iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 5 No. 1, January, 2015

New Spatial Domain Steganography Method Based On Similarity Technique

Abdul MonemS.Rahma , Matheel E.Abdulmunim, Rana J.S. Al-Janabi
Computer Science Department, University of Technology, Baghdad, Iraq

ABSTRACT

In this paper, a new steganography technique based on the similarity between cover RGB image and secret message is depended. Various steganography techniques have been proposed in literature. The Least Significant Bit steganography is one of them in which least significant bit of the image is replaced with data bit. This method is susceptible to steganography analysis and to make it more secure, in this research, cover Bmp image is divided into several blocks. These blocks can be tested to elicit blocks that are most closely resembling to a secret message, then in each block find out two channels that provide the highest similarity to secret message and consider the remaining channel as indicator. So the indicator may be different in each block. In each pixel of these extracted blocks, the indicator can be represented by one bits if there is no hidden data, otherwise, two bits are used, first bit to indicate there is embedded data, second bit to indicate to the channel that store larger number of bits. This method is more secure than conventional least significant bit method through changing sequential data storage style that the least significant bit technique uses, since secret message is divided into portions and each portion is stored into most similar block to it. So, this algorithm gives high peak signal to noise ratio for steganography image and also good capacity since each pixel containing hidden data stores five bits.

Keywords*: Color Cycle Stego, LSB modification, new indicator technique, hiding information in non-sequential style.*

1. INTRODUCTION

Steganography is the science of communicating in a way which hides the existence of the communication. The goal of steganography is to hide information inside harmless messages in a way that does not allow any enemy to even detect that information is present [1].

Cryptography is a method of secret writing and it makes a message unreadable by intruder but does not hide the presence of the secret communication. Although steganography is different from cryptography, there are many similarity between the two, and some make steganography similar to cryptography [2]. This paper will focus on steganography as independent field. Steganography is applicable to the following areas [3].

1. Secret communication and data storing
2. Media Database systems
3. Protection of data transferring
4. Access control mechanism for digital content distribution

The area differs in what feature of the steganography is utilized in each system. There are several types of steganography techniques, Least Significant Bit algorithm (LSB) is one of them. It is very vulnerable to a lot of attacks even the most regular ones. It is really simple to accumulate bit in LSB to discover secret message. This method doesn't use a sequential store of hidden information. As well as gives good capacity.
Because of steganography concern in hiding secret message, it is important to select suitable cover image that secret message can store in it, it prefers cover image doesn't exist on website, because attacker can compare between original and stego image, also smooth region should be avoided [6].

The format of this paper is as follows. Next, we explained the related work in section2, the proposed algorithms are outlined in section 3, section 4 explains the results, and conclusions are in section 5.

2. RELATED WORK

The technique of secret communications is called Steganography. Its purpose is to hide the appearance of communications over a public channel. There are several cover file formats used, but image files are one of the most popular because of their frequency on the Internet. To hide confidential information in images, there are a lot of steganography techniques and some are more complex than others, however, all of them have their pros and cons [4].

The method proposed by Parvez and Gutub (2008) introduces the concept of storing changeable number of bits in each channel. Color of the channel are used to decide the number of data bits to store. This approach provides really high capacity with low visible distortions [5].

A new RGB channel based steganography was proposed by Gandharba Swain and Saroj Kumar in (2012), it provides two levels of security, first at cryptography level and the second at

steganography level. The message using a key that provide another level of security [6].

The principle of cycling through color values in each pixel in order to store the data is called (Color Cycle Stego), this method makes the detection of hidden data much more difficult. This also means that the same colors channel were not constantly being changed. For example the first data bit could be stored in the LSB of the red channel, the second in green and the third data bit stores in the blue value, the alpha value doesn't store and the next colors used will be red again. This is because the alpha is 255, which is the same transparency levels any change can be effect in it [7, 8]. In this method, the indicator channel is computed for each block, so the channels that embed data are also changed.

