RESEARCH ARTICLE OPEN ACCESS

Capacity Performance of LSB Method On Multi-Layer Images in Steganography

Alaa Jabbar Qasim[1], Roshidi Din[2]
1,2(School of Computing,College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
Email: dralaaneen@gmail.com, roshidi@uum.edu.my)

Abstract:

To evaluate a steganographic method and cover the variation in the data, the carrying capacity of the cover data should be addressed. In relation to this, the main purpose of steganographic method is to increase the capacity and the cover to reduce variation in data. However, since the change in capacity and cover data is inversely proportional, these two purposes cannot be achieved at the same time. As such, a multi-layer steganography is used to keep the change in the cover data constant as well as to increase the capacity. In this study, a multi-layer image steganography will be discussed and compared with the non-multilayer methods.

Keywords — **LSB, Image steganography, PSNR, Security ,Data hiding.**

I. INTRODUCTION

Information hiding techniques from ancient times to the present are the techniques used. The main purpose of these techniques is to create a reliable channel for the data to be sent and transmitted. In today's digital world, many information-hiding techniques have been developed and are being developed continuously [1-3]. The most important sub-category of information hiding is steganography, one of the branches of digital media data used for protection. Scientifically, steganography is both a sub-branch of hiding information and the art of hiding information [4-8].

Meanwhile, steganalysis is defined as secret communication channels for eavesdropping and attacks to seize and analyze communication. A steganographic system is evaluated from different perspectives. These perspectives refer to how much the cover object has changed, the information storage capacity is, and how durable the system is. To evaluate the performance of a steganographic system, these three criteria must be considered. These criteria belong to steganography which is capacity, robustness, and undetectability. There are many steganographic methods available today, and the triangle above should be taken as a reference to measure the performance of these methods. Since each steganographic method follows different algorithmic methods, different analysis methods have been developed. Therefore, each method has a unique steganalysis, and it is available [9-11]. This article will talk about the multi-layer image of steganography. The main purpose is to hide data in the image and in that data with the same algorithm. Data hiding and extraction processes will be explained in detail in the following sections. Image steganography will be discussed in the second part of the paper, while in the third part, the multi-level steganography. The development of the application will be put in the fourth part, and the final part, which is the fifth, will be the conclusion and discussion.

II. IMAGE STEGANOGRAPHY

Since digital images are easy to distribute and found on almost every page on the Internet, they can be used frequently in steganographic communication. The prerequisite for applying steganography to image files is the digitization of the image [12-19]. After the pixel values are taken, which hiding function will be used is selected. After selecting the hiding function, a Steganography key should be created by obtaining information about the size, type of the data to be embedded and where it will be embedded in the cover object. The key is encrypted if desired. Then, the data to be embedded is hidden in the cover object using the hiding function and a Stego image or steganogram is created [15, 20-23]. For any steganographic system to be accepted, it

must fulfill the three basic conditions shown in the Fridrich triangle as required. These are detectability, robustness, and capacity. Detectability is detecting whether there is information in the carrier object (Stego-object). The less information is detected in a system, the more reliable the system is. The robustness condition is the criterion of how much confidential data can be transmitted to the receiving party without being corrupted on the transmission line. When the noise in the confidential data communication channel is less affected by the attacks, the more robust the system becomes.

Meanwhile, capacity refers to how much information the cover data can carry and how much information the cover data is. The media formats in which the steganography technique is most frequently applied are image formats widely used today. The most important reason for its widespread use is capacity. If it can carry it, it has that much capacity. The capacity of such a steganographic system is shown as follows, whether the steganographer has a hiding function to store one bit of information per pixel and whether the key is not embedded in the picture.

$$S = mnk \quad (1)$$

$$B=8b \quad (2)$$

$$k = \frac{S}{B} \quad (3)$$

where

S: number of pixels or how many bytes the picture consists of.
m: number of rows.
n: number of columns.
k: number of layers.

Considering that each pixel carries one byte of information, equation (1) represents the number of bytes the picture gives the information. If the picture is in RGB format, the k3 value is. If it is a Gray-level image, the k value will be 1. It is shown in equation (2) that 1 byte equals 8 bits. The capacity equation in formula (3) is obtained based on the property of the hiding function and the available information. To create a perfect steganographic system, perceptibility, robustness, and capacity criteria need to be maximized, but as the carrier's capacity increases, its perceptibility increases, and a perceptible system become unacceptable. Simultaneously, it will be difficult to talk about robustness in a steganographic system with increased capacity because the transported data will be directly affected by the losses and attacks in the transmission channel. A storage function that can use these three criteria perfectly still has not been developed, and therefore, hiding functions are tried to be evaluated by setting the acceptable criteria. Image Steganography is frequently used because the data is the best to meet these criteria, which are image data (pictures and videos).

