ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A NEW METHOD FOR REDUCING THE EFFECTS OF INCREASING INFORMATION IN DIGITAL IMAGE STEGANOGRAPHY

Nazanin Mohammadkhani Ghiasvand, Iman Beiranvand*
Department of Electrical and Computer Engineering, Eyvanekey Institute of Higher Education (Nongovernmental–Nonprofit), Semnan, Iran

ABSTRACT

Nowadays, in order to transfer data, security is one of the most important parameters in the evaluation for transmission techniques. According to the development communicational devises, possibility of data theft submissions, which should be out of reach, increased. Using images in order to store some information on them is one of the safest ways to send specific information. Considering that each image is composed of pixels, each pixel has a specific value. Added information on changes in specific areas of the image, in this case, that information may be stolen. In this paper, a new method of digital image steganography, for decreasing of changes of image and security enhancement, is presented. The propose method makes it possible to recover the data without loss of information. The results of implementation showed that after applying the proposed method, the possibility of detecting location and the value of information is very low.

KEYWORDS: Security, Digital image processing, Steganography, Hiding information.

INTRODUCTION

Nowadays, with the development of information technology in human life and more dependency on it, business data protection is crucial for a modern industry. Information is one of the most valuable assets of any organization and protection of it against others is very important. Maintaining information is necessary to continue the process of business and the economy [1-4]. For security enhancement, considering technical points is not enough, but also by creation appropriate policies, strategies and processes, also their standard, information security will be increased. For this reasons, using information security management systems are necessary [5-8]. Although, the introduction of the idea of watermarking is the year 1449 AD, but the using advanced ideas have been proposed in recent years. Besides watermarking, that its main purpose is to hide information, digital steganography has been introduced since 1990 and due to high resistance to intentional and unintentional damage, both multimedia and text, is used.

One application of steganography is watermarking with high resistance against attack. In the other words it's a combination of watermarking capability to hide the nature of the information and steganography for improve resistance of this information [9-11]. In this paper, we present a new method of digital image steganography, for reducing of increasing Information in images. In the following, after reviewing the digital image steganography methods, the proposed method and its implementation will be introduced and the results will be evaluated.

DIGITAL IMAGE STEGANOGRAPHY

If the common methods are used for steganography, with the addition of information to a specific part of the image pixels and specify the exact location of them, also send an original image with a new image to receiver, the information can be extracted. For example Fig. 1. Shows an image with 204×204 pixels that goal is the sending information via using it.

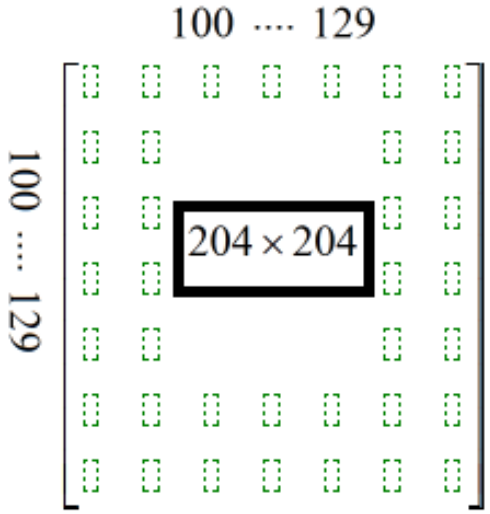
ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

Figure (1)

The information is a matrix with 30×30 dimensions, that is obtained from expansion the following matrix.

$$\begin{bmatrix}
50 & 40 & 45 & 20 & 11 & 9 & 30 & 42 & 35 & 12 \\
101 & 65 & 92 & 36 & 17 & 15 & 98 & 25 & 36 & 34 \\
25 & 15 & 26 & 59 & 27 & 48 & 75 & 86 & 51 & 52 \\
63 & 51 & 42 & 3 & 6 & 5 & 8 & 6 & 9 & 112 \\
54 & 66 & 21 & 25 & 69 & 95 & 84 & 56 & 56 & 11 \\
25 & 69 & 68 & 59 & 75 & 48 & 15 & 35 & 62 & 25 \\
110 & 45 & 78 & 98 & 65 & 32 & 12 & 45 & 95 & 68 \\
75 & 54 & 52 & 15 & 35 & 26 & 75 & 48 & 95 & 65 \\
116 & 120 & 45 & 68 & 23 & 12 & 11 & 1 & 25 & 36 \\
39 & 58 & 69 & 45 & 78 & 68 & 25 & 36 & 14 & 11
\end{bmatrix}$$

According to the following matrix, the information is located in the original image.



After addition information to original image, the image will change as shown in Fig. 2.

Figure (2)

As can be seen, the image obtained after steganography, compared to the the original, has changed a lot and caused that location of information has been specified. Therefore in this case the information can be stolen easily. In order to better comparison, this method has been implemented on two other images, which are shown in Fig. 3 and 4.

