ACSIJ
WWW.ACSIJ.ORG

A New Image Steganography Method Based on Pixel Neighbors and 6 Most Significant Bit(MSB) Compare

Mashallah Abbasi Dezfouli[1], Sajad Nikseresht[2] and Seyed.Enayatallah Alavi[3]

**[1&2] Department of Computer Engineering, Science and
Research Branch, Islamic Azad University
Khouzestan, Iran**
Abbasi_Masha@yahoo.com

Nikseresht.Sajad@yahoo.com

**[3] Department of Computer Engineering, Shahid
Chamran university of Ahwaz**
Se-alavi@yahoo.co.uk

Abstract

Today, steganography is known as an effective way to convey secret data. A wide range of techniques has been developed in this context, each seeking to improve certain problems of their own. The current paper presents a method by which, when comparing three color values at each pixel to the corresponding ones from all its eight neighbors, it is attempted to embed message bits into the two least significant bits of a color component of an image that an acceptable color difference has happened in. Due to the mechanism proposed, this method makes the message difficult to be discovered. However, since message detection does not need to insert additional data to identify the colors containing message bits, changes in image is less and the imperceptibility is higher.

Keywords: Steganography, Digital Image, Pixel, Imperceptibility.

1. Introduction

As we are now witnesses, the proliferation of computer networks has resulted in developed human relationships and these networks have their advantages for data transmission. As a means for conveying secret information, the application of computer networking requires such a technique that no one, apart from the sender and intended recipient, understands secret message even if he/she can discover the communication. To this end, many different types of encryption techniques exist that can ensure data confidentiality; however, the incomprehensible and encrypted form reveals that the message contains confidential information [1], [2]. Here, we seek to transform secret information in such a way than no one suspects the existence of the message, and steganography provides some very useful and important techniques in this field. The typical steganographic methods include the concealment of information within a transport layer (images, audio and video files) that looks a normal and justified message in order to convey certain message so that it is hard for anyone but the intended recipient to read or detect the original data.

The word steganography combines the Greek words **Stegan◌́s**, meaning "covered or protected," and **Graptos**, meaning "writing" [3]. steganography is concerned with concealing a secret message inside of a carrier, such as an image file or a media file. The key principle is that no one could suspects the existence of confidential messages, unless the sender and intended recipient.

There are five types of steganographic techniques; namely, Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Protocol Steganography. Text Steganography is among the most popular approaches used in the ancient times. And, one of the related techniques is called Null Cipher where the nth letter of every word is used to from a hidden message and taking these letters successively yields the real message [4]. In digital world, steganography is actually done by manipulating the letter size, font, spacing, typeface or other characteristics of a text. For example, containing a blank space at the end of lines represents “1”, otherwise “0” [8]. Audio Steganography can be done in several different ways. Using the least-significant bit is possible, as modifications will usually not create audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks [5]. However, since video materials are combined of audio and video files, the same methods can be used to conceal message into video files [6].

Protocol Steganography refers to the technique of embedding information within the message used network transmission [4]. An example of hidden message placed in a TCP/IP packet header is provided by [7]. Less-often used and optional fields are good choices for hiding Secret information. Image Steganography exploits image properties and the weakness of the human visual system for information hiding. The methods typically used in such steganography involve modification of spatial domain and frequency domain. The spatial domain techniques work by replacing low-order bits of the pixels with the message to be sent, while techniques in frequency domain make use of mathematical transform coefficients of the original image to embed message bits.

