A new Approach for Applying (LSB) Method for Information Hiding

MAJID J. JAWAD
Babylon University
E-mail: majid_al_sirafi@yahoo.com

Abstract

When using LSB technique on 8-bit images, more care needs to be taken, as 8-bit formats are not as forgiving to data changes as 24-bit formats are. Care needs to take in the selection of the cover image, so the change to the data will not be invisible in the stego-image.

When modifying the LSB bits in 8-bit images, the pointers to entries in the palette are changed. It is important to remember that a change of even one bit could mean the difference between a shade of red and a shade of blue. Such a change would be immediately noticeable on the displayed image, and is thus unacceptable.

The suggested approach is modifying (LSB) to be used in 8-bits colored images which uses just less than 129 colors.

Keywords*:* Information Hiding; Digital Image; Least Significant Bit (LSB)

الخلاصة

عند استخدام طريقة (LSB) في الصورة الملونة ذات 8-بت فأن هنالك عدة أمور يجب أخذها بنظر الأعتبار، وهذه الأعتبارات غير مأخوذة عند تنفيذ الطريقة أعلاه في الصـــورة ذات 24-بت، وذلك بسبب طبيعة الهيكلية المستخدمة لخزن بيانات الصورة الملونة ذات 8-بت. ومن أهم تلك الأعتبارات هي اختيار الغطاء الأمثل لتطبيق الطريقة أعلاه، وإلا فأن أي تغيير في بيانات الصورة الأصلية سوف يمكن ملاحظته، لأن أي تغيير في بيانات الصورة، ولو في بت واحدة يعني إن المؤشرات الى الألوان في الخلطة (palette) سوف يتغير أيضا.

الأسلوب المقترح هو تطوير طريقة (LSB) لتستخدم في الصورة الملونة ذات 8-بت على أن يكون عدد الألوان المستخدم في الصورة أقل من 129 لون

الكلمات المفتاحية :الاخفاء المعلوماتي،الصورة الرقمية،البت الادنى

1. INTRODUCTION

Steganography is the art of hiding information in ways that prevent its detection. Steganography is usually given as a synonym for cryptography but it is not normally used in that way. It is not intended to replace cryptography but supplement it [Dr.K.Duraiswamy.2006].

The purpose of steganography is to communicate information in a stealth manner so that anyone who inspects the messages being exchanged cannot collect enough evidence that the messages hide additional secret data. As opposed to cryptography that makes the communication unintelligible to those who do not know the proper cipher keys, steganography should make the communication inconspicuous or invisible. [Jessica Fridrich.2007].

2. WHY WE CAN NOT EMBED A SECRET MESSAGE IN 8- BIT COLOR IMAGE?

According to the structure of 8-bit image as shown in Fig (1), each pixel in it is represented by a single byte. This byte is not the color but rather is the location (index) of the color in the palette. When an image is stored, the 8 bit color index for each pixel is saved along with the palette [www.jb101.co.uk/2008/02/01/bitmap-and-indexed-images/]. So any change in data of image will be perceptible, for example if we change pixel (4,4) of value 0 (blue color) to value 2 the color of it will be red since the pointer will point to the location 2 of the palette. So we can't change any value of any pixel (i.e. the embedding in 8-bit image is impossible).

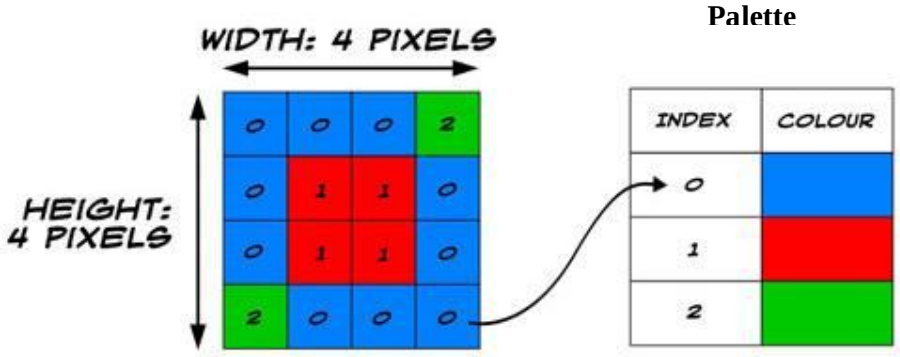

Fig. (1), Structure of 8-bit color

3. CONCEALING IN (LSB) of 24-BIT IMAGE

When applying LSB techniques to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by three bytes. Any changes in the pixel bits will be indiscernible to human eye. For example, the letter A can be hidden in three pixels. Assume the original three pixels are represented by three 24-bit words below:

