Steganography

1 st Abdelrahman Radwan School of Engineering and Applied Sciences

Nile University Giza, Egypt Email: [Ab.Radwan@nu.edu.eg](mailto:Ab.Radwan@nu.edu.eg)

2 nd Adel Saeed Saad

School of Engineering and Applied Sciences

Nile University Giza, Egypt Email: Ad.Saeed@nu.edu.eg

4 th Mohamed Khaled

School of Engineering and Applied Sciences

Nile University Giza, Egypt Email:mo.abdelwahab@nu.edu.eg

3 rd Hesham Mamdouh

School of Engineering and Applied Sciences

Nile University Giza, Egypt

Email:Hes.Mamdouh@nu.edu.eg

# ***Abstract* - TO HIDE OR PROTECT DATA, STEGANOGRAPHY IS AN ADDITIONAL STEP THAT CAN BE USED ALONG WITH ENCRYPTION. STEGANOGRAPHY AIMS TO CONCEAL AND DECEIVE. IT IS THE ART AND SCIENCE OF DISCREET COMMUNICATIONS. IT IS A TECHNIQUE WHEREBY WE PLACE A SECRET MESSAGE INSIDE (OR EVEN ON TOP OF) SOMETHING THAT IS NOT SECRET. THIS THING CAN SIMPLY BE INSIDE THE IMAGE OF ANOTHER FILE OR VIDEO, AND THE SAME APPLIES TO THE MESSAGE TO BE HIDDEN, AS THIS MESSAGE CAN BE AN IMAGE, TEXT, OR EVEN A WORD OR EXCEL DOCUMENT.**

**There are many techniques that can be used to hide information, such as (audio,** **VIDEO, Network, Linguistics, and the most well-known type of schematic diagram that our research will focus on is the image). in the image to hide it, but it has evolved so that the message content can be hidden in the pixels in the image. picture. Following the LSP method is based on converting the message to (0-1). This will be explained in more detail in the upcoming topics**

# INTRODUCTION

Humans always love the privacy and prefer to keep secrets for themselves or specific people, so he has always been keen to transmit this information in a correct way that ensures that this information is not violated by unwanted people and at the same time ensures that it arrives correctly at the desired destination. Today's security-conscious environment is a place Ideal for experimenting with new techniques to hide sensitive information, as we do not want the information to fall into the wrong hands.

Humans began to develop techniques to hide messages from time immemorial, where he started with some simple symbols and developed them, and then here we are in the era of technology and with the presence of digitization of information, a lot of data is subject to attack, so several methods of encryption and data concealment appeared, and among these methods Steganography. Steganography It is a technique of hiding sensitive information inside an ordinary, unclassified file or message, so that it is detected only at its destination, thus avoiding detection. This information can be text, an image, etc., and the same applies to the file in which the information will be hidden. The word Steganography is divided into the root of the word "steganos" a Greek word meaning "hidden", and the word "graph" is also a Greek word meaning "writing".

Steganography should not be confused with cryptography, where we transform the message to hide its meaning from someone who intercepts it. This protection is often not sufficient, unlike Cryptography where the message is completely encrypted and then can be transmitted [1]. In the following table, the difference is explained in detail [2]

Table 1 Difference between Steganography and Cryptography

|  |  |  |
| --- | --- | --- |
| Factors | Steganography | Cryptography |
| Data visibility | No | Yes |
| Type | refers to Cover Writing. | refers to Secret Writing. |
| Integrity | The structure of the data remains the same. | The structure of data can be altered. |
| Attack | Attack in Steganography is termed Steganalysis. | Attack in Cryptography is termed Cryptanalysis. |
| Security Principles | supports Confidentiality and Authentication. | supports Confidentiality, Authentication, Data Integrity, and Nonrepudiation. |

There are many types of Steganography, and each type differs in the techniques that are used to hide data, which will be explained in detail, and examples of these types are text, audio, video, protocol, and image Steganography

# LITERATURE REVIEW

The author of [7] explains how Improvements to Traditional Steganography were done, as the traditional method relies on converting the information to be hidden into bits and then storing it in image pixels, and this method is called LSB. But there are two main problems with this image in which the data was hidden:

1. An attacker can concentrate on the statistics of the LSB
2. In paletted images, forcing the LSB to the desired value may result in sub- - stantial color shifts, depending on the ordering of the palette.