2. Previous works

2.1 Least Significant Bit (LSB) Method

This is one of the most important and popular techniques of steganography. By this method, least significant bits of the pixel (in black & white images) or colors (in true color images) are used to embed secret message bits. It is a good steganographic mechanism since changes in a least significant bit yield few changes in the original image. Suppose, for example, the letter “G”, which is represented by the American Standard Code for Information Interchange (ASCII) with the numerical value as "01000111", is replaced with the following pixel values (the underlined bits represent the embedded bits):

Pixel 1 = (R=00011101, G=00111010, B=11001010) => (R=0001110**0**, G=0011101**1**, B=1100101**0**)

Pixel 2 = (R=01011001, G=10011011, B=11001110) => (R=0101100**0**, G=1001101**0**, B=1100111**1**)

Pixel 3 = (R=10010100, G=10101001, B=00110000) => (R=1001010**1**, G=1010100**1**, B=00110000)

The LSB approaches are divided into two fixed- and variable-length categories [8]. By the fixed-length methods, a given number of least significant bits of an intended byte are selected for embedding. In the variable-length methods, in contrast, various numbers of least significant bits of the intended byte are chosen [9]. Simplicity and the occurrence of little changes in the image are the advantages of these techniques, while the disadvantage includes the probability of fast detection.

2.2 Pixel Indicator Method

Adnan Gutub et al. (2010) in reference [10] developed a method where a single color among three color components of a pixel was served as the pixel indicator; meaning that it indicates which colors in the pixel contains hiding bits of a secret message. Random values are selected for the indicator of each pixel, based on which message bits are placed in other colors of that pixel. The indicator uses two bits inserted inside two least significant bits of a specific color considered as the indicator. To increase the security of this technique, the color chosen as the pixel indicator is varied, so in the first pixel, Red is the indicator, Green is Channel 1, and Blue is Channel 2. For second pixel, Green is the indicator for pixel, Red and Blue act as Channel 1 and Channel 2, respectively. Finally, in third pixel, Blue is the indicator, while Red is Channel 1 and Green is Channel 2. The embedding of message is flowcharted in Figure 1.

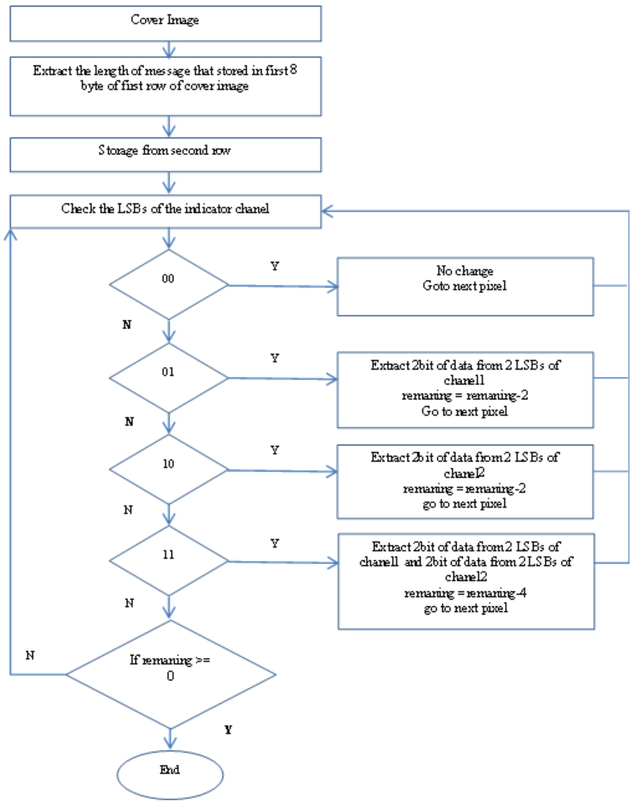

Cover Image
Extract the length of message that stored in first 8 byte of first row of cover image
Storage from second row
Check the LSBs of the indicator chanel
00
Y
No change
Goto next pixel
N
01
Y
Extract 2bit of data from 2 LSBs of chanel1
remaning = remaning-2
Go to next pixel
N
10
Y
Extract 2bit of data from 2 LSBs of chanel2
remaning = remaning-2
go to next pixel
N
11
Y
Extract 2bit of data from 2 LSBs of chanel1 and 2bit of data from 2 LSBs of chanel2
remaning = remaning-4
go to next pixel
N
N
If remaning >= 0
Y
End

Fig.1 Pixel Indicator Embedding Process[10]

Because of the application of indicator, this method needs a wide space and, obviously, registration of color information can affect image quality.