(00100111	11101001	11001000)
(00100111	11001000	11101001)
(11001000	00100111	11101001)

The binary value for letter **A** is (01000001), inserting the binary value of **A** into the three pixels, starting from the top left byte, would result in:
(00100111 11101000 11001000) (00100110 11001000 11101100)
(11001001 00100110 11101001)

The emphasized bits are the only bits that actually changed. The main advantage of LSB insertion is that data can be hidden in the least and second least bits and still the human eye would be unable to notice it [Raed Mahdi Salih.2001].

4. CONCEALING IN (LSB) OF AUDIO

When hiding information inside Audio files the technique usually used is low bit encoding which is some what similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file [Aelphaeis Mangarae.2006].

5. THE SUGGESTED MEHOD

The suggested method can be as the following:-

- **THE SUGGESTED EMBEDDIGN MEHOD**

The suggested embedding method is shown in algorithm 1 and algorithm 2.

Step 1: Choose any image
Step 2: Find the histogram of this image
Step 3: Count the number of used color
Step 4: If the number >128 go to step 1
Step 5: Re index the sequence of used colors within palette of image to be an even numbers

Step 6: Change the data of image according to the sequence in the palette
Step 7: Make duplicating to all used colors in palette (the sequences of all duplicated colors will be odd sequences and each odd sequence must be after even sequence respectively)

Algorithm 1, Re index and duplicate palette of image

Step 1: Choose the prepared image
Step 2: Choose the secret message
Step 3: Convert the secret message to binary numbers
Step 4: Count the number of bits
Step 5: for x=1 to the number of bits
Step 6: Embed bit(x) in the desired pixel
Step 7: next x
Step 8: Store the stego image

Algorithm 2, embedding the secret message

- **THE SUGGESTED EXTRACTING MEHOD**

The suggested extracting method is shown in algorithm 3

Step 1: Open Stego image
Step 2: for x=1 to number of bits
Step 3: retrieve the embedded bit from stego image
Step 4: next x
Step 5:convert retrieved bits into character
Step 6: Store the secret message

Algorithm 3, extracting the secret message

- **ILLUSTRATIVE EXAMPLE**

To implement the method, let us take 8-bit color image uses 74 colors (that is, there are 182 unused colors). The image is shown in Fig.(2)

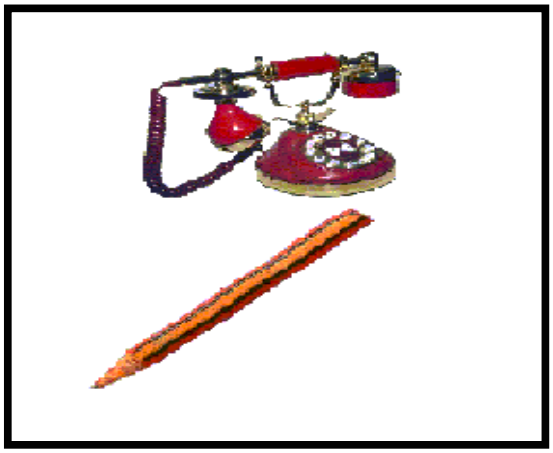

Fig.(2), the original image

The value of used palette is shown in Table (1).

