# Hide Encoded Text Within the Image by Using the Third Least Significant Bit

**Zainb Bakar Dahoos**
*Computer Dept/ Science College/ Basra University*

**Abstract**

This research includes building a system to hide the encoded text within the image file (cover) to produce material hidden file .The algorithm includes two major phases:

1 – The hide the text message encoded within the image. At this stage is hiding the text message after encrypted inside the cover (file image) ,this phase consists of two main stages, the encryption process and hiding process.

2 - Message retrieval, the include the sequence of steps involved in the process of hiding and encoded, but reversing these steps.

The hide algorithm proposed has been applied to more than image file and made a good recovery rate for data and text message without causing any noticeable distortion in the file cover and the size of the image increases the efficiency of hide and difficult , but cannot be anyone to distinguish the existence of any text within the image.

**Keywords**: Steganography, cover-image, LSBs, PSNR.

## 1.Introdution

The international network of information (internet ) is a new environment to deal with the information in the information revolution, and as a result of the increasing importance emerged serious thinking in the protection and the protection of the privacy of individuals working on them, so it is no longer the security theme relates to methods of encryption and the development of security policies and look for gaps in communication protocols , but also become also include an attempt to control the content of the information circulating online and around the world [1]. Pour all the modern technologies in the course of one , is the ease of access to information by users and which has undoubtedly resulted in the violation of her wish , that the new concept of the model circulation of information refers to the flow of information towards the user through the Internet and the means available to the other , and this calls for reconsideration of the models used in information systems. Appeared successful encryption as a way to protect the data stored and transmitted the idea was that the communication may be a security by encrypting traffic. But this is rarely true in practice arisen the need to find ways to hide messages instead of encrypted security to ensure that communication is not only encryption but also security passwords that have an existing substance to hide information[2][3].

Hide information technology represents the umbilical cord of the documents that digital steganography to hide information means information in other innocent appearance does not bring attention most importantly in this modern technology employed in it is not clear to consider in addition to the flexibility in the use of all media for the purpose of hiding where they can hide the secret message in all its forms (image , sound , text) inside the vessel information possess different properties (voice, image , text , and multimedia) and make it unconsciously by hackers and attackers , and so the information is unknown to the users of the network while keeping the content monopoly of the relevant authorities that know how to extract content . To hide information of great importance, because the information does not appear either encrypted or non-encrypted visible as a catalyst to bring protect and secure the information [4].

The hide is used in a number of areas but the area that has emerged in which is increasingly e-commerce applications, and interest in them day after day .Despite the great importance and benefits provided by this venerable science, but its spread until this moment to outweighing the deployment of cryptography[5].

The power produced by the Union of these flags may be a force to be underestimated by as their meeting with each other leads to the secret messages we get tough in the decryption and difficult to realize its existence. Then complete the research in the laboratory of many digital processing, including hide information in the digital fingerprint images and the possibility of use by men patrolling. Some may ask what the need to hide the existence of the data did not fear, the reason is due to the existence of cases may be the mere existence of doubt to the authorities or gangs or other leak information water would eliminate human life , As in cases of violations of the authorities for human rights , or during civil wars or to reporters and journalists who cover wars and Ghazat and conflicts , wishing to deliver the truth of the world , without being present their lives or the lives of others at risk.

## 2. **The Proposed System**

The proposed system to hide confidential information ( encrypted ) and send it in a subtle , where the force produced by the meeting of these two flags ( encryption and hide ) may be a force for sizeable , where they met with some of the lead to we get secret messages difficult decryption and difficult to realize its existence.

