International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 30, Issue 01) and (Publishing Month: May 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN: 2319-6564
www.ijesonline.com

Encryption Message Hide within the Image

Sahera Sead

Computer Department, Basra University, Science College, Basra, Iraq
sahera26_12@yahoo.co.uk

Abstract

The research presents a proposed algorithm to encrypt message and hide them inside the image file (cover) of the type JPG and send more subtle, and so by the message encrypted using several ways to encrypt and then hide the message in a manner to make the distance between the elements used in the hiding process is fixed, making it difficult predictability hide websites those letters within the image elements of the image analysis methods or by statistical analyzes. This method worked to encrypt and hide text messages without the case deformation to the original image or the possibility of note for changes which result hiding process, was retrieving those files easily without losing any of its components, as well as the retrieval process this place without the help of the original image or the need to create a table showing concealment sites.

Keywords: *Steganography, Cover Image, LSBs, PSNR.*

1. Introduction

That information security is a very important issue in many aspects of human life. Every person has a private information does not want to be seen by one other, or wants to send a message to another person without knowing the content of such a message, from here came the idea of encryption[1].

encryption is the art or science of hidden meaning and concept of the message and not hides its existence, any transfer of information to codes incomprehensible, so if it signed the message sent in the hands of anyone other than the intended recipient will be unable to understand the contents because he was not authorized to read it. If reached the encrypted message to the receiver on it is counterproductive to the process of encryption and decryption called for the original text and read it[2]. The receiver can decode encryption using "secret key" to be agreed in advance between the sender and the receiver, and this key is used in the processes of encryption and decryption. Without this key, we cannot do coding or decoding [3].

Information security has become aware of the focus of attention of many by researchers and interested parties who are trying to get solutions and new technologies and updated to ensure the protection of the information you send and receive via the World Wide Web for information(the Internet) without any break or disclosure by the intervener[1]. Therefore it was necessary to keep pace with the development of information security and the establishment of techniques and sophisticated means and from here emerged steganography (Information Hiding) and the evolution of the adoption of steganography technique [4].

The technique of hiding methods of protection that make sending and receiving data is not visible, so hide certain messages within a certain cap. The goal earned the process of hiding is not to raise any point to doubt the existence of hidden data, while the objective analyst of hiding is in doubt all messages sent, and checked for the presence of hidden data in them[5]. Called the process by which an attempt by the discovery and the presence of hidden information or read, change or delete the process of decoding hiding is carried out. why there was a need to find a variety of means, for the purpose of communicating information and data properly and protected from informed parties unauthorized access to this information, so it was added a new expression to the security information is listed, a security networks, which is defined as the right of protection for each linked computer network components, guaranteed data and communication tools. Where it was during the hiding of the data put into the media files so that they cannot be observed or detected or recognize the existence of movable information through those files, but

seemingly ordinary files where they are in maintaining the overall shape of the file the carrier, and hiding on two categories:
First watermarks and in which is hidden a few information such as signature, a sign the company or institution seal to authenticate the documents sent, difficult way manipulated or erased through image processing operations such as filtration, engineering transfers or add noise[6]. The second class is where the picture hiding to hide includes the largest possible important information (document, message, diagrams or images) within the text or image files that way that does not provoke curiosity, but looks as images declaration or plain text.

In this paper is organized as follows. Section 2 describes the details of the proposed algorithm. The experimental results of the proposed message hiding scheme are demonstrated in section3 .Finally, section 4 presents the conclusions for this work.

2. Algorithm Encryption and Hiding Proposed

Proposed algorithm combined scientific (encryption and hiding), is hidden confidential information (encrypted) and sent in a hidden, force produced by these two flags meeting (encryption and hiding) may be a force to be reckoned with since their meeting with each other leads to receiving the secret messages in a difficult decoding and difficult to recognize its existence. The algorithm includes two main steps:

1. Encryption and Hiding.
2. Retrieve the Message and Decryption.

2.1. Encryption and Hiding

Includes two stages:
A. The Message Encryption Stage.
B. Hide Encrypted Message Stage.