Palette #	Red	Green	Blue	Palette #	Red	Green	Blue
0	0	0	0	128	0	0	128
32	0	0	32	129	64	0	128
36	0	32	32	132	0	32	128
37	64	32	32	133	64	32	128
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
213	64	160	192	251	255	192	255
214	128	160	192	254	128	255	255
218	128	192	192	255	255	255	255

Table (1), values of used palettes of an image in Fig. (2)

Now, *we can re index the sequences of all used color within palette of image to be an even numbers*. Table (2), shows the results of *re index.*

The used colors	**Re index it into**
0	0
32	2
36	4
37	6
.	.
.	.
161	64
164	66
165	68
169	70
170	72
173	74

Table (2), results of Re index palette

Then we can make duplicating to all values of used colors in palette (the index of duplicated values will be odd number, and each odd number must be after even no. respectively).(**For example, if color no. 10 has values R=0, G=0, B=64, then the values of no. 11 will be R=0, G=0, B=64**). After that procedure, we will change the values of image according to the index of palette. Fig.(3)a shows part of actual data of image, Fig.(3)b the image after changing it's palette and actual data, and Table (3) shows the values of palettes after implementing the duplicating procedure.

94	96	2	14
18	20	86	82
12	16	0	8
2	16	94	82

Fig. (3)a, part of actual data of image after changing

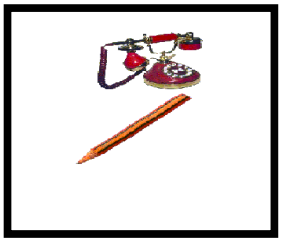

Fig. (3)b, an image after changing it's palette and actual data

(Look! , an image visually is unimpressed)

Palette #	Red	Green	Blue
0	0	0	0
1	0	0	0
2	0	0	32
3	0	0	32
4	0	32	32
5	0	32	32
6	64	32	32
7	64	32	32
8	64	64	32
9	64	64	32
10	0	0	64
.	.	.	.
.	.	.	.
.	.	.	.
52	64	96	128
53	64	96	128
54	128	96	128
55	128	96	128

Table (3), the values of palettes after implementing the duplicating procedure

Now, after changing actual data and palette, a hiding of the data can be done. For example, suppose that we want to hide the letter S (The binary value for it is (01010011)).Character (S) can be hidden in 8 pixels, so if we have the following eight pixels :-

0 (00000000) 2 (00000010) 4 (00000100) 6 (00000110)
8 (00001000) 10(00001010) 12(00001100) 14(00001110)

After embedding procedure (**by using LSB method**), the values of pixels will be :-

1 (0000000***1***) 3 (0000001***1***) 4 (0000010***0***) 6 (0000011***0***)
9 (0000100***1***) 10(0000101***0***) 13(0000110***1***) 14(0000111***0***)

That means the value of index palette 0 will be changed into 1, 2 into 3, etc. This changing will be imperceptible, since the pointing will be into palette no 1 instead 0, or 3 instead 2, and obviously no. 0 and no.1 in the palette have the same values of color (R=0, G=0, B=0) , no. 2 and no.3 in the palette have the same values of color(R=0, G=0, B=32), and so on .

6. CONCLUSIONS AND DISCUSSION

1- Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection). There are an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image.

Steganography does not only pertain to digital images but also to other media (files such as voice, other text and binaries; other media such as communication channels, the list can go on and on).

2-We can hide secret message in any pixel of an image, without any perceptible changing in it.

3- We can apply (LSB) in the palette of image

4- The extraction of secret message is blind, i.e., no original image is needed for secret message extraction.

7. References

Aelphaeis Mangarae*" **Steganography FAQ**"*, March 18th 2006 www.infosewriters/text-resources/pdf/steganography-Amangarae.pdf

Dr.K.Duraiswamy , B.E.,M.Sc.,(Engg),Ph.D." ***SECURITY THROUGH, OBSCURITY*** ", College Of Technology, Tiruchengode., 2006 www.rootsecur.net/content/dowload/pdf/ security through obsecurity.pdf

Jessica Fridrich, Miroslav Goljana, David Soukalb"***Higher-order statistical steganalysis of palette images*** " Department of Electrical and Computer Engineering, Department of Computer Science,SUNY Binghamton, Binghamton, NY 13902-6000,2007 www.ws.binghamton.edu/fridrich/research/pairs01.pdf

Raed Mahdi Salih, ***"information Hiding in Wave Media File by Using Low Bit "***, M. Sc thesis, University of Technology, 2001.

www.jb101.co.uk/2008/02/01/bitmap-and-indexed-images/