AN INNOVATIVE METHOD FOR TEXT STEGANOGRAPHY IN IMAGES WITH GIF FORMAT

An innovative method for text steganography in images with gif format

Fazeleh Akhavan Abiri
School of mathematics and computer science,
Damghan University, Damghan, Iran.
akhavan916@gmail.com

Hassan Dana Mazraeh
School of mathematics and computer science,
Damghan University, Damghan, Iran.
dana@du.ac.ir

Resumen: En este trabajo se sugiere un método innovador basado en valores pares o impares de los elementos de matriz de imagen con formato GIF para la criptografía de texto. Los resultados de la implementación de este método para el texto de esteganografía en una imagen en formato GIF, que muestra la eficiencia e idoneidad de este método.

Palabras clave: Esteganografía, Criptografía, Imágenes Gif innovadoras.

Abstract: In this paper, an innovative method based on odd or even the values of the elements of image matrix with GIF format is suggested for the text cryptography. The results of the implementation of this method for steganography text on an image in GIF format, which shows the efficiency and suitability of this method.

Keywords: Steganography, Cryptography, Innovative, Gif images.

Citar, estilo APA: Akhavan F & Mazraeh H (2017). An innovative method for text steganography in images with gif format. Revista QUID (Special Issue). 1931-1935.

1. INTRODUCTION

Today, the growth of the Internet as One of the main factors in information and communication technology has grown dramatically, and information and communication security is essential. One of the ways to increase the security of communications is cryptography. The cryptography is a technique for securing and confidentiality of communications. The purpose of the encryption is confidentiality. Given that produced the hidden message of a code is the result of applying cryptographic algorithms. This code contains a message that usually requires a shared key between the sender and receiver to decrypt it. Another technique is to increase the safety of steganography.

Steganography is the art and science of invisible communication of messages. This is done by hiding information in other information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing".(Singh, 2014) In steganography using the image, the secret message is embedded inside the image that the visual quality of the image is not reduced and the message is sent to the end user. We see samples of another file. In some cases, even obvious of a hidden communication is problematic. In such cases, even this secret relationship should be kept secret. In such cases, steganography techniques can be used. That's mean first, encode the message and then steganography it. For example: if someone accesses the encrypted text, they will find that the text contains encrypted messages and will try to decode it. But in steganography, third person's (other person) does not at all know the secret message in the text. When the presence of information is hidden, visible or even suspicious, steganography has failed. Therefore, the power of steganography can be enhanced by combining it with cryptography.

Today steganography is mainly done on computers with digital data that carries waves and uses inside of network communication channels.

steganography in common currency, government documents, stamps and decryption documents or transmission of information.

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the destination the slave shaved hair Hidden message was read. (Morkel et al, 2000)

The other method used by ancient Greeks was writing the message under wax. In the past, they wrote letters on plaques that was plated wax. They wrote a text message on the stick then plated wax it. (Bandyopadhyay et al, 2000)

Steganography and cryptography are used to hide the message from unwanted reading. Of course, these are differences together. Cryptography focuses on hiding the contents of a message but in the steganography, the purpose is to hide any indication of the existence of a message inside
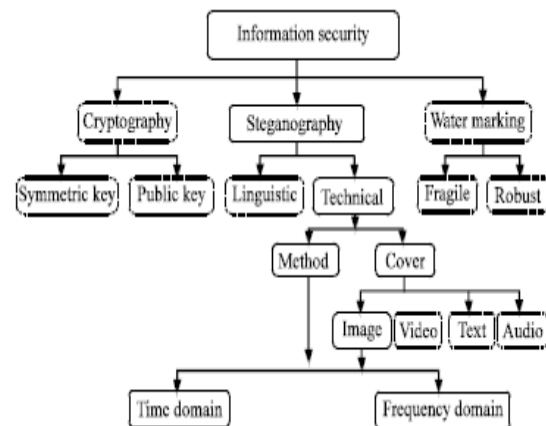

Figure 1. The status of steganography in information security

1.1 Related Works

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. The LSB based image steganography embeds the secret inthe least significant bits of pixel values of the cover image(Kavitha et al, 2012). In (Liu , 2012) a system of mixing art image generation and information concealing reinforcing the disguise sway for various information hiding applications is anticipated. In (K. Xu et al , 2009) investigate the utilization of salient curves in synthesizing intuitive, shape revealing textures on surfaces, shape-revealing

compositions on surfaces. In (Otori and Kuriyama , 2007) proposes another kind of picture coding strategy utilizing surface image synthesis. Frequently arranged dotted-pattern is initially painted with colors selected from a texture sample, for having highlights relating to inserted information. In (Cheng and Wang , 2006) gift a high-capacity steganographic approach for three-dimensional (3D) two-dimensional figure meshes. They beginning utilize the delineation information of a 3D model to engraft messages. Their methodology with achievement joins each the abstraction domain and the illustration domain for steganography. In (Provos and

Honeyman , 2003) three totally diverse aspects in information hiding system encounter with each other: capacity, security, and quality(Patil , 2017).