A. The Message Encryption Stage

At this stage, the message is encrypted and composed this stage of several processes which are as follows:

Input Message: are at this stage to enter the text message, for example:

"Keep this information in your private files"

Find Length of the Message: We are finding the message length any number of letters the message input.

Reverse the Direction of the Message: We rewrite the letter are inverted (i.e. reverse arranged from left to right or from right to left), for example, the letter used in the previous example:-
"selifetavirpruoyninoitamrofnisihtpeek "

Replace Letters Location : In this type of encryption takes all four consecutive letters are altered, so that the first item in the fourth location .The second element in the first location. The third elements in the second location and fourth element to the third element, and this applies to each of four consecutive letters and have previous example output as follows: **"iselafetpviryruooninmitanrofhisietpek"**

The Process of Converting Letters: In this process are chosen password, and ignores repeated the letters are letters floor distribution on the main diameter of the matrix (used secondary diameter in case you need to supplement password) characters, and then write the alphabet English (26) non-existent in the password symbols to complete the matrix line after line, for example when choosing a password STAR WAR as shown:

S B C D E
F T G H I
J K A L M
N O P R Q
U V X Y W
Z

Then read the matrix progressively from left to right, and write letters in a line under the english letters, which read letters in diagonal line from top to bottom (must be the matrix elements 26 characters), as follows**:**

ABCDEFGHIJKLMNOPQRSTUVWXYZ
EDICHMBGLQSTARWFKPYJOXNVUZ

To make encryption read letters from top to bottom (i.e. read the sequence of letters in the english alphabet) and parallels underneath is it required that we write the letter, for example, if the explicit text

I HAVE TWO BOOKS

Output will be encrypted:
LGEXH JNW DWWSY

When applying this process to the letter previously entered gets the following: **"mysrdoskgxmtvtqnnemeimkdetnohmymskgsf"**

Geometric Shapes: At this stage is a model or a certain geometric pattern when writing the message, where this form rectangular body. I.e., when the creation of any form leads to a change clear text (message) for the purposes of cryptographic, used at this stage to form a geometric composed of four columns either the number of rows depends on the size of the message that the approved encryption methods on geometric shapes security may give a limited degree but can be used as a stage intermediate , but the purpose of the security increase was dropping off letters message in a rectangular column-column and sequentially, the application of this process on the previous example we get the following**:**

m	m	i	y
y	t	m	m
s	v	k	s
r	t	d	k
d	q	e	g
o	n	t	s
s	n	n	f
k	e	o	
g	m	h	
x	e	m	

Character Conversion to Decimal value: at this stage, the text is converted to decimal values in order to be dealt with and perform calculations on them. As follows:
32 107 101 101 112 32 116 104 105 115 32 105 110 102 111 114 109 97 116 105 111 110 32 105 110 32 121 111 117 114 32 112 114 105 118 97 116 101 32 102 105 108 101 115

Convert Text values to Binaries: The processes of converting the resulting values of the previous stages to the binary values dismantle any decimal values, so the output is as follows:

0010000001101011011001010110010101111000
0001000000111010001101000011010010111100
1100100000011010010110111001100110011101
1110111001001101101011000010111010001100
1001011011110110111000100000011010010110
0111000100000011110010110111101110101011
1100100010000000111000000111001001101001
1110110011000010111010001100101001000001
0110011001101001011010001100101011100110

Binaries Reverse Process: At this stage, we are in the heart of the value of each bit of bits resulting from the previous stage that is all (0) keep suit (1) and vice versa , so the output is as follows:

