© Journal of the Technical University - Sofia
Plovdiv branch, Bulgaria
"Fundamental Sciences and Applications"
Vol. 26, 2020

Finding the Optimal Color Channel for Information Hiding in LSB Insertion Method

Andaç ŞAHİN MESUT, Özlem AYDIN, Emir ÖZTÜRK

Trakya University, Engineering Faculty, Computer Engineering Department
Edirne/Turkey

andacs@trakya.edu.tr, ozlema@trakya.edu.tr, emirozturk@trakya.edu.tr

Abstract. Huge amount of data is shared online with the development of technology and internet. This development provides various potential to users. Although, securing the data on the digital platform has been one of the most important issues. Various methods have been developed for data security. Encryption and steganography are the most used ones. These are used as complementary rather than alternative. While the purpose of the encryption is to protect the content of the data, steganography is concerned with hiding the existence of the data. Therefore using two methods together will increase data security. Steganographic methods could be applied to different types of digital media. In this study LSB (Least Significant Bit) insertion method which is widely used to hide information in image video and audio files will be applied on image files with 24-bit bmp format. The data will be hidden in only one of the channels. After evaluating the changes on each channel, best channel to hide data will be selected and used.

1. Introduction

Steganography is a very ancient data hiding method dating back to Ancient Greece and Herodotus. The word steganography is derived from the Greek alphabet, whose roots come from the words "στεγαυος" and "γραΦειν". It has a meaning of "covered writing" [1]. The purpose of the steganography is to hide the presence of information or confidential data. The message or a file that we want to send online is stored in another innocent-looking media, preventing third parties from being aware of the message being transmitted [2]. With this approach data could be stored on many environments like text, audio, image, video, html files or TCP/IP packets.

In this approach, the medium which has the hidden information is called cover-data or cover-object, and the resulting medium is called stego-text or stego-object [3].

To hide information into image files there are several steganographic methods. Least significant bit insertion method is one of the widely used methods [4]. In the least insignificant bit method, the last bit of each byte of pixels in image is replaced by the bits of the data we want to hide.

It is important to identify the channel with minimum change for LSB process to hide the information. Too much change of bits in LSB method causes detection of a change on the cover object. Therefore, keeping the change to a minimum will make it difficult to detect the hidden information.

In this study, a method is developed to select optimal color channel for hiding data is automatically in a 24-bit bmp format image file. JPEG-like image compression formats store the input images by

 Online ISSN 2603-459X

encoding them in the frequency domain. For this reason, the bitmap format has been chosen since encoding and decoding an image with JPEG on stego image causes data loss even in lossless compression.

2. Least Significant Bit Insertion Method

The least significant bit (LSB) insertion method is a widely used and it is simple to apply. However, if the method is applied carelessly, data loss could be occured [5]. The LSB insertion method is based on replacing the least important bits of the cover-object in order to store confidential data in such a way that the human eye cannot detect. In this method, the change of trailing 1 or 2 bits cannot be perceived by the human eye.

The addition to the last bit can be done sequentially, from the beginning or end of the image, or by making changes to a specified pixel using a random function generator.

A digital image is in the form of a matrix of N rows and M columns. Each element of the matrix is called pixels. 24-bit images use 3 bytes per pixel. The color of each pixel is obtained from three main colors: Red (red), Green (green), Blue (blue). Each color can be between 0 and 255. This is called the RGB value of the pixel [6].

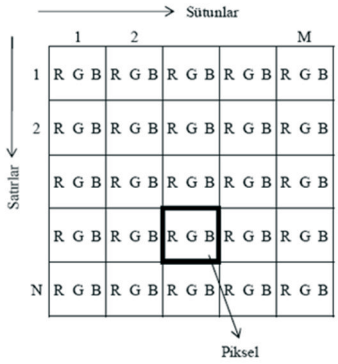

Figure 1. The structure of 24 bpp digital image.

For 24 bpp pictures, LSB method is applied as follows. Let the bit sequence to be hidden be “101011”. The RGB color values of the two pixels next to each other are given as follows.

01000110 11000001 01101011 (70,193,107)
01000111 11000011 01101000 (71,195,104)

After the last bit of each byte of the pixels are used for information hiding, the changing bits and the new values of the pixels are as follows.