The main purpose of this paper is to Offers a text steganography method using GIF images.

discuss the achievements of this paper.

2. GIF FORMAT

The Graphics Interchange Format (better known by its acronym GIF) is a bitmap image format that was developed by US-based software writer Steve Wilhite and has since come into widespread usage on the World Wide Web due to its wide support and portability.

The format supports up to 8 bits per pixel for each image. In this format used a color table with 256 elements. The amount of each byte or pixel refers to one of the elements in this table. For example, for storing an image 100×100 pixel a 100×100 matrix is created with 8-bit elements, each of which based on its value, refers to a color from the color table. It also supports animations and allows you to paint a color table of up to 256 colors for each frame. This limits the color table, gif format is for reproduction color photographs and other images with continuous color suited, also it is suitable for simple illustrations such as graphics or logos with uniform color schemes.

GIF images are compressed using the Lempel–Ziv–Welch (LZW) lossless data compression technique to reduce the file size without degrading the visual quality. This compression technique was patented in 1985.

3. OUR INNOVATIVE METHOD FOR STEGANOGRAPHY IN IMAGES WITH GIF FORMAT

In this method, the concept of odd or even of the entries of the matrices of the GIF images plays main role. To embed bits of the secret message in the cover image, we assume the matrices of the GIF images as a string of pairs of integer numbers. In continue, we give specific meaning to the pairs based on being odd or even of their values as following table.

Table 1. Meaning of the string of the pairs

The first entry of the pairs	The second entry of the pairs	The meaning
Even	Even	0
Even	Odd	1
Odd	Even	1
Odd	Odd	0

To do steganography based on Table 1, we act as follows:

• If the bit of the secret message is 0 and the entries of the corresponding pair are (Even, Even) or (Odd,

So in section 2 we will introduce GIF images. In section 3 we propose a method for the text cached inside GIF images, and in Section 4, we describe the experimental results, and finally, in Section 5, we will

Odd), then we don't change the values of the entries of that pair. On the other hand, if the entries of corresponding pair are (Even, Odd) or (Odd, Even), then we convert them to (Even, Even) or (Odd, Odd) by adding or subtracting one unit to the first entry of the corresponding pair.

• If the bit of the secret message is 1 and the entries of the corresponding pair are (Even, Odd) or (Odd, Even), then we don't change the values of the entries of that pair. On the other hand, if the entries of corresponding pair are (Odd, Odd) or (Even, Even), then we convert them to (Even, Odd) or (Odd, Even) by adding or subtracting one unit to the first entry of the corresponding pair.

The procedure of our method is as follows:

Step1. Obtain the ASCII code of secrete message.

Step2. Obtain the matrix of the cover message.

Step3. Consider the elements of the matrix as a string of integer pairs.

Step4. Apply Table 1 on the matrix of Step 3.

4. EXPERIMENTAL RESULTS

To show utility and capability of our method, we consider an example as follows:

Example 1. Assume the secret message is "Hello" and the cover message is Figure 2. At first step we obtain the ASCII code of the secret message is as Table 2.
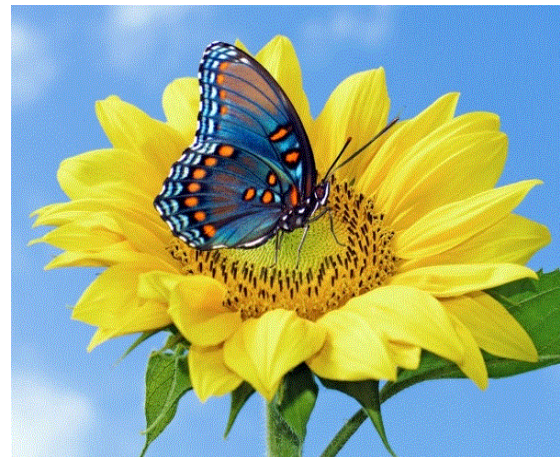

Figure 2. Cover message of the first example

Characters of secret message	ASCII code
H	01001000
e	01100101
l	01101100
l	01101100
o	01101111

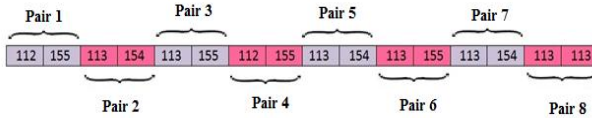In this example, 16 entries of the first rows of the matrix of the Figure 2 is as follows

Figure 3. 16 entries of the first rows of the matrice of the cover message

The first bit of the first character of the secret message is 0 and the first pair of the Figure 3 is (Even, Odd). Therefore, according to presented method in this paper, we change the first bit of the first pair of the Figure 3 from 112 to 111. In continue, we apply presented method on remaining bits of the first character of the secret message. Finally, we obtain following vector
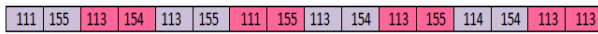