1101111110010100100110101001101010001110
1110111111000101110011110010110100011000
1101111110010110100100011001100110010000
0100011011001001010011110100010111001010
1010010000100100011101111110010110100100
0011101111110000110100100001000101010000
1101110111111000111110001101100101101000
0100110011110100010111001101011011111100
011001100101101001011100110101000110

So we've got a coded message that will later have hidden inside the colored image**.**

B. Stage Hide the Encrypted Message

At this stage, the encrypted text message is included within the cover (image file). This stage consists of two parts embedding and retrieval is as follows**:**

1. Include Encrypted Text Message Image:

It includes the following operations:
a**.** Input Image.
b. Measure and one size 256x256 image
c. Find the Image Size.
d. Image segmentation into three levels:
I1 = X(:,:,1),I2 = X(:,:,2),I3 = X(:,:,3)

Set the image that will hide the first letter of the text, and (E) component of the location and on the assumption that the first location E (i, j) = (25,5) . Assuming that the tonal value in this site was the red color (R = 200), green (G=210),blue(B=186) . Converting the color value of the element to a binary

- $R=(200)_{10}=(1100\ 10\mathbf{00})_2$
- $G=(210)_{10}=(1101\ 0\mathbf{010})_2$

- $B=(186)_{10}=(1011\ 1\mathbf{010})_2$

e. Taking the character from any text began eight (bytes), then byte cut into three parts, such as contains part first (2)bits , the second and third magistrates each of them contains the (3) bits sequentially. for example, to hide the character (k) of the previous message turns the character into a binary value $K=(107)_{10}=(01101011)_2$
Then byte character segmentation into three parts: $P1=(11)_2$,$P2=(010)_2$, $P3=(011)_2$.

f. Replace the bits bytes each color of the three colors are one of the parts of the character in the least significant bits site to configure the value of bytes of three new colors for the item. This means that hide the first part of the character (P1) in LSBs of red byte. $Rnew=(110010\mathbf{11})_2=(203)_{10}$ and hide the second part of a character (P2) in LSBs of green byte.$Gnew=(11010\mathbf{010})_2=(210)_{10}$. Hide the third part of a character (P3) in LSBs of blue byte $Bnew=(1011\ 1\mathbf{011})_2=(187)_{10}$.

g. The hiding distance calculated by taking (4) bits of green or any other color (N) and added to the key value (key = 9). $S=(N)_2+(Key)_{10}$
$S=(0010)_2+(9)_{10}=11$.

h. locate the next element to hide in order to calculate the hash distance and add it to the current location of the item. Any site next item is as follows: Enew=(25 ,5+11)=(25 ,16)

i. repeating steps (f, g, h) until the end of text characters (encrypted message).

2.2. The message retrieval and decryption

It includes two major phases:
A. retrieves the encrypted message phase
B. phase decrypt the message.

A. Retrieving the Encrypted Message phase
Retrieving the encrypted message hidden inside the colorful stage image is as follows:
a. determine the location of the item image that holds the first letter of the letters hidden text.
b. read the color value of the image and extract the three bytes that represent the red, green and blue values. $Rnew=(1100\ 10\mathbf{11})_2$, $Gnew=(11010\mathbf{010})_2$, $Bnew=(1011\ 1\mathbf{011})_2$.

- Then take binaries substituent in the hiding of every color from the color process where we take the first two of the least important of a layer of red (11) and three bits of the least important of the green layer (010) and three bits of the least important of the blue layer (011).
- They are then assembled to be byte value characters (01101011).

c. Select the next item which will be retrieval site and then calculates the distance.
d. repeating steps (a, b and c) until the end of the message encoded.

