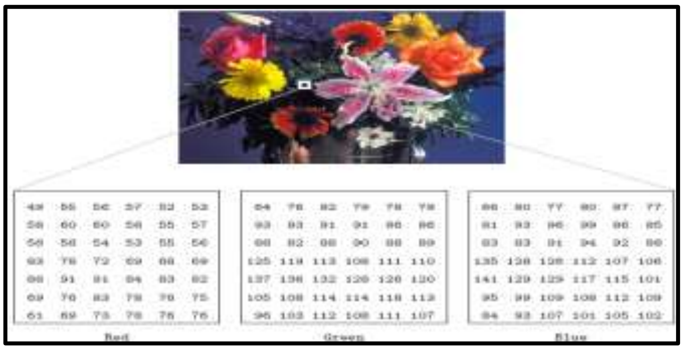


Figure 1.8: Color Image

5. CHAOS THEORY

The Chaos theory defines the behavior of specific nonlinear dynamic systems, which exhibit dynamics under particular conditions and effectively cannot be predicted or controlled and very sensitive to initial conditions, where the initial conditions are a point where the chaotic system begins

Since the last years, numerous researchers have studied chaos theory in many fields, such as electronic systems, fluid dynamic, laser and climate. Due to Chaos properties, it is implemented nowadays in many various areas like engineering, computer science, mathematics, physics, geology, biology and robotics [16].

Chaotic systems have the following essential properties:

1. A Chaotic system is bounded, its movement is all the time restricted by a certain region and is called a chaotic domain.
2. A Chaotic system is deterministic, which means that the chaotic system behavior is well-defined by mathematical equations and their future is predetermined by the initial conditions.
3. It is very sensitive to initial conditions and parameters, a small change in the initial conditions and parameters set for the chaotic system could lead to huge difference outcome of the chaotic system after a few iterations.
4. Randomness, the situation may be changed in a qualitative way or make the system chaotic under specific condition. However, a status may be arised or maybe not.
5. A Chaotic system appears to be disordered, but indeed, it is not; beneath the disorder is an order and creative chaos.
6. Unpredictable, even when the current state of a chaos system is well-known, it is useless attempting to predict the next state of the chaotic system, in other words, it is hard or impossible to predict the behavior in the long term.
7. Aperiodic, the chaotic system proceeds in an orbit where there is no occasion replicates itself, that is, this orbit is never periodic.

5.1 Chaotic Maps

A chaotic map is a non-linear dynamic system which reveals pseudo randomness behavior. The Chaotic sequence is created in a simple way through the using of different equations [17].

In the subsections below, a concise description of some chaotic maps is given:

a. Logistic Map

In 1845, Pierre Verhulst proposed the Logistic map, which is a popular and simple chaotic map. Logistic map became very popular when it was used in 1979 by the biologist Robert M. May, where the equation of one dimensional Logistic map is shown in Equation (1):

$x_{n+1} = a \times x_n \times (1 - x_n) \ldots (1)$

In which $x_n \in [0,1]$, x_0 denotes the initial condition and a is a constant parameter between 0 and 4. For ($3.5699 < a \leq 4$), Equation (1) shows a chaotic behavior [17]. Figure (1.9) depicts Logistic map.

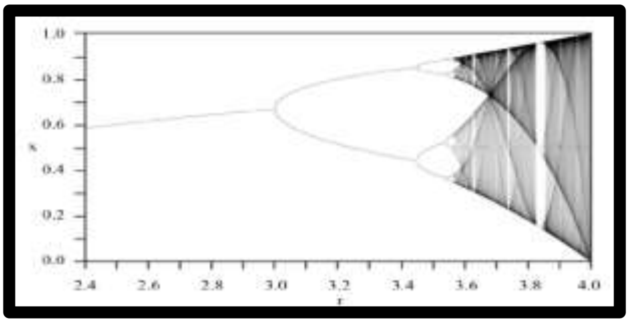


Figure 1.9: Bifurcation Diagram of Logistic Map

DOI : 10.31695/IJERAT.2020.3642

b. Hénon Map

Hénon map was introduced by Michel Hénon, it is a two dimensional discrete time dynamical chaotic map defined by Equations (2) as follows:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \qquad (2)$$

In which (x_n, y_n) and (x_{n+1}, y_{n+1}) are the current and next chaotic states respectively, where a and b are positive parameters. For the classical Hénon map, the value of a=1.4 and b = 0.3 and thus the map exhibits chaotic behavior [17]. Hénon map is shown in Figure (1.10).