In non-plate images, the risk is reduced when using the LSB method by increasing or decreasing the original value (with care for overflow and underflow), or by forcing the LSB to ensure one of the two closest possible values since it is known that any Something stored inside the computer is stored in the binary system, and the matter also depends on the pixels, as they have three colors, and these colors are stored in the form (1-0). If we want to store the data to be hidden in the image, the data will be converted to (1-0) and each bit will be stored in the closest possible two values to the binary value of the pixel. So, this is what the author[9] covered in his article, where he wanted to hide the number 200 in three pixels, showing their values:.

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 1010110**0** 01100011)

The engineer, Savitha Bhallamudi, used the same method used in [9], but this time she used it to hide an image inside another image[6], but some problems appeared that Ron Crandall talked about in [7], which lies in the fact that if LSB is used on light-colored images, they can be easily detected

In contrast to these, the Taliban hid the text of the abbreviation using the language of invented text messages.

This project was done using J2ME programming language (Java 2 Micro Edition) and tested on a Nokia N71 mobile phone they used the text steganography method, as they mentioned earlier in their article [5].

SMS is a combination of the terms used in SMS but it is abbreviated. These terms can also be used in abbreviations for text masking. Recognized words and phrases in SMS shortening forms for this use. These words could be common nouns such as University, which is abbreviated as Univ, or they could be words from a list of words used in SMS, such as "you" which is abbreviated as "u". Information is hidden in the text, as above, through the use of whole or abbreviated forms of words or phrases. Inverse operations are used to extract information. With this technique, the use of SMS terms not only attract attention but also has a larger selection of words to choose from because, in addition to the standard abbreviations, short sentences for SMS are also used.

And also prepare a program in the same Java language to extract these abbreviations, and if the program notices more than one abbreviation in the same word or sentence, the abbreviations will be separated by a comma (,).

# METHODOLOGY

In this section of the paper, all the steps of the methodology will be discussed in detail including LSB and the method that the code will follow in order to hide the images

### LSB ( Least Significant Bit )

Each image contains pixels, and each pixel carries three colors, and each color contains 8 bits, and as we know that whenever we move in the binary number system from right to left, the value of the number increases, as shown in the image below ***figure 1.***

***Diagram

Description automatically generated***

***Figure 1: Binary system***

The same applies to the colors in the pixel (RGB), as the actual value of the color is found in (MSP), so if we want to hide an image in another image or anything else inside an image, it will be converted to the binary system and store this value in the (LSB), for example, the first four bits as maximum.

### Steps for hiding message image:

In the beginning, we must pay attention to a very important condition, which is the size of the images. It is obvious that you will choose the image of the smallest size to be (the Message) that you want to hide in the image of the largest size (Cover Image) in order to ensure that the image disappears when the bits are distributed.

1) Noise is added to the Cover image to make it easier to disguise

2) Separate the bit planes of each image (Cover & Message)

As mentioned before, the MSB (most significant bit) plane contains most of the shape and color information of an image. It is generally ideal to replace up to 4 least bitplanes of the cover image, with the upper 4 bitplanes without revealing changes in the resultant image [6]

3) Replace the least 4 bitplanes of the cover image with the 4 most significant bitplanes from

4) Get the resultant Steganographic image

# RESULTS and DISCUSSION

# In the beginning, we start by defining the image that will be (Cover) and the other will be (Message), taking into account the size, as the cover image must be larger than the message in order to hide it, and this is shown in figures 2 and 3, where ***figure2*** represents the cover and ***figure3*** the message



***Figure 2 : Cover Image***

A butterfly on a flower

Description automatically generated

***Figure 3: Message Image***

The images will be stripped of their colors in order to obtain black and white images with the addition of noise to the cover Images, as shown in ***figures 4 and 5***. There are two main reasons for converting images to black and white, the first reason is that by reducing the number of colors in the image, there is less information present in the cover image, which makes it difficult to detect the presence of a hidden message, and the second reason is to reduce the size of the images, which will contribute to the non-occurrence of Doubt about the size of the image, as the steganographic image is larger than other images that are equal to it in the same dimensions.

The reason why noise is added to the cover image is to make the encrypted message less clear and to reduce the possibility of detecting the message. Also, the changes made to the cover image to encrypt the message are less clear and blend with the noise.