Figure (3)

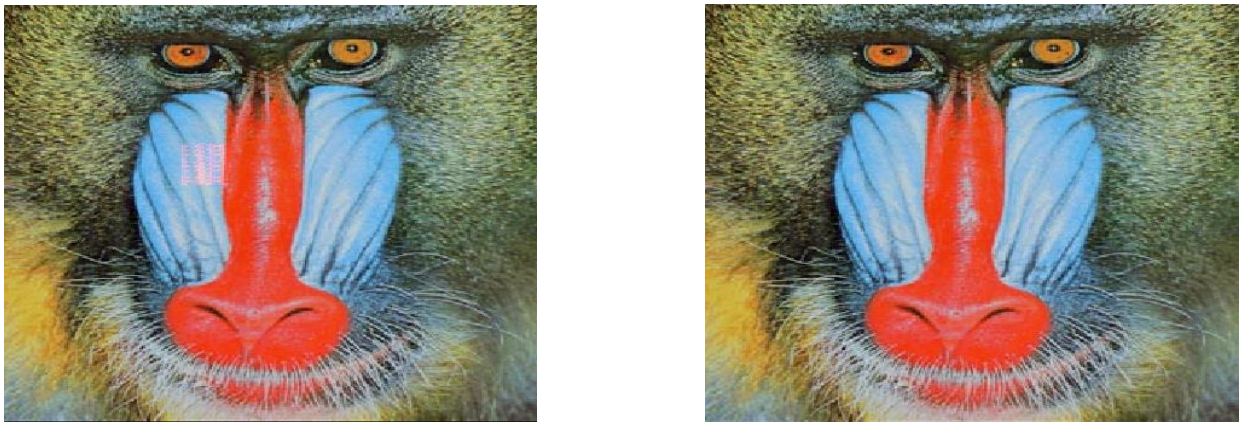
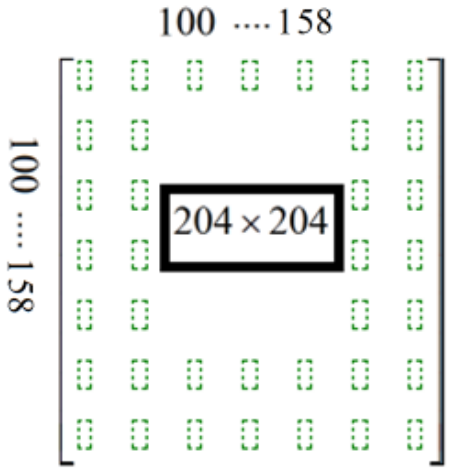


Figure (4)

As can be seen in these images, the effects of the addition of information are evident, that this effect may be less depending on the images, but does not disappear. In the following, a method with high efficiency and low computational complexity will be introduced.

PROPOSED METHOD

In the proposed method, in order to prevent theft of data that added to the image, in first step the location of information is changed, then values of information in accordance with different methods are changed, so that the original data is not deleted. For example, if the desired information is placed in pixels as following, the changes will be less.



Also, considering that incoming data can be negative or too large, the division of them on a certain value can be very useful.

RESULT AND DISCUSSION

In this section, using proposed method, the problem of the method that introduced in last section will be corrected. In Fig. 5. effect of using the proposed method on the above images is shown.

Figure (5)

As shown in Fig. 5. Location of information that added to the image and their values aren't recognizable and therefore can't be extracted by other users. Also, considering the linearity of the process, information can be recovered easily. If the target is sending information with the following ranges $\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$, sinusoidal functions can be used and in this case, assuming that the input is x, equation (1) can be used.

$$x' = \frac{x \wedge 2 + \sin(\cos(x)) + x}{100} \qquad (1)$$

As much as data are more important, the algorithms would be more complex and therefore much time and cost are needed for implementation.

CONCLUSION

Information security is one of the most important parts of the information transmission. Nowadays many techniques in order to hiding data in images are proposed. Digital image steganography is one of the best ways to send secure information, however, in the base case, due to the specified location and values of the information, it's extremely vulnerable. In this paper, a new method for enhancement of security in digital image steganography was presented. The results of implementation of this method show that location and values of information are indistinguishable and if this method is used, the information can be transmitted with high security.

REFERENCES

1. Jagetiya, A., & Krishna, C. R. (2014). Digital Image Steganography. *Cover Story What, Why and How of Software Security 7 Cover Story Developing Secure Software 9*, 23.
2. Jena, B. (2014). *High payload digital image steganography using mixed edge detection mechanism* (Doctoral dissertation).
3. Das, P., Kushwaha, S. C., & Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on* (pp. 845-849). IEEE.
4. Ghebleh, M., & Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation*, *19*(6), 1898-1907.
5. Yin, Z., & Luo, B. (2015). MDE-based image steganography with large embedding capacity. *Security and Communication Networks*.
6. Swain, G. (2014). Digital image steganography using nine-pixel differencing and modified LSB substitution. *Indian Journal of Science and Technology*, *7*(9), 1444-1450.
7. Zhou, J. M., Pan, Y., & Yang, R. E. (2014, April). DCT-Based Digital Image Steganography. In *Applied Mechanics and Materials* (Vol. 496, pp. 1986-1990).
8. Xu, S., & Lai, S. (2014, July). An Optimal Least Significant Bit Based Image Steganography Algorithm. In *Proceedings of International Conference on Internet Multimedia Computing and Service* (p. 42). ACM.
9. Bansal, S., & Dalal, S. (2014). A Study on Digital Image Steganography and Watermarking. *Biometrics and Bioinformatics*, *6*(6), 145-148.
10. Nag, A., Singh, J. P., Biswas, S., Sarkar, D., & Sarkar, P. P. (2014). A Huffman Code Based Image Steganography Technique. In *Applied Algorithms* (pp. 257-265). Springer International Publishing.
11. Singh, S., & Attri, V. K. (2015). Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm. *International Journal of Signal Processing, Image Processing & Pattern Recognition*, *8*(5).