01000111 11000000 01101011 (71,192,107)
01000110 11000011 01101001 (70,195,105)

3. Evaluation of Steganographic Methods

When evaluating a steganographic method or algorithm, 3 basic criteria are taken into consideration. These are named as:

- Capacity
- Change in cover data
- Resistance.[7]

There are various measurement methods for determining the change in the cover data or the error rate in the picture. The most well-known among them are; MSE (Mean Squared Error), RMSE (Root Mean Squared Error) and PSNR (Peak Signal to Noise Ratio). MSE is the average of the sum of squares of errors. RMSE is the square root of MSE. Sometimes, instead of MSE, the relationship of the magnitude of the error to the peak (peak) of the original pixel value is concerned. In such cases, PSNR method is used [7].

Steganalysis methods are used to measure the resistance criterion. Steganalysis is a method that aims to find out if there is any information in a cover data and to obtain this information. Some of these methods are Histogram Analysis, RS Steganalysis, Chi-Square Test and Visual Attacks [7].

In LSB method, capacity is related to the size of the picture.

4. Developed Application and Obtained Results

The developed application performs the data hiding the in the given image file. The channel for hiding data could be selected either manually or automatically. The application calculates how much changes are made in each color channel when entering data in real time for automatic channel selection. The application then select the channel that carries the data hiding process is minimal change. One byte is used to store the channel information in order to determine which channel has information during the reading stage. At the stage of reading the data, this given character is searched in each channel, and if it is found, the rest of the data is read from this channel. The size of the data to read is stored after this one byte field. The developed application is given in Figure 2. The application detects the amount of changed bits of each channel real-time and performs information hiding to the channel with the least bit change. In this way, it is aimed to minimize the possibility of detecting information.

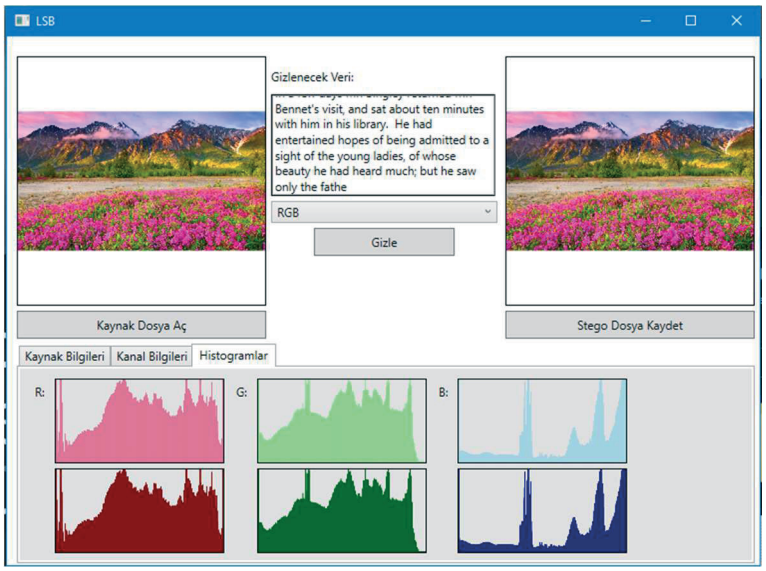

Figure 2. Developed application.

In the experiments, several different pictures with four different classes as large and small at two different levels of complexity are selected (Figure 3) and 1, 3 and 10 kb parts of “Oxford, Pride and Prejudice, Chapter 1-3” were hidden on them (Table 2).

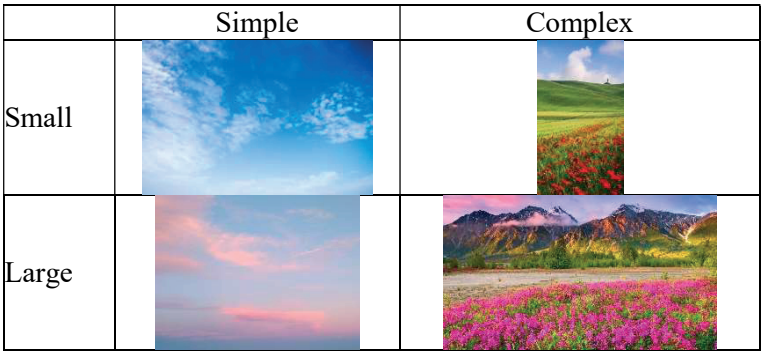

Figure 3. Examples of Cover-Images

In addition, the information storage capacity of each image is given in Table 1 in bytes.