The algorithm includes two major phases:
1 – The hide text message encoded within the image.
2 - Message retrieval

### 2.1. First phase (The hide text message encoded within the image)

At this stage is hiding the text message after encrypted inside the cover (file image) this phase consists of two main stages:
1) The Encryption Process
2) Hiding Process

## 2.1.1. The Encryption process

For the purpose of increasing the confidentiality of the proposed algorithm has been the work of a special blade to the text by conducting the following operations for encoding text sender before the process of hide : -

**1**. Read the message text message from a text file, for example, "I will be in Baghdad"

**2**. Convert text to decimal values in order to be dealt with and perform calculations on them, as in the following:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 32 | 73 | 32 | 119 | 105 | 108 | 108 | 32 | 98 | 101 |
| 32 | 105 | 110 | 32 | 66 | 97 | 103 | 100 | 97 | 100 |

**3**. Find the length of the message to be used in the next stages of encryption and hide.

**4**. Substitution orthographic

To be encryption more complicated we add this type of encryption, in this process is taken every four letters (values ) in a row and are altered positions defined by the function F = (4 1 2 3), that the purpose of switching sites is blending letters (values ), so that cannot be easily broken and that this technique strengthens algorithm and makes them resistant to attack analyst code, the text changed in a method complex , taken every four consecutive values and bring it back to their positions, according to the following: -

- Value fourth takes the first value.
- The first value takes the second value.
- The second value takes the third value.
- Value third takes the fourth value .

While noting the possibility that at the end of the message data preparation less than four remains as it is without the switch and thereby control the situation. Output that we get it as inflowing:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 119 | 32 | 73 | 32 | 105 | 108 | 108 | 105 | | |
| 98 | 101 | 32 | 97 | 110 | 32 | 66 | 100 | 103 | 100 | 97 |

**5**. Bringing the next character for each character by adding one to the value of each character until moving to the next character and as in following:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 120 | 33 | 74 | 33 | 33 | 106 | 109 | 109 | 106 | |
| 99 | 102 | 33 | 98 | 111 | 33 | 67 | 101 | 104 | 101 | 98 |

**6**. Xor factor applied to the results of the previous stage and with a special key (default) key = 113 any message that the values resulting from the previous stages are made to this step[8], output shall be as in following:

80 59 80 80 27 28 28 27 18
23 80 19 30 80 50 20 25 20 19

**7**. Reversing the values of the message, so that the final value is the first and the last are first, any transfer values in the left to right and vice versa, output shall be as in following:

19 20 25 20 50 80 30 19 80 23
18 27 28 28 27 80 80 59 80

**8**. Recent operation from operations encryption is to convert binary entered text (message) convert any one to zero and turn the zero -to-one, where you must precede this process the process of converting the resulting values of the stages of encryption prior to the binary values of any dismantling of the decimal values , which took all the resulting decimal value applied to the output of this code shall be as in following:

00010011000101000001100100010100001100100101000000011110000100110101000000010111000100100001101100011100000111000001101101010000010100000011101101010000000001001

And then apply this process, the heart of any binaries to be a series of the (bits) that will be hidden in the image file as in following:

11011001110101111100110111010111100110110101111111000011110110010101111111010001110110111100100111000111110001111100100101011111010111111000100101011111111110110

### 2.1.2. Hiding Process

After encryption process and the creation of the message transmitted then begin the process of embedding, which begins the process of creating the image (cover) and then embedding, which rely on the idea of cover-ups within the third least significant bit[6], in terms of this process includes the following steps: -

1. Read the image, where the image is color images (RGB).
2. Resize the image with 256x256.
3. Find the dimension of image (number of rows and number of columns ).
4. Image segmentation into three levels, where it is embedding in the third layer, which are in the form of binary matrix.
5. Data transfer to the third layer binary and convert the resulting matrix to matrix unilateral.
6. Taking encrypted bits message (i.e., taking one bit at a time) where they are hiding inside least significant bit and the third as in Figure (1).