3. PROPOSED ALGORITHM FOR STEGANOGRAPHY TECHNIQUE

In this approach, two color channels are selected to store data because of similarity between itself and secret message and the remaining one can be considered as an indicator channel. So, secret message is divided into several parts and each part of it is checked with blocks to find out the most similar block to it. After that, the block's number are registered to reconstruct the message according to block's location. Each 5 bits of message is compared to specific pixel if (threshold) difference between four bits of that message and one channel is smaller than or equal to 1, then this message can be stored in this pixel. For example, if we have pixel that consist of three channel (RGB) assume the indicator channel is Red and the value of that pixel is:-

(R: - 01110111, G: - 10011001, B: - 01010101)

Sample message is (11000)

After embedding sample message, sample pixel become:-

(R: - 01110111, G: - 10011000, B: - 01010101)

The LSB of Green channel become (1), while Blue channel still the same. The threshold can be controlled, it can be increased to three (11) without effect on stego image.

4. RESULTS AND DISCUSSION

There are a lot of steganography techniques, the most common one is the LSB algorithm where the information is hidden in sequential style. leading to relatively high detection of information due to being susceptible to all 'sequential scanning' based techniques. This method solve sequential embedding problem by hiding parts of secret messages into blocks according to their similarity to those blocks. Because of the character can be represented by 5 bits, we can hide 4 bits in one data channel if the (threshold) difference between hidden data and channel is smaller than or equal to 1 and embed the last bit in another channel.

Input: - BMP image, Secret Message Output:- Stego BMP Image

Step1: - In BMP file, divide image into 8x8 blocks.

Step2: - Divide the secret message into several parts.

Step3:- Compare each part with the extracted blocks.

Step4: - Determine the similar blocks with these parts.

Step5: - Embed the block's numbers that are similar to these parts according to the sequence of secret message in cover image.

Step6: - For every determined blocks, test every pixel in the block which contains three channels. Determine the highest two similar channels to that part of secret message and make the last as indicator of that blocks.

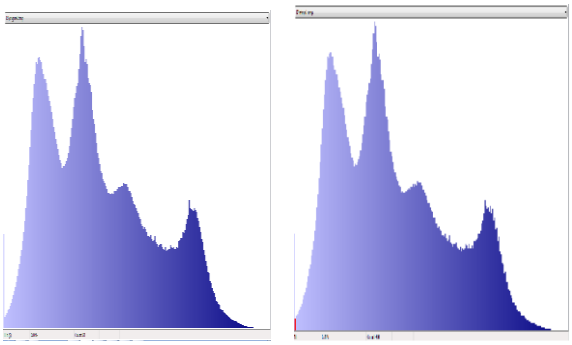
Step7: - The indicator are tested to find out the number of zeros or ones in least significant bits of each pixel per block.

Step8: - Calculate the lowest number of even zeros or ones then consider the lowest of them to indicate existing information in pixel.

Step9: - Make the first pixel from each extracted block as indicator to determine the indicator channel

Step10: - If there is information in the pixel then set the second bit in order to indicate to the channel that containing the largest number of bits (4 bits) so the other contain only one bit.

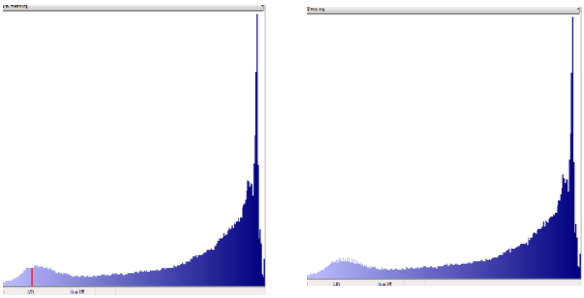
Step11: -Repeat steps from six to ten until all message are completed.



