Volume XXVI 2023
ISSUE no.2
MBNA Publishing House Constanta 2023

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

(Simple) applications of steganography for images

To cite this article: M. Rusu, M. Stoica and C. Răcuciu, Scientific Bulletin of Naval Academy, Vol. XXVI 2023, pg. 94-99.

Submitted: 24.04.2023
Revised: 05.08.2023
Accepted: 29.08.2023

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-23-I2-011

(Simple) applications of steganography for images

M.Rusu, M.Stoica, C.Răcuciu

mihaicristian.rusu@yahoo.com

Abstract. Steganography, alongside cryptography, are efficient methods for confidential information transmission. The subject of this paper will be represented by a method of communicating in secret based on steganographic techniques. In the paper's contents a steganographic solution for hiding a text in a container image will be presented, as well as the reverse operation of extracting the text from the steganographic image obtained from a direct method. The result of applying the steganographic method will be compared for different resolutions of the container images. An analysis will be able to occur through visual inspection. The paper's purpose is to highlight the capacity of integration of the stegotext correlated to the image's resolution.

1. Introduction

Information security is a domain of interest, and it's currently facing pretty serious challenges, due to the development and progress of technology, accessibility of data transmissions or information through communication channels.

Therefore, while increasingly utilized but with a vast history, steganography represents a way to transmit concealed information, without them being detected or to raise suspicion.

Complementary, detection of files that contain information hidden through steganographic methods is called steganalysis, and it represents the countermeasure to steganography, just the way cryptanalysis is the countermeasure to cryptography.

From all multimedia file types, image files are the most commonly used in steganography and offer multiple advantages in hidden information transmission. The steganographic methods applied to images are represented either in the spatial domain, or in the frequency domain.

The schemes that are based on steganographic algorithms must fulfill a series of criteria such as imperceptibility, robustness to errors, storage capacity.

The most common method is LSB (Least Significant Bit), which implies, in its classic version, the substitution of the last bit from the image's pixels that will transport the hidden contents.

In this paper a steganographic application will be presented, which will be used to generate the steganogram and then extract the inserted hidden text enclosed in container images.

2. Steganography

The word ‘steganography’ is composed from the Greek words ‘stegos’, meaning ‘roof’ or ‘covered’, and ‘graphia’ which means writing. Steganography is the art and science of concealing information inside of other information in such a way that nobody other than the sender and receiver will know of the existence of hidden information.[1]

Steganography is closely related to cryptography in the sense that they both attempt to conceal information. Cryptography will scramble the message so that it cannot be understood, but will arouse suspicion of a potential hidden message by itself. On the other hand, steganography will conceal the

message inside of another piece of information, and as a result, will be much harder to notice at first glance, if at all. However, when both steganography and cryptography are used, the security of the hidden message will be much harder to defeat, due to both visual concealment and the encryption of the message.[3] For the general process of creating a stego-image, see Figure 1 below.

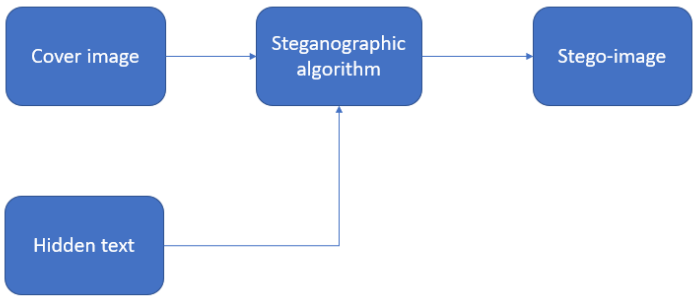

Figure 1. Diagram of the steganographic process

2.1. Requirements for steganography

A steganography tool or a scheme based on steganographic algorithms should fulfill the requirements of a steganographic system which includes but is not limited to imperceptibility, capacity, robustness and security.[2] These criteria impact the message, in terms of information capacity and detection, and are defined as follows:

- Imperceptibility – Imperceptibility is one of the main features of all steganographic methods for hiding confidential data inside a cover image, and refers to the quality of the stego-objects after embedding the information to be concealed.[2] See imperceptibility comparison between Least Significant Bit (Figure 2.1) and Most Significant Bit (Figure 2.2) of a cover image with the hidden text “The grass is green and the sky is blue”.
- Capacity – Capacity refers to the highest amount of data which can be hidden in any cover media without visual distortion. Sometimes, high embedding capacity can result in visual distortion of the stego-object, and it’s best that methods for concealing vast amounts of information should always consider examining imperceptibility as a main feature.
- Robustness – Robustness is a key component in protecting steganographic images against a wide variety of factors that can compromise the secret information inside a stego-object. These factors, like noise, compression, scaling, rotation and other methods that manipulate the cover image, negatively impact the quality of the stego-object, and almost always results in the loss of the hidden data.[2][4] All three of the aforementioned criteria have an impact on the overall quality of the stego-object. As such, the strengths of one of these requirements may become the weaknesses of another. A good tool or method for steganography will take this into consideration, and take advantage of these strengths while minimizing any weaknesses.
- Security – The resistance of stego-objects against steganalysis techniques is what is referred to as security of the steganographic technique or tool. Therefore, a secure steganographic method will ensure that the secret information will not be detectable by any means, as the goal is to transmit concealed data in a secure manner over an insecure transmission channel, without it being accessed by an unauthorized entity or system.[2]

Figure 2.1. Stego-image using LSB

Figure 2.2. Stego-image using MSB

2.2. Image steganography algorithms

To conceal information inside a cover image, a steganographic algorithm or method is used to hide secret data. These differ from one to another based on factors like algorithm complexity, alongside the aforementioned criteria.