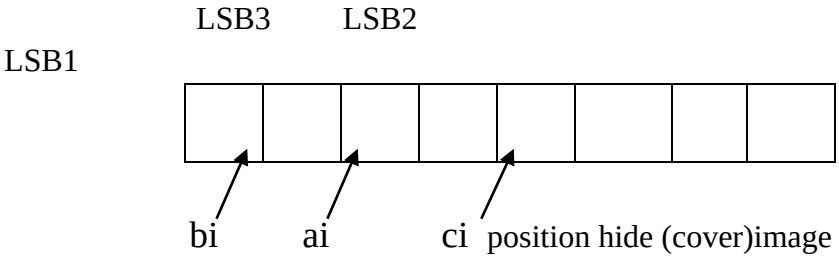
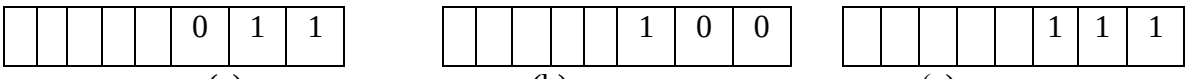



Figure (1) position bit the hide

That's where:
Si: bit encrypted message.
Ci: bit third of the image.
ai: bit the first image.
bi: bit the second for image.
A) If (Si = 1) and (Ci = 0) , it is :
ai = 0, bi = 0
B) If (Si = 0) and (Ci = 1) , it is :
ai = 1, bi = 1
C) IF (Si= Ci) ,it is no thinking.
D) Included (Ci = Si).
E) Repeating step (6) until the end of the bits of the message.

- To illustrate the process of the modified on bit first and bit second in each byte Suppose that:

(Si=1), ( Ci=0),(ai=1), (bi=1)




(a) Byte before embedding

(b) byte after embedding and modifying

(c) byte after embedding and without modifying

Figure (2) the process of embedding

Where we note from Figure (2) that the value of the byte after the embedding and modifying $(00000100)_2$ which is closer to the value of the byte before embedding $(00000011)_2$, where the byte value without modification $(00000111)_2$, where the biggest difference (7-3 = 4) that any (4) closer to (3) from (7), the same applies to the second case of the modification.

- If we assume that:
( Si = 0), (Ci = 1), (ai=0), (bi=0)

Byte value before embedding $(00000100)_2$, byte value after embedding and without modification $(00000000)_2$, byte value after embedding and modifying $(00000011)_2$, that's where (3) closer to (4) of zero.

**2.2. Process of Retrieving the Message**

The include the sequence of steps involved in the process of hiding and encoded , but reversing these steps to be as follows: -

1. Retrieve the bits message from the last of the output image file ( cover) ,the same process that I mentioned earlier in the sixth step of the process of embedding any access to the site of the third least significant bit in each byte and retrieve the bit of it , and as in following:

11101100111010111110011011101011110011011010111111100001111011001010111111010001110110111100100111000111110001111100100101011111010111110001001010111111110110

2. The heart of the resulting binaries i.e. converting one to zero and zero to one as in following:

00010011000101000001100100010100001100100101000000011110000100110101000000101110001001000011011000111000001110000011011010100000101000000111011010100000000001001

3. Converting the resulting binaries to decimal values as in following:

19 20 25 20 50 80 30 19 80 23 18 27
28 28 27 80 80 59 80 9

4. reverse the values of the message, so that the value of the last first and the first value is the last and as in following:

9 80 59 80 80 27 28 28 27 18 23
80 19 30 80 50 20 25 20 19

5. a process xor and the resulting values of the previous stage and with the key used in the encryption and all the values , as in following:

120 33 74 33 33 106 109 109 106 99 102
33 98 111 33 67 101 104 101 98

6. Brought the previous character for each character and add one to every value of the previous values , as in following:

119 32 73 32 32 105 108 108 105 98 101 32
97 110 32 66 100 103 100 97

7. Reverse alphabetical substitution taken every four consecutive values and bring it back to their positions, according to the following: -

- Value first takes the second value.
- The second value takes third value.
- The third value takes the value of the fourth.