Histogram of Original Image (A)

Histogram of stego image (A) after embedding 8182 bytes

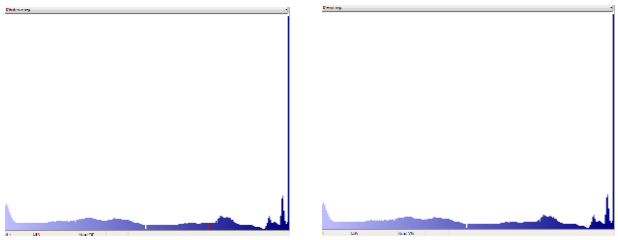
Fig. (1):- Explain histogram of original and stego image (A) to compare between them



Histogram of original image (B)

Histogram of stego image (B) after embedding 8182 Bytes

Fig. (2):- Explain histogram of original and stego image (B) to compare between them



Histogram of Original image (C)

Histogram of Stego image (C) after embedding 8182 bytes

Fig. (3):- Explain histogram of original and stego image (C) to compare between them

Fig. (1), (2) and (3) explain that the histogram of original and stego image are similar to each other which means the proposed algorithm gives high quality of stego image comparing to the original one. Peak signal to noise ratio (PSNR) and mean square error (MSE) can be used to measure that quality. Table (1) explains the impact of embedding data on the original image:-

Table (1):- Explains the mean square error and peak signal to noise ratio

Image Name	*Image Size (KB)*	*Embedded Data Size (BYTE)*	*Mean Square Error (MSE)*	*Peak Signal to Noise Ratio (DB)*
Image (A)	***230400***	***6142***	***0.047***	***61.38***
Image (A)	***230400***	***8182***	***0.06***	***60.34***
Image (A)	***230400***	***12743***	***0.09***	***58.46***
Image (A)	***230400***	***49136***	***0.315***	***53.14***
Image (B)	***396***	***8182***	***0.213***	***54.83***
Image (B)	***396***	***12743***	***0.325***	***53.00***
Image (C)	***773***	***6142***	***0.114***	***57.54***
Image (C)	***773***	***8182***	***0.139***	***56.69***

Each PSNR value in table (1) is higher than (50 db) which means it gives high quality for stego image, as well as, it is really difficult for attacker to extract secret message because hiding process is not in a sequential form. From table (1), it can conclude that large number of data can be embedded in image as well as no visual artifact can be observed.

5. CONCLUSION

Recently, Security plays a controlling role in computer science, the importance of security is further increased because of internet usage.

This method provides high level of security for two reasons. First, the embedded secret message in cover image is not in a sequential fashion to prevent attacker to know that there is even secret message. Second, because it depends on similarity principle it gives high quality for stego image above 50 DB. Other feature, it provides high capacity because it embedded five bits in each pixel that has similar bits to secret messages (four bit in one channel and one bit for another one).

REFERENCES

[1] Neil F. Johnson. "Steganography", Technical Report. November 1995.

[2] Victor OnomzaWaziri, PhD, AuduIsah, PhD and Abraham Ochoche," Steganography and Its Applications in Information Dessimilation on the Web Using Images as SecurityEmbeddment: A Wavelet Approach", International Journal of Computer and Information Technology, Volume 01, Issue 02, 2012.

[3] Shubhendu S. Shukla, Vijay Jaiswal, Sumeet Gupta and Anurag Singh," Steganography Technique of Sending Random Passwords on Receiver's Mobile", IOSR Journal of Computer Engineering,Volume 15, Issue 3, PP 17-25, 2013.

[4] Jameelah H.S.," Discrete Cosine Transform using in Hiding Image Technique", Al- Mustansiriyah J. Sci., Vol. 23, No 7, 2012.

[5] Mohammad TanvirParvez and Adnan Abdul-Aziz Gutub," RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, 2008.

[6] Gandharba Swain and Saroj Kumar," A Noval Approach to RGB Channel Based Image Steganography Technique", iInternational Arab Journal of E- Technology, Vol. 2, No. 4, 2012.

[7] Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur," A Dynamic RGB Intensity Based Steganography Scheme", World Academy of Science, Engineering and Technology,vol.4,2010

[8] Ravi kumar ,KavitaChoudhary and NishantDubey," An Introduction of Image Steganographic Techniques and Comparison", International Journal of Electronics and Computer Science Engineering, Volume1,No. 3,2012.