Out of many techniques, a few are more well known, like spread spectrum, which spreads hidden data throughout the cover-image, decreasing the probability of detection; patchwork, a technique which adds redundancy to the hidden information and scatters it throughout the image in two areas of the image, all while maintaining robustness throughout the compression of the images; and least significant bit, which aims to completely avoid detection to the naked eye.[4]

3. Least Significant Bit

Least Significant Bit (LSB) is a simple, common way to embed information inside a cover image. As the name implies, this steganographic method uses the last bits of each pixel of the cover image to embed the desired data, therefore the resulting stego-image will seem almost unmodified, as if no modification was done to the cover image in the first place.

A 24-bit image contains pixels, which are defined by three colors: red, green and blue. A pixel is composed of a combination of the three colors, and each color contains a value ranging between 0 and 255, which is a total of 8 bits or one byte. By using this steganographic method, we can store 3 bits in each pixel, due to the fact that only the last bit of each color is changed. The advantage is that the changes are hard to detect using the human eye.[4]

For example, to store one character in a 24-bit image, using 8 bits per character, roughly 3 pixels (or 2.6 pixels) would be needed to store the character. As a result, to store a number of n characters in any 24-bit image using LSB through the 3 color channels, the cover image would need to have at least $n*(2+2/3)$ pixels.

Therefore, the least significant bit steganographic method is reliable through high capacity, robustness through relying on the color channels, and imperceptibility.

4. Results and comparisons

Below are listed, from Figure 3.1 to Figure 3.8, the visual comparisons between stego-images using variations of the LSB steganographic algorithm, which change the bit the hidden text is encoded to, on the cover image. Bit 0 is referred to as the least significant bit, and bit 7, the most significant bit.

Figure 3.1. Bit 0

Figure 3.2. Bit 1

Figure 3.3. Bit 2

Figure 3.4. Bit 3

Figure 3.5. Bit 4

Figure 3.6. Bit 5

Figure 3.7. Bit 6

Figure 3.8. Bit 7

4.1. Analysis

The stego-images from Figure 3.1 to Figure 3.8 are transporting the same hidden message on the same cover image, and the hidden message can be obtained with similar variations of the LSB steganographic algorithm. The imperceptibility, capacity and robustness criteria of the steganograms above will be evaluated and compared.

4.1.1. Imperceptibility. The visual impact of the algorithm's variations on the container images, affecting both its quality and 'detection rate', which would alert an unauthorized entity to the existence of hidden data inside the stego-image, is shown in Table 1 below. Detection rate and image quality, which range from 'invisible' or 'unaltered', to 'visible' or 'altered' have been quantified using values from 0 to 1.

Table 1. Detection rate and image quality degradation

Bit	Alteration rate
0	0.01
1	0.02
2	0.06
3	0.12
4	0.33
5	0.50
6	0.94
7	1.00

4.1.2. Capacity. All used variations of the LSB algorithm share the same data transmission capacity, due to all of them relying on the same method of carrying every bit on each pixel's color channels' specified bit. The higher the capacity, the more imperceptibility will be affected, as more pixels are altered for each bit of information to be concealed.

4.1.3. Robustness. All used variations of the LSB steganographic method apply the changes aforementioned in order to conceal and transmit hidden data. Despite that, the analysis found that variations where the changed bit is 'more significant' (or where the stego-image is more visually distorted) are more secure regarding attacks on the hidden data, like compression, scaling, rotation and other methods that negatively impact the quality of the stego-image. As such, the more visible the changes to the cover image (due to MSB), the more robust the stego-image is against unintentional alteration. The robustness is directly proportional to the alteration rate per 'bit significance' found in Table 1.

5. Conclusion

Steganography is a method to hide information inside of other data, and is more powerful when enhanced with cryptographic methods for further concealment of hidden information.

Good steganography algorithms and methods benefit from the upsides of criteria, like imperceptibility, capacity and robustness, which enhance the quality, size and security of the hidden message, while avoiding the downsides of the same criteria. However, most methods enjoy the benefits of some criteria while being affected by the lack of others.

For example, LSB conceals information 'in plain sight' inside a cover image, making use of high data capacity, but lacks robustness. On the other hand, MSB is visually impacting on the visual object, lacking the stealth of LSB while being very robust and the same capacity as its counterpart.

References

[1] J.R. Krenn (2004). Steganography and Steganalysis

[2] Dalal, M., & Juneja, M. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimedia Tools and Applications*, *80*(4). https://doi.org/10.1007/s11042-020-09929-9

[3] Bateman, Philip (2008). Image Steganography and Steganalysis. University of Surrey

[4] Morkel, T., Olivier, M. S., & Eloff, J. H. P. (2005). an Overview of Image Steganography. *Africa*, *83* (July).