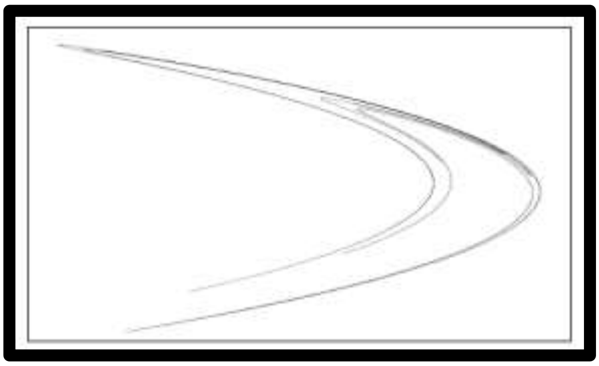


Figure 1.10: Henon Map Attractor.

5.2 Chaos and Cryptography

The close association between chaotic systems and cryptography leads to make chaos-based algorithms the best choice for encrypting data. For real time applications, encryption scheme which takes lesser execution time, but without compromise with the preferable security is desirable. Chaos-based encryption technique is a good mixture of security, high speed and less power consuming.

The properties of chaotic systems like sensitive to initial conditions and parameters, randomness, have attracted the interest of researchers, since such properties indeed fulfill the vital principles of cryptographic algorithms design. Exploiting these favorable features, chaos-based algorithms have revealed superior characteristics in complexity and security.

In 1989, Matthews, a British mathematician, firstly employed chaos for encryption, who suggested a new encryption algorithm generating key stream based on Logistic map and encrypting the information by stream cipher method. In 1998, Fridrich Scharinger suggested the first chaos-based image encryption algorithm with confusion and diffusion design, which are two important properties of a secure cipher as identified by Claude Shannon in his masterwork "*Communication Hypothesis of Secrecy Systems*" [18].

6. PROPOSED ALGORITHM IMPLEMENTATION

To illustrate how the proposed algorithm will operate, the process is divided into three processes (Encryption, Steganography and Desteganography):

6.1 Encryption Process

The encryption process takes the following steps:

1. Load the text file and read the text.
2. Convert the text into binary matrix. *to be encrypted using XOR.
3. Take the size of the binary matrix length and width. *to be used to convert the binary matrix to binary value with one dimension.
4. Generate the Henon Map chaotic sequences and convert it to binary.
5. Encrypt the original binary values of text with Henon binary values using XOR.

The encryption code in MATLAB:

```
clear all
close all
```

DOI : 10.31695/IJERAT.2020.3642

```
clc
text='originaltext'
 ascm=double(text);
binasc=dec2bin(ascm);
[rt ct]=size(binasc);
t=rt*ct;
nn=1;
for it=1:rt
    for jt=1:ct
        sd(nn)=binasc(it,jt);
        nn=nn+1;
    end
end
sd=double(sd);
for i=1:length(sd)
if sd(i) >=49
    sd(i)=1;
else sd(i)=0;
end
end
%% The Henon Map % where a and b are the proposed algorithm parameters
%% The code% We start by defining the initial values
x(1)=0.8888;
y(1)=0.9999;
a=1.4;
b=0.3;
% and now we begin the iteration (10000 iterations):for i=2:10000
for i=2:(rt*ct)+200
    x(i)=1-1.4*(x(i-1)^2)+y(i-1);
    y(i)=b*x(i-1);
end

for ii=1:length(y)
if x(ii) >= 0.5
    x(ii)=1;
else
    x(ii)=0;
end
    if y(ii) >= 0.5
    y(ii)=1;
else
    y(ii)=0;
end
end
x=x(51:t+50);
y=y(51:t+50);
x=xor(sd,x);
y1=xor(x,y);
y1=dec2bin(y1);
rn=y1';
```

6.2 Steganography Process

The Steganography process takes the following steps:

1. Load the image that will be used for hiding text.

2. Extract each color level RGB of the image.
3. Convert each color level to binary.
4. Load the text that to be hidden in the image.
5. Encrypt the text with encryption process
6. Hide each bit of the encrypted text in the least significant bit in each image level Red, Green then Blue.
7. Save the image that contains the hidden text.