	Simple	Complex
Small	20812	90880
Large	633981	180000

Table 1. Capacity of images in bytes

	Small		Large	
	Simple	Complex	Simple	Complex
1Kb	R: 0.007 G: 0.016 B: 0.024	R: 0.002 G: 0.003 B: 0.005	R: 0.0002 G: 0.0005 B: 0.0008	R: 0.0009 G: 0.0019 B: 0.0028
3Kb	R: 0.024 G: 0.048 B:0.073	R: 0.005 G: 0.011 B: 0.017	R: 0.0008 G: 0.0016 B: 0.0024	R: 0.0028 G: 0.0057 B: 0.0086
10Kb	R:0.080 G:0.163 B:0.246	R: 0.018 G: 0.037 B: 0.056	R: 0.0020 G: 0.0050 B: 0.0080	R: 0.0095 G: 0.0191 B: 0.0287

Table 2. MSE of stego-images

The MSE values obtained are given in Table 2. To calculate MSE, the pixel values of the original and modified images are compared and summed by taking the squares of the differences for each pixel, and the total value is divided by the number of pixels. For channels, this calculation is done separately for each channel in pixels.

As seen in the Table 2, the change rate of bits decreases as the size of the picture increases and error rate increases as the hidden data grows. Thus, a large amount of data hidden on a small picture will increase MSE and also increase the probability of detection. Also, when the given capacities in Table 1 are examined, the values in Table 2 show that the complexity of the picture does not have an effect on MSE. In small images, the MSE value of complex image is less because it is larger and MSE is lower for simple image on large ones because simple image is also larger.

The application we developed selects the channels shown in bold in Table 2 for steganography operation. To achieve this, the application performs the hiding operation simultaneously for all channels in memory before the information hiding process. When a request is made to hide data afterwards, the application calculates the amount of change of channels in memory, and selects the channel with the minimum change and hides the data to selected channel.

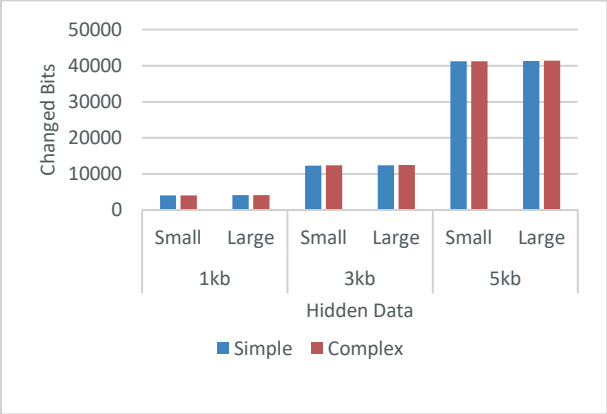

Figure 4. Mean changed bits for different files

In order to obtain the chart in Figure 4, data is hidden in all channels in the picture respectively, and the changing number of bits is obtained. Then, these changes are averaged for all images. As can be seen from the chart, the complexity of the picture does not have a big impact on the changing number of bits. It is also seen that the changing number of bits is not related to the size of the picture.

5. Conclusions

In LSB method, it is important to minimize the change of bits in order to reduce the possibility of obtaining confidential information. In this study, the channel selection process, in which the change was kept to a minimum, was performed by tracing the bit changes.

MSE after hiding information decreases with the size of cover-data used. In addition, the complexity or color variation of the selected image did not affect the bit changes caused by the hidden information. For all image files used, the least change of bits appeared in the red channel while the most appeared in the blue channels. Even in the picture with the most changes, there was no visible change on the histogram.

In order to select optimum channels to hide data, the application we developed has followed the changes in memory and selected the minimum changing channels. Thus, it is aimed to minimize the detectability of data hiding process.

References

[1] Murray A.H., Burchfiled R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.

[2] Wang H., Wang S., "Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47, no. 10, October 2004.

[3] Kharrazi M., Sencar H.T., Memon N, "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series, April 22, 2004.

[4] Sellars D., "An Introduction to Steganography", Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400W/ NIS04/papers99/dsellars/index.html

[5] Cox I.J., Kilian J, Leighton T., Shamoon T., "A Secure, Robust Watermark for Multimedia", Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1, 174, Springer-Verlag, Berlin, 1996, pp. 185-206.

[6] Morkel T., Eloff J.H.P., Olivier M.S., "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005/

[7] Westfeld A., Pfitzmann A., "Attacks on Steganographic Systems", Information Hiding. Third International Workshop, IH'99, Dresden, Germany, September/October, 1999, Proceedings, LNCS 1768, Springer-Verlag Berlin Heidelberg 2000. 70.