2.3 A Better RGB Channel Based Image Steganography

This technique exploits the idea of Pixel Indicator; any color with maximum value between three color components of the original image is chosen as the color indicator. If Red is the indicator, then Green is Channel 1 and Blue is Channel 2. When Green acts as the indicator, Red is Channel 1, while Blue is Channel 2. And, when

Blue is the indicator, then Red and Green are Channel 1 and Channel 2. The algorithm of this method is described as follows:

Step-1: Receive the secret message. Apply RSA Algorithm and convert it to cipher text. Now get it in binary.

Step-2: Receive the RGB Image. Convert to binary. Calculate the sum of R channels of all the pixels, sum of G channels of all the pixels and sum of B channels of all the pixels. The channel having maximum sum is the indicator channel. Four bit data is to be hidden in one of the channels other than the indicator, in the following manner.

Step-3: Suppose, the two channels other than the indicator channel are channel1 and channel2. If R is the Indicator channel, then G is channel1 and B is channel2. If G is the Indicator channel, then R is channel1 and B is channel2. If B is the Indicator channel, then R is channel1 and G is channel2.

Step-4: Divide the cipher text into groups of four bits each.

Step-5: Take the next pixel, take the next four bits of cipher text. Do any of the following 4 sub steps.

(a). If (channel1 value ⩽ 63 and channel2 value > 63) Embed the 4 bits of cipher in channel1 and set 8th bit of indicator channel to 0.

(b). If (channel1 value > 63 and channel2 value ⩽ 63) Embed the 4 bits of cipher in channel2 and set 8th bit of indicator channel to 1.

(c). If (Channel1 value ⩽ 63 and channel2 value ⩽ 63) Then, If Channel1 value ⩽ Channel2 value, Embed in channel1 and set 8th bit of indicator channel to 0. Otherwise Embed in channel2 and set 8th bit of indicator channel to 1.

(d). If Channel1 value > 63 and channel2 value > 63) do not embed in this pixel.

Step-6: If embedding of cipher text is not yet over go to step-5.
Step-7: Stop

The message can be Extract just by retrieving the starting and final color indicator and pixel indicator embedded in reserve positions, and reading the message bits based on the color indicator of each pixel. Then, decrypting encrypted data is only possible with using the RSA algorithm.

Compared to the Pixel Indicator method, this technique uses small number of bits as the indicator. However since four message bits are placed inside 4 least significant bits of the color, the possibility of changing in image will be more, and therefore image quality will be diminished.

3. Proposed Method

Like any other steganographic techniques, the present method is composed of two processes of message embedding and Extraction. Each of these processes will be described below.

3.1 Message Embedding Process

3.1.1 Color Selection Algorithm

In this step, an image is read pixel by pixel from left-to-right and top-to-bottom, and six most significant bits are selected from each color in the pixel and compared to corresponding ones at all eight neighboring pixels. If compared difference is higher then a given N, then the intended color in the certain pixel is selected to embed information in two least significant bits. Figure 2 shows how to read an image. As seen from Figure 2, pixels along the edge of the image will never chosen as selecting pixels. These pixels are used to hold little information that will be described latter.

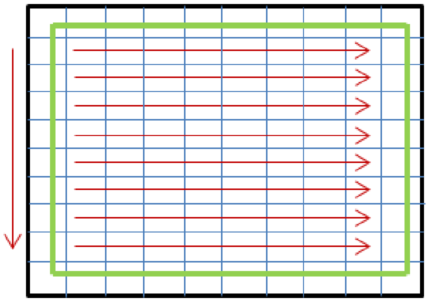


Fig.2 Reading Scheme of Image Pixels

Figure 3 shows, for example, the Pi,j pixel with a distinguished color and compare its colors with all neighbors.