B. Decrypt the Message Phase
The decryption process is the opposite of the encryption process take any steps encryption itself, but any versa begin the last step and we're done with the first step, and operations include the following:
a. process re-reverse binaries**:** In this process, unlike the value of every bit of bits retrieved the message means that every (0) to change it (1)
and vice versa, was the result of the previous example as follows**:**
0010000001101011011001010110010101111000
0001000000111010001101000011010010111100
1100100000011010010110111001100110011101
1110111001001101101011000010111010001100
1001011011110110111000100000011010010110
0111000100000011110010110111101110101010
1100100010000000111000000111001001101000
1110110011000010111010001100101001000000
0110011001101001011010001100101011100110

b. process re binaries to a decimal value: At this stage we refund of decimal values of binaries, as follows:
32 107 101 101 112 32 116 104 105 115
32 105 110 102 111 114 109 97 116 105
111 110 32 105 110 32 121 111 117 114
32 112 114 105 118 97 116 101 32 102
105 108 101 115
c. converting decimal values to letters convert decimal values to letters, as follows:

m m i y

y t m m

s v k s

r t d k

d q e g
o n t s
s n n f
k e o
g m h
x e m

d. decode geometric shapes: In this process we rearrange the letters to form a linear begin moving on the characters from the first column and then the second and so on, as follows**:"mysrdoskgxmtvtqnnemeimkdetnoh mymskgsf"**

e. retrieval process of converting letters : In this process we are trying to bring every letter of the encryption matrix including the corresponding matrix lettering original text, as follows**:"iselafetpviryruooninmitanrofhisietpe k"**

f.re characters location process: In this process we letters to their original positions, which we are in the encryption stage we took all four characters and switch positions so that the fourth letter in the first position and the first character a second location and the second character in the third site became the third in the fourth site, as follows**:**

"selifetavirpruoyninoitamrofnisihtpeek"

g. retrieval process of the direction of the message: Turn the direction of the message to get character original text as follows**:**

"keep this information in your private files"

3. Results

The proposed algorithm is applied to several images to see the resulting image quality after the process of hiding are used measure peak signal to noise ratio (PSNR), which measure the extent of hiding accuracy and lack of discrimination encrypted message hidden in the image the human eye. For hide images measure for accuracy includes square calculation error and defined the following two equations (1),(2):

MSE = $\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(fij - gij)^2$ **……(1)**

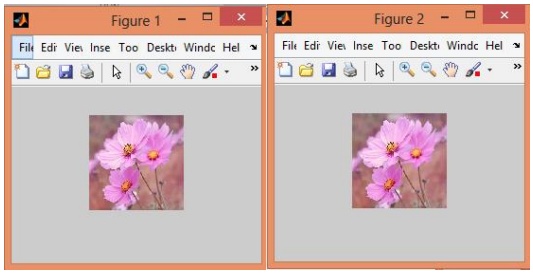
PSNR = 10 $\log_{10}\frac{L_2}{MSE}$**…….(2)**

Whereas**: M, N:** are the row and column for the cover of the image**.** fij**:** Unity is the image of the picture (cover) by hide**.** gij**:** Unity is the image of the images after the message disappears encoded within it**. L:** is the level of the signal (for a picture that you book eight binary digits per unit summit, It is a sham (L = 255). Table(1) shows the value of MSE, PSNR after the application process hiding on several images of different sizes and messages encrypted number of different characters**.**

Table 1: Measure MSE, PSNR pictures of different sizes and different length messages

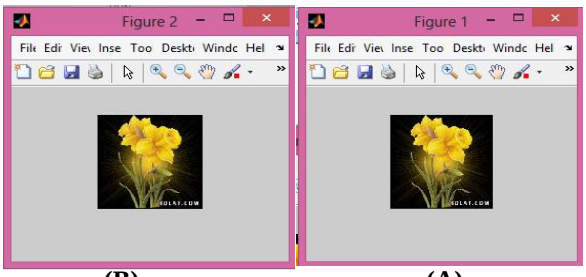
Image Name	*Image Size*	*Message Length*	*MSE*	*PSNR*
Image1	128 X 128	35 / 66	0.0326 / 0.2010	52.2136 / 48.0794
Image2	344 X 278	35 / 132	0.0600 / 0.0992	59.3844 / 57.1881
Image3	350 X 350	35 / 158	0.0564 / 0.3025	58.9441 / 56.1016
Image4	267 X 275	35 / 212	0.0566 / 0.3258	63.1248 / 52.8724

