Technium Vol. 9, pp.60-65 (2023)
ISSN: 2668-778X
www.techniumscience.com

Color Pattern Steganography in Images

Dr. Hassan M.N. Mohammed Zaki

Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Nineveh
Email: hmn1973@uomosul.edu.iq

Abstract. Text steganography into images is one of the important strategies that are used to hide the transmitted secret messages via internet connections. Most of the proposed methods required mapping key to recover the hidden secret messages and implement more complex algorithms in hiding and recovering processes. The paper proposed an improved method to hide text in image cove based on the color pattern of the cover image. It based on the sequence of the new occurrence of the color. The results showed that the proposed method has high performance in hiding with extremely low PSNR(<0.002). The low differences between the original image and the stegno image provide more secured hiding that satisfied the State-of-Art. The proposed method can be used in transmitting classified and confidential messages via public internet connections.

Keywords. Steganography, Color image, Cover image, Secret message, LSB, PSNR, Color Channels.

I. INTRODUCTION

Security issues have great interest since ages and the steganography was the first methodology to secure messages. Till nowadays, the steganography had an importance role in data security. is the art of hiding information [1]. The digital images are the most perfect media to hide any secret information according to the large data that have less effects on the images. Thus, image steganography had been developed. Image Steganography can be defined as hiding different types of information inside a cover image [2]. The images rather contained three channels of colors that displayed together in a screen with red, green and blue channels. Hence, the images are a 3D array of pixels contained the values the performed the color. Hiding secret text or other types of information into these values [3].

Many studies had been presented to hide secret messages into the images. In [4], the authors presented a steganography system based on Invertible Steganography Network to hide larger images into a cover image. By which, the authors presented some solutions for both steganography and recovery of images and their large size In [5] the authors presented a steganography system that implement the stylized images in transforming secret image. The perform five stages including two stages for stylization of both secret and cover images. The system based on the quaternion exponent moment that calculated for the colors in both images in order to choose the perfect pixel to hide in. the authors

in [6] presented a steganography system based on a simple deep convolutional autoencoder that was designed to hide the secret image into a cover image with less distortion. They increase the payload of the cover image. In [7] the author presented a crypto system based on edge detection in the cover image. The edge of an object in the image consisted of three pixels that are used to embedded the secret bits of the secret message.

In this paper an enhanced steganography system that implement low programing cost with no complicated calculations. It based on the 3d color array of the image pixels. The rest of this paper includes the image steganography in sec2, the methodology of the proposed steganography system in sec3, results in sec4 and conclusions in sec5.

II. Image steganography

Image steganography is the art of hiding secret information into a digital image without any changes on its size and appearance. The image steganography aims to hide the secret message into the cover image to obtain stegno image that can be safely stored or transported via network or internet.

Image with different formats are large files those consisted of 3D array represent the pixels of the image. Each pixel required a set of three values that represent the displayed color of the pixel. Each of the three value needs one byte to be stored in[8]. The bytes of the images are used in steganography process according to the steganography algorithms or methods with discretion key that referred to the pixels and color channel that the bits of the secret key are hide in.

The lest significant bit LSB is one of the first implemented algorithms in image steganography that replaced one bit form the cover image with one bit from the secret message[9]. Later, other algorithms with other selected bit strategies had been presented to face the steganalysis methods or attacks that aims to obtain the secret message in the stegno image.

Several techniques had been implemented to add more robustness to the steganography algorithms such as chaotic, machine and deep learning etc. eben cryptography had been implemented to enhance the security of the secret messages.

IIII. PROPOSED ALGORITHM

The current study proposed a pattern steganography system based on the bins in the histogram of the cover images without any required mapping for the positions of the hidden bits. The proposed systems have two phases: firstly the hide the secret message into an image, secondly, recover the hidden secret message from the stegno image.

- Hiding phase

The hiding phase of the proposed system includes two steps. They are

Technium Vol. 9, pp.60-65 (2023)
ISSN: 2668-778X
www.techniumscience.com

Step one: preparing the location of the pixels that the bits of the secret message would be hide. Two of the three channels would be selected. The values of the selected channels would be ascending arranged without reparation like the histogram bins. Each corresponded values of a pixel used as coordinates for the position that the secret message would be hide in. the position allocated at the unselected channel of colors in the cover images. Figure 1 illustrates that.