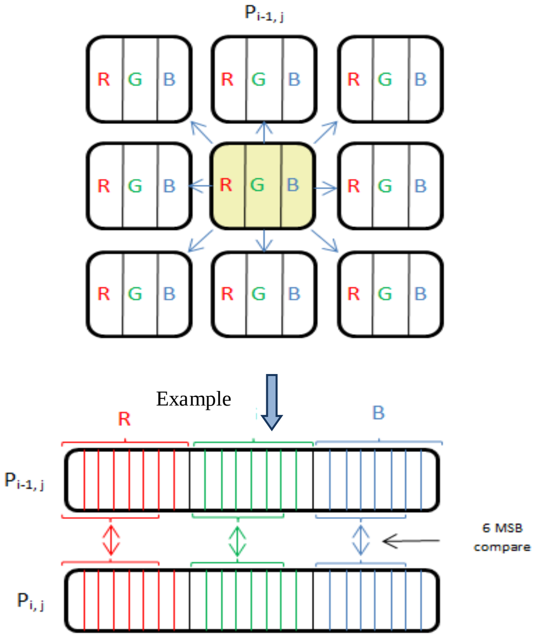


Fig.3 6 MSB Compares

The following Pseudocode shows how to read an image and select colors of the pixel.

```
For Ycount = 1 To Picture.Height – 1
    For Xcount = 1 To Picture.Width - 1
        Select MainPixel
        For Each Neighbor In MainPixel.8Neighbors
            If |MainPixel.R.6MSBbits – Neighbor.R.6MSBbits| > N then
                Choice MainPixel.R    //For Embed in 2 LSB bits
            End if
            If |MainPixel.G.6MSBbits – Neighbor.G.6MSBbits| > N then
                Choice MainPixel.G    //For Embed in 2 LSB bits
            End if
            If |MainPixel.B.6MSBbits – Neighbor.B.6MSBbits| > N then
                Choice MainPixel.B    //For Embed in 2 LSB bits
            End if
        Next
    Next
Next
```

Using this mechanism for selecting colors can be justified by the fact that message bits are embedded in positions where acceptable color differences happened. Because in such positions, changes in color intensity are more difficult to detect. Optional values are given for N; with greater values of N, those with higher color differences are selected. Choosing a small number of colors, however, results in the reduction of data embedding capacity.

In order to determine the effect of N on selecting colors, the color selection algorithm is applied for the below picture by different values of N. This is a standard Peppers color image of size 256 × 256.

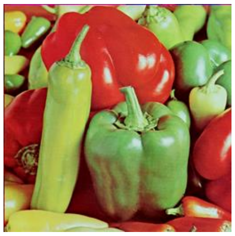
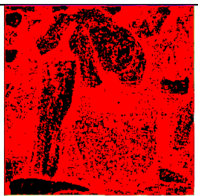
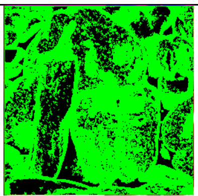
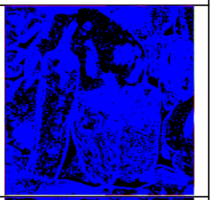
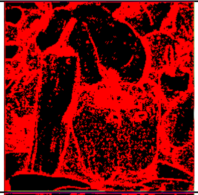
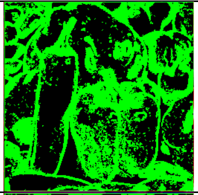
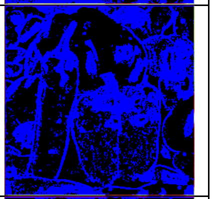
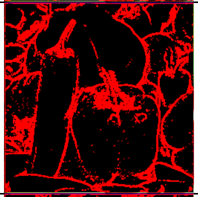
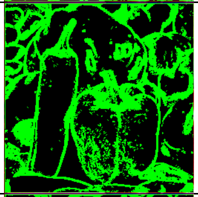
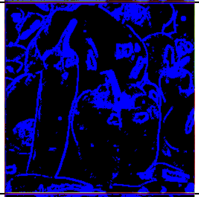
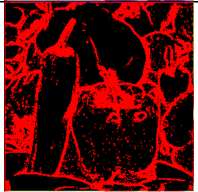
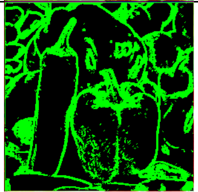
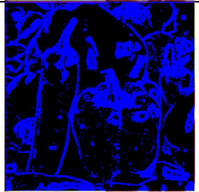
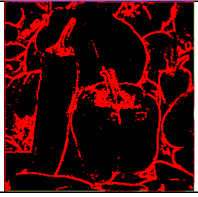
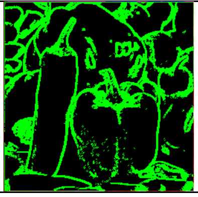
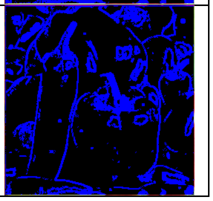