Figures (1), (2), (3), (4) describes the images before hide the cipher text and beyond**.**



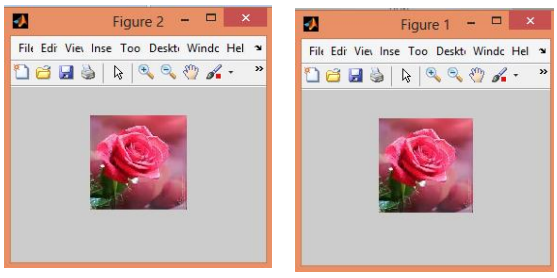
(A) (B)

Figure 1: (A) the original image before hide text (B) the image after encrypted text hiding



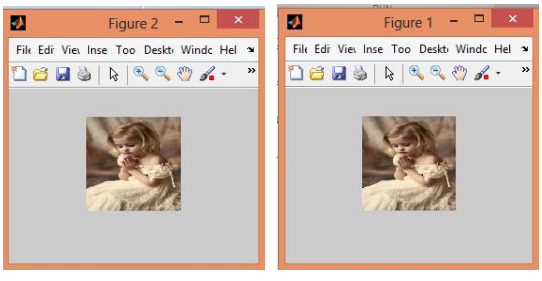
(B) (A)

Figure 2: (A) the original image before hide text (B) the image after encrypted text hiding



(B) (A)

Figure 3: (A) the original image before hide text (B) the image after encrypted text hiding



(B) (A)

Figure 4: (A) the original image before hide text (B) the image after encrypted text hiding

4. Conclusions

Through the application the encryption algorithm and hide the proposed to the hide information encrypted and through results obtained were reached the following conclusions **:**

a. Whenever encryption has been added steps have increased the strength of encryption, and thus increasing the security of data sent**.**

b. The distance between the hash picture elements claiming to reduce the possibility of hidden text revealed the fact that distribution depends on a secret key secret key to be agreed upon, as well as the displacement is a fixed distance, and the roads that are used to hide the sequential and steady pace, they are more likely to discover And provoke doubt among thieves or intruders**.**

c. After the implementation of the results proved the possibility to hide the text of any duration was in the form of any extension was for example, the type of JPG, BMP**.**

d. After removing the cover, the resulting text be exactly identical to the original text**.**

e. The use of key value with the value of the portion of the image element output after the hiding operation you can control distance of hash and thus the work of balancing the size of the text you want to hide the size of image of the cover**.**

F. proportion of hiding in this way be less compared to conventional methods for the existence of abandoned spaces without hiding because of the adoption of the displacement mechanism in the process.

References

[1] W.M. Farmer, Overview of Cryptography."07-cryptography erview.pdf", 2003.

[2] W. Stallings," Cryptography and Network Security", Prentice Hall, New Jersey, 1999.

[3] Seberry J. &Pieprzyk J.,"Cryptography An Introduction to computer Security", prentice-2002.

[4] Bender, W., et. al., "Applications for Data Hiding", IBM Systems Journal, Vol.39, No.5 3 & 4, 2000.

[5] Cvejic, N., "Algorithms for Audio Watermarking and Steganography", Department of Electrical and Information

Engineering, Information Processing Laboratory, University of Oulu, 2004.

[6] Cummins, J., et. al., "Steganography and Digital Watermarking", School of Computer Science, the University of Birmingham, 2004.

[7] Randy L. Haupt and Sue Ellen Haupt, "Practical Genetic Algorithms", Second Edition, A John Willey & Enetic Sons, Inc., New York,2004.

[8] D. Kohn, "The Code breakers: The Story of Secret Writing", Scribner, New York, 1996.