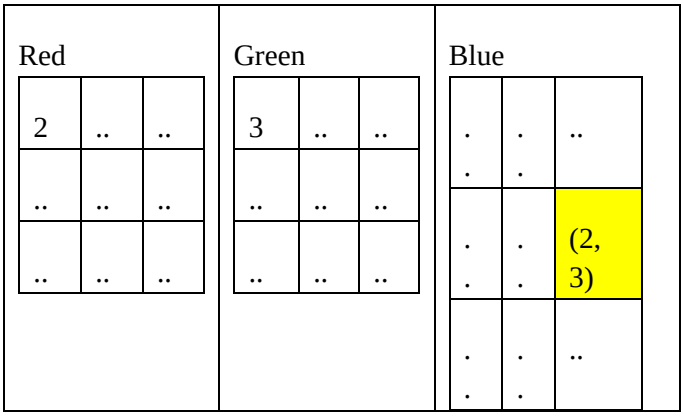

Figure 1: determine Hiding position.

The previous figure showed the position that located by the values of the red and green channel. Thus, the allocated position would be used to hide single bit of the secret message.

Step two: The secret message is converted to a string of bits. The byte of the allocated position would be converted to bits too. one bit of the cover image would be replaced with one bit of secret message for each allocated position. The replacement is based on LSB method. The number of the values in the first selected channel determine the payload of the proposed system. Thus, full colored images are used to provide more values.

Recovery

The recovery process also based on allocation of the hidden bits. The same color channel would be used to map the location of the secret bits. They would give the coordinates of the byte that the secret bit is hidden in. The collection of the hidden bits would be gathered to recover the secret message.

IV. RESULTS AND DISCUSSION

The proposed system had been implemented on a core i5 intel CPU with 8GB RAM using python ver3.8.3 programing language and Pycharm Ver2020.3.3 (Community Edition). Some images with high number of colors are used for experiments.

The selected cover images have many colors to be used in hiding the secret messages. Thus, less bits had been changed in the cover images. In fact, it depended on the numbers of ones and zeros in LSB. The following are some of the selected images in figure 2.

Figure 2: Example for the selected images.

For explaining the replacements' changes table 1 illustrate an example for a secret message with 16 characters (bytes) that produces 128-bit sequence to be hide with evaluation using peak signal to noise ratio PSNR.

Table 1: Cover Images Comparison

Img No.	Resolution	No. color	PSNR
01	311 x 194	255	0.0021
02	474 x 355	254	0.0007
03	474 x 266	255	0.0010
04	1366 x 768	255	0.00012
05	2560x 1440	255	0.000034

06	730 x 585	255	0.0003

According to table 1, the image size is very important to achieve good PSNR. The larger images are better in the proposed method. The number of differences is an important indicator because less replacement 0s by 1s or vise versa reduces the PSNR too.

In the proposed method, no need for a key mapping for the location of the secret messages. The proposed method determine the locations and perform required replacements.

V. CONCLUSION

The steganography is an essential strategy to secure data or messages. Text steganography into images is one of the methods to secure confidential texts that transmitted via internet. The proposed method hides the secret messages into high colored images with regular resolution. The achieved results showed that the proposed method had extremely low PSNR. Just little differences between the original cover images and the setgno images.

The proposed method can be used without mapping key to allocate the hidden bits of the secret message. Thus. it is easy to recover the secret message on the receiver side.

The proposed method can be more enhanced by different replacement methods. It can be used to transmit high classified and confidential messages.

1.1. References

1.2.

[1] Alabdali, N., & Alzahrani, S. An Overview of Steganography through History. International Journal of Scientific Engineering and Science, Volume 5, Issue 2, pp. 41-44..

[2] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.

[3] Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A Novel Image Steganography Method for Industrial Internet of Things Security. IEEE Transactions on Industrial Informatics, 17(11), 7743–7751. doi:10.1109/tii.2021.3053595

[4] Lu, S. P., Wang, R., Zhong, T., & Rosin, P. L. (2021). Large-capacity image steganography based on invertible neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 10816-10825).

[5] Li, Q., Wang, X., Ma, B., Wang, X., Wang, C., Xia, Z., & Shi, Y. (2021). Image steganography based on style transfer and quaternion exponent moments. Applied Soft Computing, 110, 107618. doi:10.1016/j.asoc.2021.107618.

[6] Subramanian, N., Cheheb, I., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). End-to-end image steganography using deep convolutional autoencoders. IEEE Access, 9, 135585-135593.

[7] Setiadi, D. R. I. M. (2019). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2019.12.007.

[8] Al-Taie, R. (2021). A Review Paper: Digital Image Filtering Processing. Technium Vol. 3, Issue 9 pp.1-11.

[9] Ayyed, D. (2020). Image Steganography Based Sobel Edge Detection Using FPGA. Technium Vol. 2, Issue 6 pp.23-34.