- Value fourth takes the first value as in following:
  32 73 32 119 105 108 108 32 98 101 32 105 110 32 66 97 103 100 97 100

**8**. Converting the each resulting values to text character and thus retrieve the encrypted message and the hidden full, namely:

"I will be in Baghdad"

### 2.3. Experiments and Results

applied algorithm proposed on more image file type (jpg) and of different sizes and use the scale peak signal to noise ratio (PSNR) , which measures the accuracy of hide and non-discrimination hidden text in the image by the human eye, for hiding images measure for accuracy includes the account box error identifier and the following two equations(1),(2)[10] : -

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (Fij - Gij)^2 \ldots\ldots (1)$$

$$\text{PSNR} = 10 \log_{10} \frac{L^2}{MSE} \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

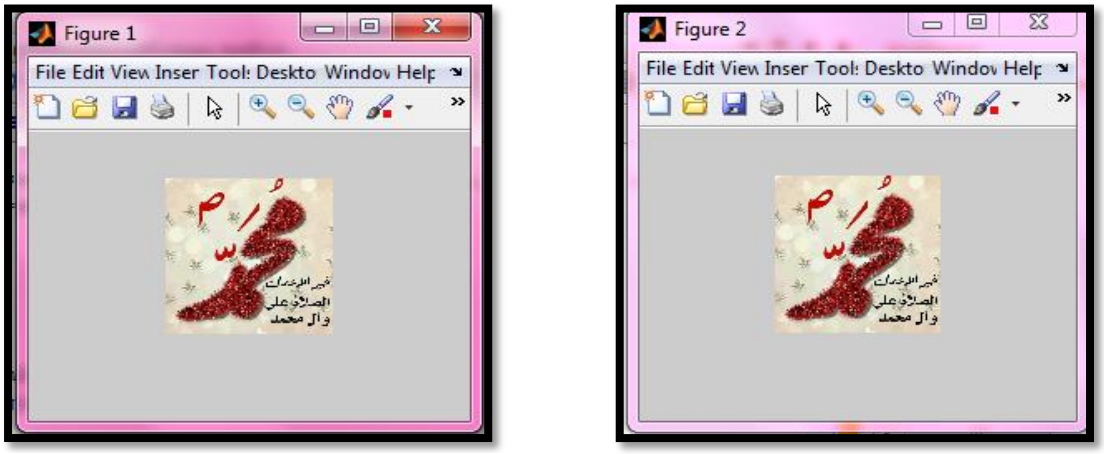
That's where:
M, N: are the row and column for the cover image.
Fij: is the unit of the image (cover) before the hide.
Gij: is unit of image (cover) after hide text inside.
L: is the level of the top of the signal (for a image) and which assign 8 binary digits per unit, it is a sham (L = 255), table (1) illustrates the value of MSE, PSNR after applying the process of hide on several images of different sizes and texts after different characters.

Table (1) measure of MSE, PSNR images of different sizes and the length of the text is different.

| Imagename | Image Size | Text Length | MSE | PSNR |
|---|---|---|---|---|
| Image1 | 400X355 | 1312 | 3.1939 | **7.1853** |
| | | 2210 | 6.3321 | **125.7852** |
| | 650X470 | 1312 | 0.8976 | **145.3689** |
| | | 2210 | 1.2182 | **153.120** |
| Image2 | 400X355 | 1312 | 7.2467 | **178.1242** |
| | | 2210 | 10.7914 | **143.2135** |
| | 650X470 | 1312 | 1.6613 | **135.8950** |
| | | 2210 | 1.9867 | **152.9125** |
| Image3 | 400X355 | 1312 | 23.2918 | **139.9426** |
| | | 2210 | 39.5041 | **138.8215** |
| | 650X470 | 1312 | 3.15568 | **137.2378** |
| | | 2210 | 5.8815 | **146.0487** |
| Image4 | 400X355 | 1312 | 2.2078 | **172.2559** |
| | | 2210 | 4.2567 | **151.6944** |
| | 650X470 | 1312 | 0.7824 | **134.2832** |

| | | | | |
|---|---|---|---|---|
| | | 2210 | 1.1237 | **142.3504** |

Clearly from the table(1) that he increase the length of the text increases the value of MSE , and less than the value of PSNR , but the rate of increase a very small percentage which indicates the efficiency of the algorithm used in the hide , although the length of the hidden text as well as it increased the size of the image increases the efficiency of hide and difficult , but cannot be anyone to distinguish the existence of any text within the image and figures (3) , (4) , (5), (6) describes the images before and after the hide text .