III. MULTI-LAYER STEGANOGRAPHY

Multilayer steganographic methods have been proposed to increase the capacity and security of the carrier [24]. For example, it is aimed to increase the capacity of cover data with a carrying capacity of 10 Kb to 12 Kb. Another advantage of multi-layer steganography is that while increasing the capacity, the change in the carrier increases almost to non-existent or does not increase at all [25]. Thus, the mathematical model of multi-layer steganography can be represented as a dimension of s, k as follows.

$$s = log_{\frac{b}{a}}(MNk) \quad (4)$$

$$C = \sum_{n=1}^{s}\left(\frac{MNK}{\left(\frac{b}{a}\right)^{n}}\right) \quad (5)$$

$$C' = \frac{MNK}{\left(\frac{b}{a}\right)} \quad (6)$$

$$K = \frac{C-C'}{C'}\ 100 \quad (7)$$

$$r = \frac{C}{MNK}\ 100 \quad (8)$$

where

s: number of levels.
b: is how many bits the pixel values are expressed.
a: number of bits to be embedded in a pixel.
m: number of rows in the image.
n: number of columns.
k: number of layers.
C': capacity of the cover data in hiding using single-layer steganography.
C: is using multi-layer steganography.
K%: The capacity of the cover data in the concealment.
r: ratio of the hidden data to the cover data.

Therefore, the capacities LSB., b=8, e=1) of the multi-level steganography are shown in Table 1.

TABLE I
CAPACITIES GAINS USING MULTILAYER STEGANOGRAPHY

(LSB, B=8, A=1, 1 BPP)

Dimension $(m \times n)$	**64X64**	**256X256**	**512X512**	**1536X1536**
s	4	5	6	7
k	14.2578	14.2822	14.2853	14.2857

In Table 1, it can be seen that the gain values of the multi-layer application of the *LSB.* are given. Even with only 2-level steganography, the increase in bandwidth was 12.5%. Although multi-layer steganography is more complex, it significantly increases the capacity. One of the biggest advantages of the multi-layer image steganography method is the increase in bandwidth, in which the change in the picture remains almost the same.

The distortion rate of the pictures is calculated with *M.S.E.* (Mean Square Error) and *PSNR* (Peak Signal Noise Rate) metrics as presented in equation (9) and equation (10). A high *PSNR* indicates that the distortion in the picture is low [26].

$$MSE = \frac{1}{MN} \sum_{i,j} \left(P_{i,j} - P'_{i.j}\right)^2 \quad (9)$$

$$PSNR = 10.log \frac{Max\left(P_{i.j}^2\right)}{MSE} \quad (10)$$

Besides that, there four images have been used in this study which is *Lena*, *Nature*, *Peppers*, and *Baboon*, as shown in Figure 1

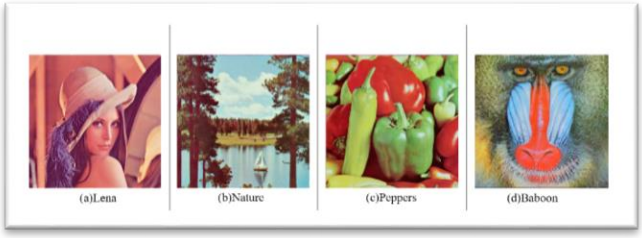

Fig. 1 Four images are applied in LSB. method used

Firstly, data was embedded in the images in Figure 3 using the classical *LSB.* Method. Then, the data was embedded using multi-layer image steganography, and its capacity (bandwidth) was increased. A two-level multi-layer image steganography structure was used, and the bandwidth was increased by 12.5%. The *PSNR* results are given in Table 2.

TABLE 2
PSNR RESULTS ARE VERY CLOSE TO EACH IMAGE USED IT.

Image	***LSB.*** **(1-layer images) (100% Capacity, 1bpp)**	***LSB*** **(2-layer images) (114% Capacity, 1.14 bpp)**	***LSB*** **(4-layer images) (114% Capacity)**
Lena	48.3568	44.8572	48.3648
Nature	48.1875	36.7469	48.1263
Peppers	48.3374	44.6697	48.3600
Baboon	48.3126	36.7448	48.3356

As shown in Table 2, *PSNR* values are quite close to one another. The average percentage change in *PSNR* was 0.059 %. This is a small and insignificant ratio. Based on the statistics shown above, the bandwidth (capacity) of data concealing accomplished using the multi-layered picture steganography method has risen without compromising the quality of the cover data. However, when the carrying capacity was enhanced using traditional techniques, the *PSNR* change amount averaged 15.6275 %. The quality of the carrier picture degraded as capacity grew using traditional approaches. Image quality and capacity have a negative connection with traditional techniques. The capacity of the image has increased by 14 percent as a result of the aforementioned application, while the *PSNR*, the quality parameter of the image, has decreased by 15 %.