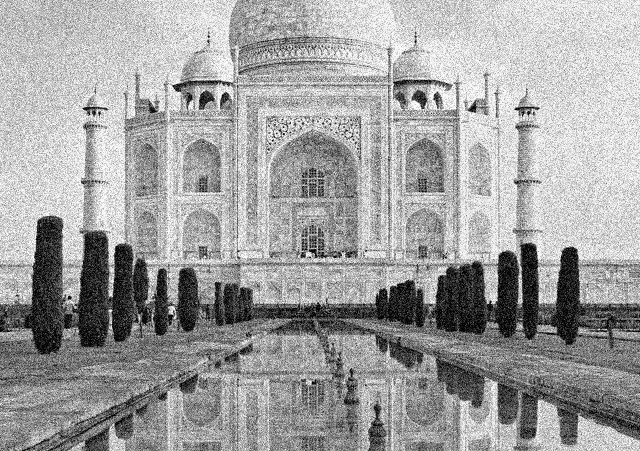


***Figure 4: Cover Image After stripping the colors and adding noise***



***Figure 5: Message Image After stripping the colors***

After stripping the colors and adding noise, we will take the first four bits (MSB) of the image message in order to preserve as much information as possible about the image and store it in the (LSB) of the cover image so that we do not change the content of the cover image significantly, then we get the Steganographic image as shown in ***figure 6.***



***Figure 6: Steganographic Image***

To extract the hidden image, we apply (for Loop) to the (LSP) of the steganographic image (the last 4 bits on the right) and convert them to (MSP), so we get the image as shown in ***figure 7***.



***Figure 7: Message Image After extraction***

# CONCLUSION

Image steganography is a technique used to hide a message within an image file. This method has gained popularity and can be an effective way to transfer information securely, and there are many different ways to implement this process, the most famous of which was the (LSP), but it is important to remember that it is not completely guaranteed and can be discovered with a few observations, for example of a hidden image of it A larger storage size than a normal image with the same dimensions, where the size of a Steganographic image can reach several megabytes, unlike regular images that may reach kilobytes, and the same applies to the rest of the steganography types.

# APPENDIX

In this link, there are all of the images used, as well as the Code for converting images to steganographic, in addition to the Code for extracting the hidden image

[ <https://drive.google.com/drive/folders/1OKE--hRXYn7J_vSbXaJGjTm5DUwN42jm?usp=sharing> ]

REFERENCES

[1] Simplilearn, “What is steganography? A complete guide with types &amp; examples,” Simplilearn.com, 18-Nov-2022. [Online]. Available: https://www.simplilearn.com/what-is-steganography-article. [Accessed: 30-Nov-2022].

[2] K. Panigrahi, “Difference between steganography and Cryptography,” Tutorials Point. [Online]. Available: https://www.tutorialspoint.com/difference-between-steganography-and-cryptography.

[3] N. Provos and P. Honeyman. (2003, Jun.). “Hide and seek: An introduction to steganography.” IEEE Security and Privacy Journal. [On line], 1(3), pp. 32-44. Available: http://niels.xtdnet.nl/papers/practical.pdf [Jul., 2011].

[4] J. Qin, Y. Luo, X. Xiang, Y. Tan and H. Huang, "Coverless Image Steganography: A Survey," in IEEE Access, vol. 7, pp. 171372-171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[5] M. Shirali-Shahreza and M. H. Shirali-Shahreza, "Text Steganography in SMS," 2007 International Conference on Convergence Information Technology (ICCIT 2007), 2007, pp. 2260-2265, doi: 10.1109/ICCIT.2007.100.

[6] S. Bhallamudi, “(PDF) image steganography - researchgate,” 01-Dec-2015. [Online]. Available: https://www.researchgate.net/publication/314116270\_Image\_Steganography. [Accessed: 30-Nov-2022].

[7] R. Crandall, “Some notes on Steganography - Binghamton University,” Some Notes on Steganography, 18-Dec-1998. [Online]. Available: http://dde.binghamton.edu/download/Crandall\_matrix.pdf.

[8] A. Swathi, “[PDF] video steganography by LSB substitution using different polynomial equations: Semantic scholar,” undefined, 01-Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/Video-Steganography-by-LSB-Substitution-Using-Swathi/86f30a65533748f9278e882511a1fa4d349f156f. [Accessed: 30-Nov-2022].

[9] M. . Shah, “An overview of image steganography,” Proceedings of the Fifth Annual ..., 08-Jun-2014. [Online]. Available: https://www.academia.edu/2943481/An\_overview\_of\_image\_steganography. [Accessed: 30-Nov-2022].