Fig.4 Pepper 256 × 256

Table 1: Margin specifications

N	Selected components of Red to be embedded in two LSBs	Selected components of Green to be embedded in two LSBs	Selected components of Blue to be embedded in two LSBs
1			
2			
3			
4			
5			

According to Table 1, it can be found that with greater values of N, those with higher color differences are selected. In other words, higher N will select the edge of the image to embed message bits.

Some potential colors are now determined, and so it is enough to transform message into binary numbers and embed it inside two least significant bits of potential colors.

In order to prevent increased changes in the original image while embedding messages with low capacity, message bits are first embedded in the first least significant bit of potential colors, and next if some bits remained, they will be placed in the second least significant bit of potential colors. Figure 5 shows a byte with specified positions of first and second LSB.

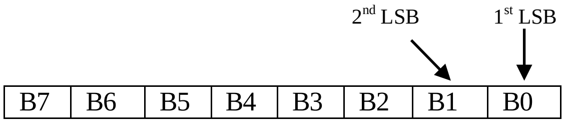


Fig.5 Position of LSB's

3.2 Data Extraction Process

To retrieve message needs to know two values: one for N, and other for coordinates of intended pixel and color where the last bit of the message is placed. As follows, these values will be embedded in the first least significant bit of the color components in the pixel along the edge of an image that presented by green color in Figure 2. The character "#" is used as a separator.

N	#	X	#	Y	#	Color

Fig.6 Header of message

When these values obtained, the message can be easily retrieved by using the color selection algorithm and reading the least significant bits according to the method of embedding message bit.

4 Experimental results

The proposed technique is investigated through a comparative study with ref [11]. For this end, nine standard images of size256 × 256 are used to compare two parameters of capacity and transparency. To determine the first parameter, the capacity available for message embedding by the proposed method is computed in terms of bit. To compute the second, The PSNR criterion is applied. The higher value of PSNR indicates small changes and higher transparency of the image. The PSNR criterion is given as below [12].

$$\text{MSE} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{x,y}-C_{x,y}\right)^2}{M\times N} \qquad (1)$$

$$\text{PSNR} = 10\times log_{10}\left(\frac{c_{max}^2}{MSE}\right) \qquad (2)$$

where M and N are width and height of the image, respectively. C and S represent the original image and the steganography image. And, C_{MAX} specifies the maximum value of pixel intensity that is 255 for 8 -bit images.

Fig.7 Standard pictures

Table 2: Results

Picture	***Message Size(bit)***	***Ref.[11]***			***Proposed***		
		Capacity(bit)	***PSNR***	***MSE***	***Capacity(bit)***	***PSNR***	***MSE***
Aerial	8000	8696	51.569	0.453	**381734**	**65.063**	**0.020**
Airplane	8000	12152	52.335	0.379	**219384**	**65.084**	**0.020**
baboon	8000	86832	42.486	3.667	**383926**	**55.061**	**0.202**
Building	23000	29386	47.556	1.141	**268942**	**60.442**	**0.058**
Earth	60000	72808	44.319	2.405	**275776**	**56.286**	**0.152**
Lena	70000	72336	42.725	3.550	**334148**	**55.610**	**0.178**
Parrots	100000	116040	40.938	5.239	**207498**	**54.065**	**0.254**
peppers	130000	139756	39.995	6.506	**348300**	**53.019**	**0.324**
SailBoat	105000	110980	40.960	5.211	**347906**	**53.868**	**0.266**