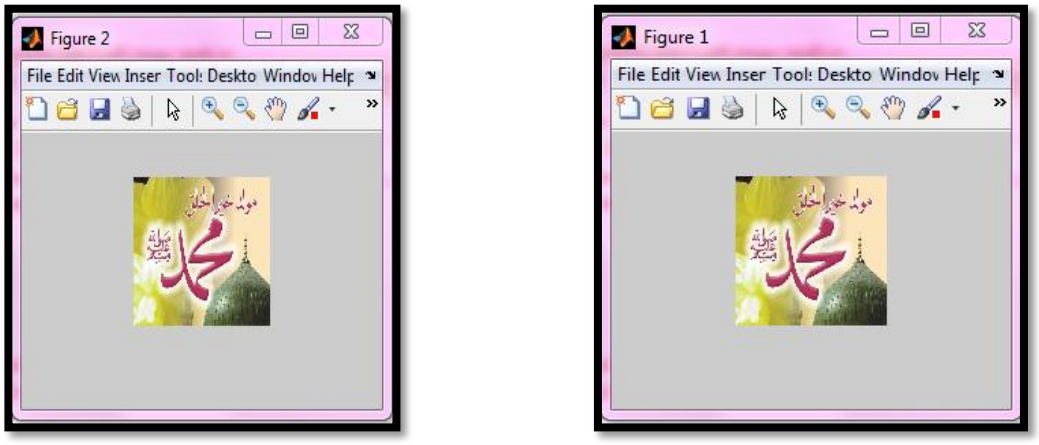



(a) The original image of size (400x355) (b)Image after hide text length 1312 character

Figure (3) (a) the original image of size (400x355)
(b)Image after hide text length 1312 character

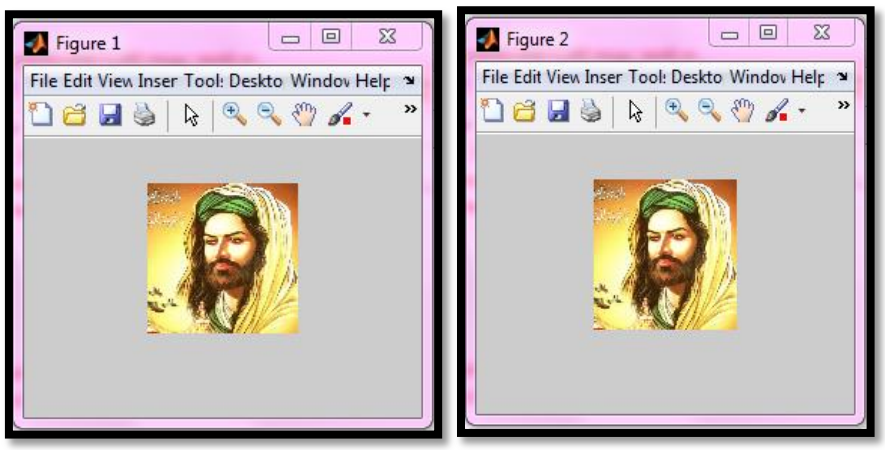

a) the original image of size (650x470 ) (b)Image after hide text length 2210 character

Figure (4) (a) the original image of size (650x470)
(b)Image after hide text length 2210 character




(a) The original image of size (400x355) (b)Image after hide text length 1312 character

Figure (5) (a) the original image of size (400x355)
(b)Image after hide text length 1312 character




(a) the original image of size (650x470 ) (b)Image after hide text length 2210 character

Figure (6) (a) the original image of size (650x470)
(b)Image after hide text length 2210 character

## 2.4. Conclusions

1) Due to the use of color images RGB where which each pixel consists of 24 binary and being does not contain the color palette, in addition to that each color is represented by eight binary digits (one byte), and has been storing binary number one in every color of the tricolor when comparing the original image with the image that contain hidden text, it is the difference that is almost invisible.