The Steganography code in MATLAB:

```
x=imread('3.bmp');
 [r2 c2 f2]=size(x);
x1=x(:,:,1);
x2=x(:,:,2);
x3=x(:,:,3);
 x1=dec2bin(x1);
x2=dec2bin(x2);
x3=dec2bin(x3);
 filename = 'dd.txt';
 A = importdata(filename);
text=char(A);
[p q]=size(text);
[rn rt ct]=HM(text);
n=1;
sd=int32(length(rn)/3);
sd=length(rn)-sd;
for i=1:length(rn)-sd
 x1(i,8) =rn(n);
 x2(i,8) =rn(n+1);
 x3(i,8) =rn(n+2);
 n=n+3;
end
x(:,:,1)=uint8(reshape(bin2dec(x1),r2,c2 ));
x(:,:,2)=uint8(reshape(bin2dec(x2),r2,c2 ));
x(:,:,3)=uint8(reshape(bin2dec(x3),r2,c2 ));
subplot(1,2,1); imshow(x);title('Input Image');
subplot(1,2,2);  imshow(x); title('Image after stego);
imwrite(x,'newimage.bmp')
```

6.3 Desteganography

1. Load the image that contains the encrypted text (Stego Image).
2. Extract the text from the stego image.
3. Decrypt the text by repeat the encryption process with XOR.

The dencryption code in MATLAB:

```
%De Stego
x1=x(:,:,1);
x2=x(:,:,2);
x3=x(:,:,3);
[r c]=size(x1);
x1=dec2bin(x1);
x2=dec2bin(x2);
x3=dec2bin(x3);
%  decriptext=dec2bin(ENCimageDCE);
n=1;
```

DOI : 10.31695/IJERAT.2020.3642

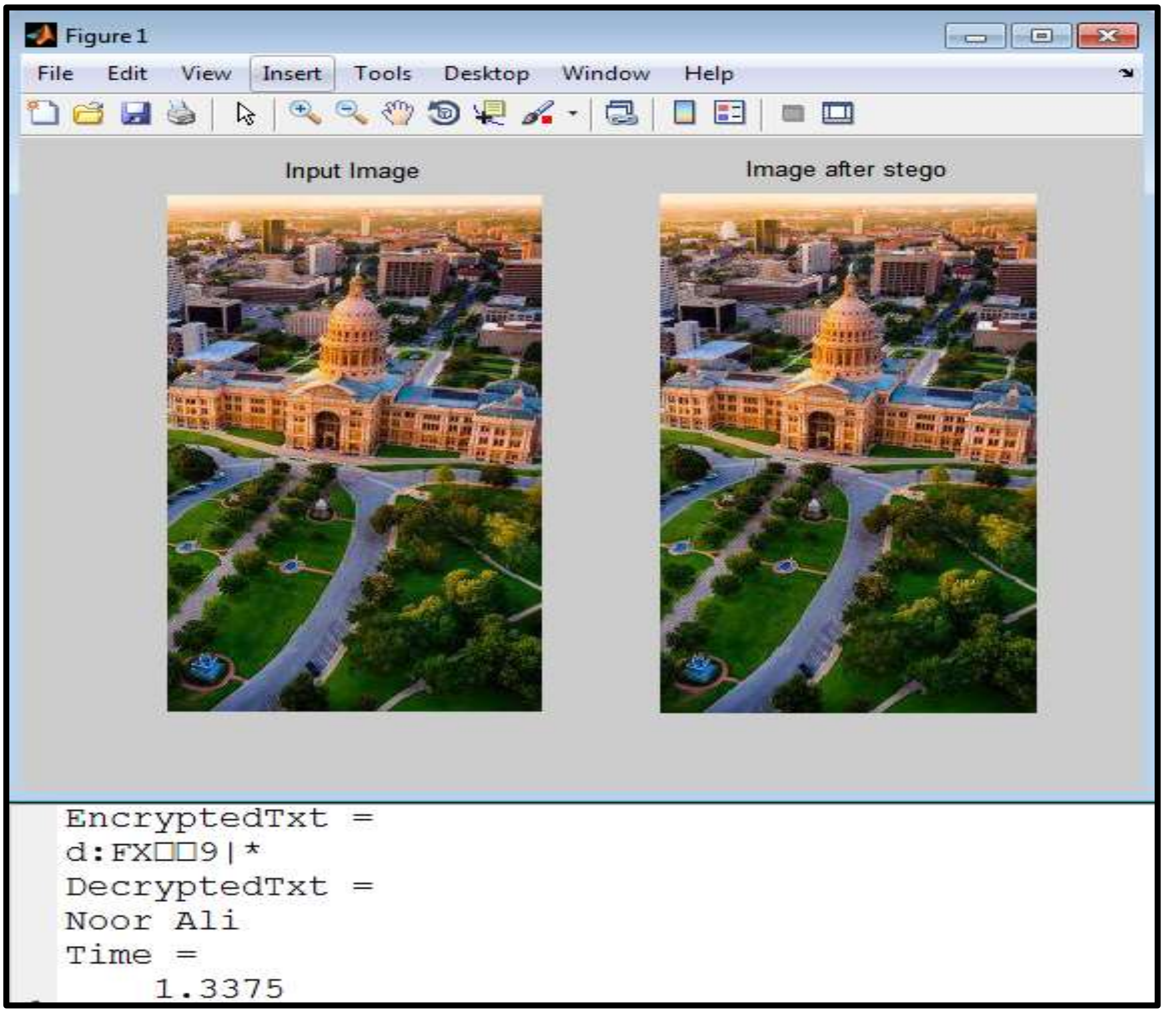
```
for i=1:length(rn)-sd
 textbin(n)   =x1(i,8);
 textbin(n+1) =x2(i,8);
 textbin(n+2) =x3(i,8);
 n=n+3;
end
if length(textbin) ~= length(rn)
z=length(rn)- length(textbin);
z1=zeros(1,z);
z1=num2str (z1);
textbin=[textbin  z1]';
else textbin;
end
%
ng=1;
for io=1:rt
    for jo=1:ct
   textbin1(io,jo)=textbin(ng);
   ng=ng+1;
    end
end
% decriptext=dec2bin(x);
%  textbin=decriptext(1:rt*ct,8)
 ascimessage=bin2dec(textbin1);
 messageDEc = char(ascimessage);
 EncreptedTxt(p,:) = messageDEc;
 [rnn rt1 ct1]=HM(messageDEc);
 nn1=1;
for it=1:rt1
    for jt=1:ct1
        rnn1(it,jt)=rnn(nn1);
           nn1=nn1+1;
    end
end
 rnnn=bin2dec(rnn1);
 DecreptedTxt(p,:) = char(rnnn);
 time=toc;
 save('ee.txt','DecreptedTxt');
disp('EncryptedTxt = ');
disp(EncreptedTxt);
disp('DecryptedTxt = ');
disp(DecreptedTxt);
```