5 Conclusions

The current paper provided a technique by exploiting differences made between colors to embed message bits in two least significant bits. Since color selection is based on color differences and values of variable N, the message will be hard to detect. Furthermore, as there is no need to insert additional information, changes in image will be small and image quality will be higher. Another important point to be mentioned is that embedding which is first applied on first least significant bits and, then, second least significant bits yields few changes in the original image for messages with small sizes. Because changes in second least significant bits will make more changes in color values. Therefore, it is likely to be avoided, unless this approach needs to be worked.

References

[1] Shirali-Shahreza, Mohammad Hassan, and Mohammad Shirali-Shahreza, "A new approach to Persian/Arabic text steganography", 5th IEEE/ACIS International Conference on Computer and Information Science (ICISCOMSAR06), 2006 , pp. 310- 315.

[2] Kawaguchi, Eiji, and Richard O. Eason, "Principles and applications of BPCS steganography", Photonics East (ISAM, VVDC, IEMB), 1999, pp. 464-473.

[3] Magut, Sheila Jeruto, "An Overview of Digital Steganography", Jurnal ilmiah, 2010.

[4] Rabah, Kefa, "Steganography-the art of hiding data",Information Technology Journal 3, no. 3, 2004, pp. 245-269.

[5] T. Moerland, "Steganography and Steganalysis", Universiteit Leiden, Rhone-Alpes , 2003.

[6] Papapanagiotou, Konstantinos, Emmanouel Kellinis, Giannis F. Marias, and Panagiotis Georgiadis, "Alternatives for multimedia messaging system steganography", Computational Intelligence and Security, 2005, pp. 589-596.

[7] Ahsan, Kamran, and Deepa Kundur, "Practical data hiding in TCP/IP", Proc. ACM Workshop on Multimedia Security, vol. 2002, 2002.

[8] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang,"Fingerprinted secret sharing steganography for robustness against image cropping attacks", INDIN'05. 2005 3rd IEEE International Conference, 2005, pp. 717-724.

[9] Lou, Der-Chyuan, and Jiang-Lung Liu, "Steganographic method for secure communications", Computers & Security 21, no. 5, 2002, pp. 449-460.

[10] Gutub, Adnan, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, "Pixel indicator high capacity technique for RGB image based Steganography", WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications, 2008.

[11] Swain, Gandharba, and Saroj Kumar Lenka, "A Better RGB Channel Based Image Steganography Technique", Global Trends in Information Systems and Software Applications, 2012, pp. 470-478.

[12] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing 90, no. 3, 2010, pp.727-752.

Mashallah, Abbasi Dezfouli B.S. in Math. From Jundi shapour Uni. 1971 Ahwaz, Iran, M.S. in Computer Eng. U of Utah 1978 Salt lake City USA, Ph. D. in Computer software, New South Wales 1994 Astralia' assistant Pro. At Shahid Chamran Uni. And Science and Research Khouzestan, Islamic Azad University Research interests includes Image processing, and Data Mining. Book title Software Engineering and more than 30 papers.

Sajad, Nikseresht received the B.S. degree in Software Engineering from the Islamic Azad Uni and the M.S. degrees in Software Engineering from Ahvaz Science and Research Branch in Iran, in 2008 and 2013, respectively. His research interests include Steganography and image processing.

Seyed.Enayatallah, Alavi B.S. Computer Eng. From Isfahan University of Technology 1993 Isfahan, Iran, M.S. in Computer Eng. Shiraz University 1996 Shiraz, Iran, Ph. D. in Computer Eng., BNTU 2011 Minsk,belarous, assistant Pro. At Shahid Chamran Uni. Research interests includes Image processing, and neural network. More than 30 papers.