IV. CONCLUSION AND DISCUSSION

In this study, the multi-layer steganography and its advantages over single-layer steganography are mentioned. In particular, it is seen as an important feature that increases the bandwidth and carrier capacity. For example, if we accept the complexity of a single-layer steganographic model as O(n), the complexity of the 2-layer implementation of the same model will appear as O(nlogn). However, as the capacity increases, the deterioration in the cover data also increases. Capacity can be increased by keeping the change in the cover data constantly by using the multi-layered method. This method can also be used especially in onion routing and multi-level security applications. In onion routing, the

carrier (onion) carries more than one message, and these messages are encrypted with various keys. The user with the relevant key can decipher the onion and obtain the relevant message. For the onion to be formed, layered steganography can be used. Thanks to the underlying data being hidden under the cover data, more than one message can be carried. In addition, this method can also be used in multi-level security applications.

ACKNOWLEDGMENT

We would like to thank the Dean, School of Computing, UUM CAS, Universiti Utara Malaysia, for their moral support to the achievement of this work. A special thanks to the School of Computing members for providing a special support to finalize this work.

. REFERENCES

1. *Hussain, M., et al., Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 2018. 65: p. 46-66.*

2. *Rasmi.A, D.M.M., HIGH DATA EMBEDDING USING LSB AND PIXEL INTENSITY BASED METHODS. International Journal of Advanced Research in Computer Science and Software Engineering, 2017. 8(7).*

3. *Rani, N. and J. Chaudhary, Text steganography techniques: A review. International Journal of Engineering Trends and Technology (IJETT), 2013. 4(7): p. 3013-3015.*

4. *Qasim, A.J., et al., Review on techniques and file formats of image compression. 2020. 9(2): p. 602–610.*

5. *Din, R., A.J.J.B.o.E.E. Qasim, and Informatics, Steganography analysis techniques applied to audio and image files. 2019. 8(4): p. 1297–1302.*

6. *Din, R., et al., Review on steganography methods in multi-media domain. 2019. 8(1.7): p. 288-292.*

7. *Roshidi Din, O.G., Alaa Jabbar Qasim, Analytical Review on Graphical Formats Used in Image Steganographic Compression. Indonesian Journal of Electrical Engineering and Computer Science, 2018. Vol 12, No 2: p. pp. 441~446.*

8. *QASSIM, A.J. and Y. SUDHAKAR, Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm. 2015.*

9. *Altaay, A.A.J.S., Shahrin Bin Zamani, Mazdak. An introduction to image steganography techniques. in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT). 2012. IEEE.*

10. *Altaay, A.A.J., S.B. Sahib, and M. Zamani. An introduction to image steganography techniques. in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT). 2012. IEEE.*

11. *Zaidan, B., et al., Stego-Image Vs Stego-Analysis System. International Journal of Computer and Electrical Engineering, 2009. 1(5): p. 572.*

12. *Sharda, S. and S. Budhiraja, Image steganography: A review. International Journal of Emerging Technology and Advanced Engineering, 2013. 3(1): p. 707-710.*

13. *C.Gayathri , V.K., Study on Image Steganography Techniques International Journal of Engineering and Technology (IJET), 2013.*

14. *Hamid, N., et al., Image steganography techniques: an overview. International Journal of Computer Science and Security (IJCSS), 2012. 6(3): p. 168-187.*

15. *Choudhary, K., Image steganography and global terrorism. International Journal of Scientific & Engineering Research, 2012. 3(4): p. 12.*

16. *Chanu, Y.J., K.M. Singh, and T. Tuithung, Image steganography and steganalysis: A survey. International Journal of Computer Applications, 2012. 52(2).*

17. *Cheddad, A., Steganoflage: A new image steganography algorithm. 2009, University of Ulster.*

18. *Kharrazi, M., H.T. Sencar, and N. Memon, Image steganography and steganalysis: Concepts and practice, in Mathematics And Computation In Imaging Science And Information Processing. 2007, World Scientific. p. 177-207.*

19. *Dhanarasi, G. and A. Prasad, Image steganography using block complexity analysis. International Journal of engineering science and technology, 2012. 4(7).*

20. *Cheddad, A., et al., Digital image steganography: Survey and analysis of current methods. Signal processing, 2010. 90(3): p. 727-752.*

21. *Raja, K., et al. A secure image steganography using LSB, DCT and compression techniques on raw images. in 2005 3rd international conference on intelligent sensing and information processing. 2005. IEEE.*

22. *Chandramouli, R., M. Kharrazi, and N. Memon. Image steganography and steganalysis: Concepts and practice. in International Workshop on Digital Watermarking. 2003. Springer.*

23. *Frączek, W., W. Mazurczyk, and K.J.J.o.U.C.S. Szczypiorski, Multi-level steganography: Improving hidden communication in networks. 2012. 18(14): p. 1967-1986.*