The images used in experiments are presented in Table (1.1).

Table 1.1. Test Images.

Images			
Name	**#1**	**#2**	**#3**
Format	**JPG**	**JPG**	**BMP**
Size	**(320*180) Bytes**	**(256*256) Bytes**	**(250*250) Bytes**

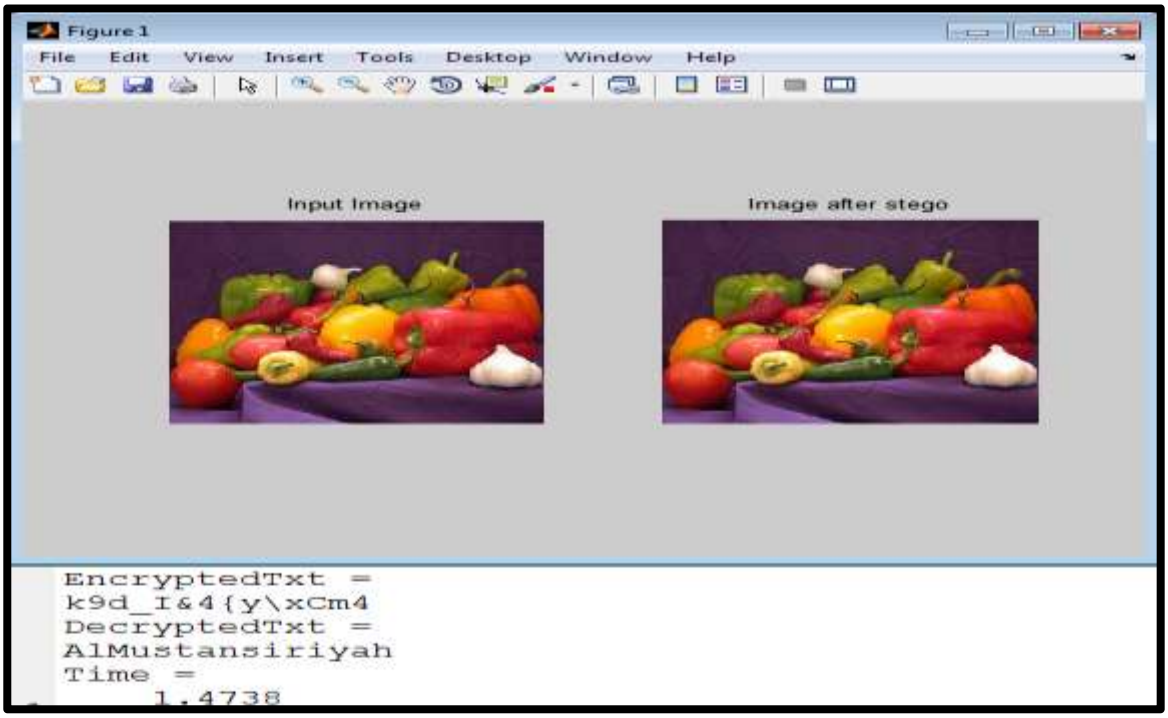
The following figures show original image, image after steganography, encrypted text hidden inside the image, decrypted text and execution time for test images using proposed algorithm in Matlab.



```
EncryptedTxt =
d:FX□□9|*
DecryptedTxt =
Noor Ali
Time =
     1.3375
```