Figure 4. The obtained vector from applying presented method on first character of the secret message on first row of the matrix of the cover message

Left side of Figure 5 shows the original cover message and the right side shows the covers message after applying presented steganography method.
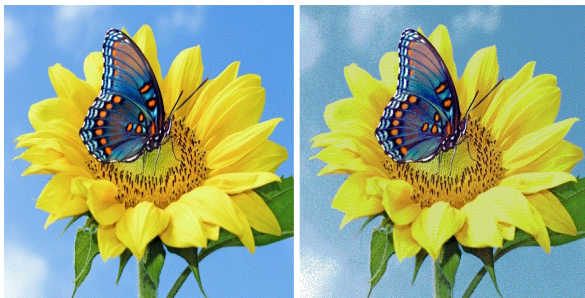

Figure.5. Left image is original cover message and right image is applied presented method cover message

Example 2. Assume the secret message is "I am fine." and the cover message is Figure 6. After applying steps of presented method we have Figure 7.
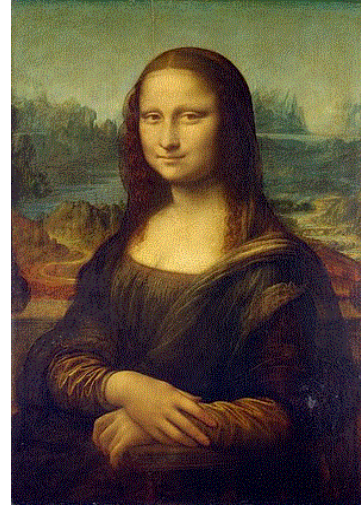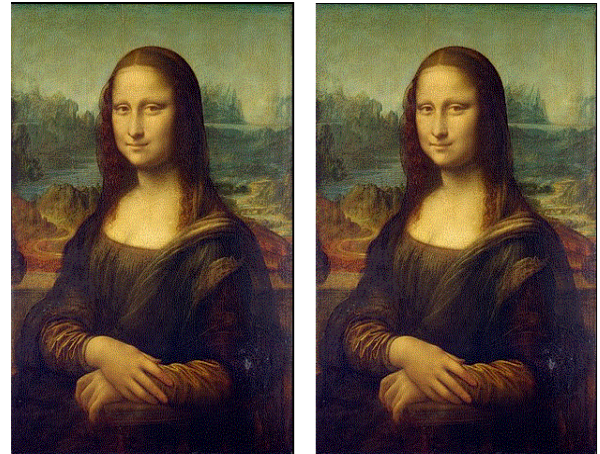

Figure 6. Cover message of the second example

Figure 7. Left image is original cover message and right image is applied presented method cover message

5. DISCUSSION AND CONCLUSION

In this article, a steganography method based on odd or even GIF image in image matrix elements was presented. The results show that this method can be combined with cryptography methods to encrypt the main text giving an efficient method. In the presented method in this paper, we tried to save the main massage in the element mass with minimum variation. The quality of the main image has not been changed significantly. The capacity of its steganography is also in a high level since all of the main image matrix elements can be used. The hidden massage could be encrypted with one of the symmetric encryption methods to put the hidden massage in the image before applying this method. It causes the steganography enhances.

REFERENCES

Aishwarya P, Snehal S, Chandni S, Kalyani P, S. N. Bhosale, B. E Students (2017), *Survey on Recent Steganography Approaches*, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 1, January.

Bandyopadhyay, S. K., Bhattacharyya, D. (2008), Ganguly, D., Mukherjee,S. and Das, P, *A Tutorial Review on Steganography*, University of Calcutta.

Cheng Y.-M. and Wang C.-M.(2006), *A high-capacity steganographic approach for 3D polygonal meshes*," Vis. Comput., vol. 22, nos. 9-11, pp. 845-855.

K. Xu et al. (2009). *Feature-aligned shape texturing,* ACM Trans. Graph., vol. 28, no. 5, 2009, Art. ID 108.

Morkel, T., Eloff, J. H. P. and Olivier, M. S. (2000), *An overview of image steganography*, Information and Computer Security Architecture (ICSA) Research Group, in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav (2012). *Steganography Using Least Significant Bit Algorithm*, International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June.

Otori H and Kuriyama S, "Data-embeddable texture synthesis," in Proc. 8th Int. Symp. Smart Graph., Kyoto, Japan, 2007, pp. 146-157.

Provos N and Honeyman P. (2003) *Hide and seek: An introduction to steganography*, IEEE Security Privacy, vol. 1, no. 3, pp. 32-44, May/Jun.

S.-C. Liu and W.-H. Tsai. (2012). *Line-based cubism-like image A new type of art image and its application to lossless data hiding*, IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1448-1458, Oct.

Singh, K. U. (2014), *A Steganography Technique for Hiding Information in Image*, International Journal of Emerging Technologies in Computational and Applied Sciences, 8(2), March-May, 2043, pp. 134-137.