2) The encryption method is of appropriate security specifications as well as the

accounts of low complexity and low vulnerability to the recovered images and a few vulnerable to attack harmful.

3) Note that increasing the length of the text increases the value of MSE and PSNR less value and by very few, which shows the efficiency of hide algorithm in spite of the length of the text.

4) From the previous figures and table(1) we note that the proposed algorithm maintains the integrity of the data transmitted (to the fact that the value of the proportion of the error in the MSE is close to zero), which also maintains to keep the image file of in hide is not aware the human eye.

## 3. References

[1]. B. Pfitzmann, "Information Hiding Terminology," *Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174,* Springer-Verlag, Berlin,
pp. 347-356 , 1996.
[2] Rabinovich, "*Steganography–a Cryptography Layer*" Vlad, 1999.
[3] Arampatzis, Avi T., "*Data Hiding*", Report Katholieke Universiteit Nijmegen, School voor Informatica, Bedrijfsgerichte Informatica, 1999.
[4] Brown, C. W., Shepherd, B. J. "*Graphics File Formats Reference and Guide*", Manning Grennwich, 1994.
[5] Iyengar, Venugopal, "*Hiding Messages in Images and Text:Risk Associated with the Technology of Steganography*", 2003.
[6] Cristobal, Patricia, "*Steganography: A Privacy Protector or Just a Computer Security Trick?* ", SANS Institute FIRE 2003 As part of GIAC practical repository. Washington D. C, 2003.
[7] Katzenbeisser, Stefan & Pertitcolas, Fabien A. P.,"*Information Hiding Techniques for Steganography and Digital Watermarking*", 1st edition, Artech House Boston London, 1999.
[8] Qi, Hairong; Snyder, Wesley E. & Sander, William A., "*Blind Consistency-Based Steganography for Information Hiding in Digital Media*". Multimedia and Expo, ICME '02.
Proceedings.IEEE International Conference on Vol. 1, p.: 585- 588 , 2002.
[9] Sellars, Duncan, "*An Introduction to Steganography*",Computer Science Department, University of Cape town South Africa,1999.
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html.

**اخفاء نص مشفر داخل صورة باستخدام البت الأقل أهمية الثالثة**

**زينب باقر دهوس**
*جامعة البصرة/ كلية العلوم/ قسم الحاسبات*

**الخلاصة**

يتضمن هذا البحث بناء نظام لإخفاء نص مشفر داخل ملف صورة (الغطاء) لينتج ملف المادة المخفية , وتتضمن الخوارزمية مرحلتين رئيستين:

1- اخفاء الرسالة النصية المشفرة داخل الصورة, في هذه المرحلة يتم أخفاء الرسالة النصية بعد أن يتم تشفيرها داخل الغطاء(ملف الصورة)وهذه المرحلة تتكون من عمليتين رئيستين, عملية التشفير وعملية الإخفاء.

2- استرجاع الرسالة, وتتضمن الخطوات المتبعة في عملية الإخفاء والتشفير ولكن بعكس تلك الخطوات .
تم تطبيق خوارزمية الإخفاء المقترحة على أكثر من ملف صوري وحققت نسبة استرجاع جيدة لبيانات الرسالة النصية ودون إحداث أي تشويه ملحوظ في الملف الغطاء , وكذلك فانه بزيادة حجم الصورة تزداد كفاءة الإخفاء ويصعب بل لايمكن لأي شخص تمييز وجود أي نص داخل الصورة.

**الكلمات المفتاحية:** الكتابة المخفية ,صورة الغطاء,البت الأقل أهمية,نسبة قمة الإشارة إلى الضوضاء.