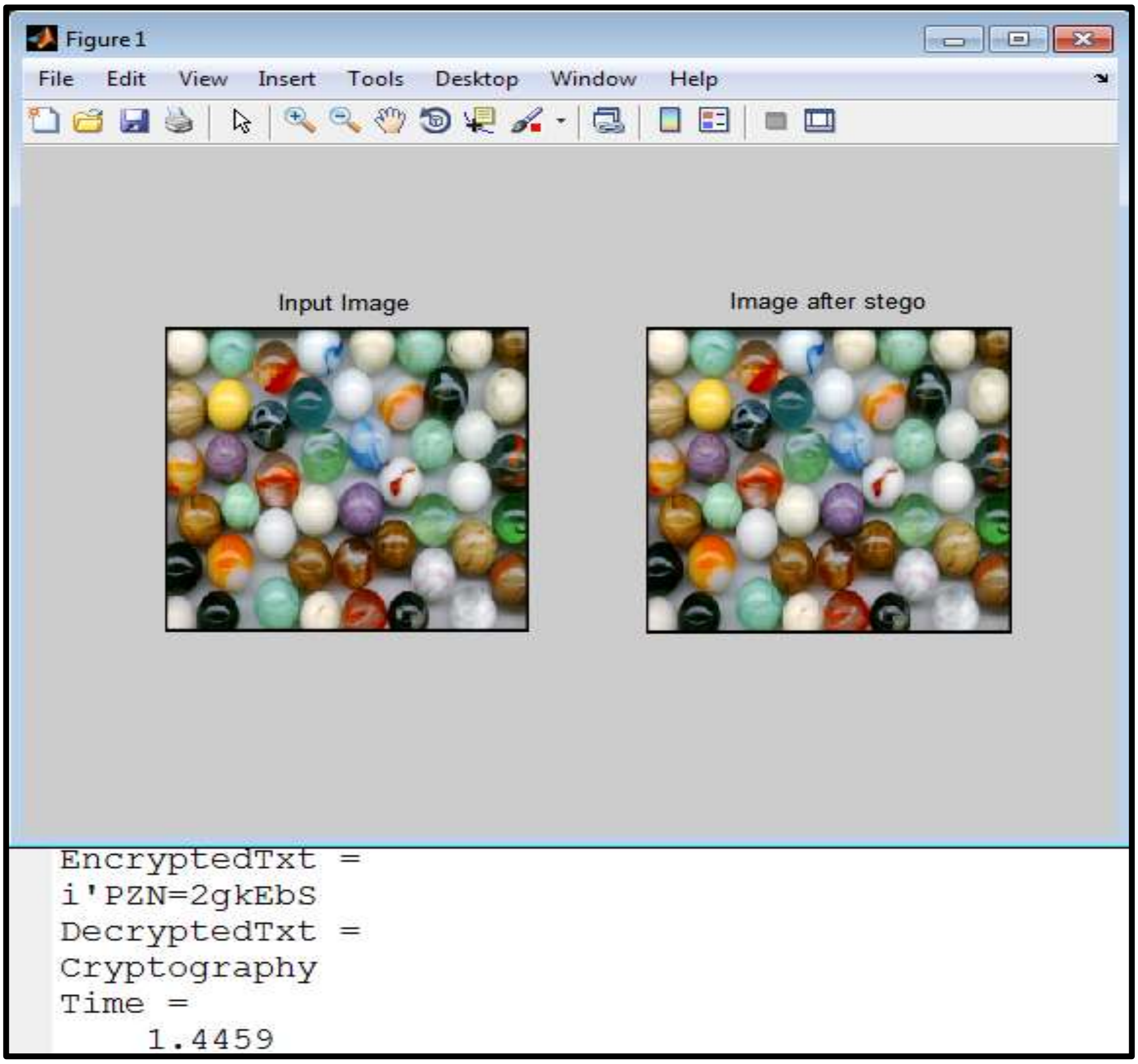
Figure 1.11: Image #1 (Original, Stego Image)

DOI : 10.31695/IJERAT.2020.3642



```
EncryptedTxt =
k9d_I&4{y\xCm4
DecryptedTxt =
AlMustansiriyah
Time =
       1.4738
```

Figure 1.12: Image #2 (Original, Stego)



```
EncryptedTxt =
i'PZN=2gkEbS
DecryptedTxt =
Cryptography
Time =
       1.4459
```

Figure 1.13: Image #3 (Original, Stego)

DOI : 10.31695/IJERAT.2020.3642

From figures above, one can see that the stego images which contain the hidden text using proposed algorithm have nothing refer to the hidden text.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad – Iraq for its support in the present work.

CONCLUSIONS

The main conclusions from designing and implementation of the proposed algorithm are:

- The proposed hiding algorithm can hide any kind of message in general; the sender does not deal with any fixed models.
- Hiding the text into the image using LSB technique with the help of XOR operation based on chaotic map gives more security and complexity.
- Hidden text can be recovered after extraction text by LSB technique
- Use of steganography provides strong security and invisible communication.

REFERENCES

1. Ikhlas Falih Alsudany**. (** 2006).**Analysis and Detection of Information Hiding in Digital Images**, M.Sc, University of *Technology*, Department of Computer Science.
2. Anupam Mondal and Shiladitya Pujari.(2015).**A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients,** Computer Network and Information Security, MECS, 3, pp.42-49.
3. Christof Paar and Jan Pelzl.(2010).**Understanding Cryptography, A Textbook for Students and Practitioners**, Foreword by Bart Preneel, Springer-Verlag Berlin Heidelberg.
4. Charles P. Pfleeger.(October 13, 2006). **Security in Computing**, 4th Edition, Prentice Hall.
5. Gary C. Kessler. (17 November 2006).**An Overview of Cryptography**, Available at: http://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf.
6. Richard A. Mollin.(2007). **An Introduction to Cryptography**, 2nd Edition, Chapman & Hall/CRC.
7. Michael E. Whitman and Herbert J. Mattord,(2011). **Principles of Information Security**, 4th Edition, Course Technology.
8. B. Rajan.(2011). **Independent Domain of Symmetric Encryption using Least Significant Bit** , M.Sc. Thesis, University of Dalarna, Computer Engineering.
9. Najla'a Abd Hamza Muhsassan.(2005). **New Robust Information HidingTechnique,** Msc. University of Technology, Informatics Institute for Postgraduate Studies,.
10. Morkel, T., Eloff, J. H., & Olivier. M. S. (2014, June). **An overview of image Steganography**. In Information Systems Security Association(ISSA), pp. 1-11.
11. Sura Fahmy Yousif.(2014). **Wavelet Based Image Stenographic System using Chaotic Signals,** Msc. AL-Mustansiriya University, College of Engineering.
12. TU Tran.(2002). **steganography the art of hiding data.** Mills College.
13. Rafael C. Gonzalez and Richard E. Woods.(2007). **Digital Image Processing**, 3rd Edition, Prentice Hall.
14. Ze-Nian Li, Mark S. Drew and Jiangchuan Liu.(2014).**Fundamentals of Multimedia**, Springer International Publishing Switzerland, 2nd Edition.
15. Alasdair McAndrew.(2004). **An Introduction to Digital Image Processing with Matlab**, Course Technology.
16. Pianhui Wu.(May 2013). **Research on Digital Image Watermark Encryption Based on Hyper Chaos**, Faculty of Business, Computing and Law, University of Derby.
17. Mahmoud Maqableh.(8, December 2015) **A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map**, Journal of Software Engineering and Applications.
18. Chong Fu et al., (, 2014).**A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy**, Entropy, 16.

DOI : 10.31695/IJERAT.2020.3642