International Annals of Science
ISSN: 2456-7132
Volume 8, Issue 1, pp. 143-149, 2020
DOI: https://doi.org/10.21467/ias.8.1.143-149

SHORT REVIEW

Steganographic Techniques Classification According to Image Format

Khaldi Amine

Computer Science Department, Faculty of Sciences and Technology, Artificial Intelligence and Information Technology Laboratory (LINATI), University of Kasdi Merbah, 30000, Ouargla

* Corresponding author email: amine.vision@live.fr

Received: 05 June 2019 / Revised: 24 October 2019 / Accepted: 28 October 2019 / Published: 04 November 2019

ABSTRACT

In this work, we present a classification of steganographic methods applicable to digital images. We also propose a classification of steganographic methods according to the type of image used. We noticed there are no methods that can be applied to all image formats. Each type of image has its characteristics and each steganographic method operates on a precise colorimetric representation. This classification provides an overview of the techniques used for the steganography of digital images

Keywords: Steganography, data hiding, digital image, Least Significant Bit, DCT, LUT.

1 Introduction

The problem of the secret data exchange has always existed. Cryptography provides an effective means of protecting secret data by making it unintelligible to unauthorized persons; however, the simple act of communicating with encrypted messages attracts attention. This can be problematic when it concerns a communication channel monitored by a third party, which can, at the slightest suspicion, destroy the communication between the two parties [1]. In these cases, a communication containing a secret message between two persons should appear normal to the person controlling the channel. For this scenario, steganography represents the alternative to cryptography. Steganography, or the science of secret communication, is a method of hiding a secret message within an innocuous host medium, so that the resulting medium appears to be unaffected (undetectable concealment) by inserting the secret message. The goal is to go unnoticed a message in another message. It is distinguished from cryptography, which seeks to make a message unintelligible to other than whomever it may concern [2]. The aim is to make it difficult or impossible to distinguish between an original medium and a medium modified by the insertion of a secret message. Nowadays, with the development of the Internet and the explosion of digital mediums (sounds, images, and videos) shared on the different communication networks, steganography becomes a popular practice and accessible to anyone wishing to communicate discreetly with other people. Steganography is based on the idea of security by obscurity: if no one knows that there is has a hidden file, no one will look at it or retrieve it. And with everything that goes on the Internet, and the number of attached files that people are exchanging, nobody has enough computer resources to scan all these transfers of images, sounds and other files [3]. The scientific community was particularly interested in this discipline. The researchers showed that the steganography applied to the current digital media represents a real challenge involving many disciplines: mathematics, statistics, signal processing, information theory, and game theory. Among the mediums which are very suitable for the concealment of information, we distinguish digital images. Since this type of medium is very commonly exchanged on the Internet, a great majority of the research work is devoted to it. In this paper, we are also interested in digital images as a medium cover. We will in this paper make a classification of steganographic methods and

those according to the digital image formats on which they operate. The remainder of the paper is organized as follows: In section 2 we present the steganography and these main characteristics and property. Then, in section 3 we will detail the different steganographic techniques and methods. In the fourth and last section we propose a classification of steganographic methods.

2 Steganography

Steganography (steganos Greek, cover and graphein, writing) is the art of hiding a secret message within another carrier message (text, image, sound, video ...) of an innocuous character, so that the existence of the secret is hidden from it. With cryptography, security is based on the fact that the encrypted message is incomprehensible to unauthorized persons, with steganography, security is based on the fact that the presence of a secret message will probably not be suspected and detected. Inserting a message into the chosen file involves changing parts of his code. The whole art of steganography is to make sure that these changes are invisible or inaudible [4]. The smaller the message and the larger file, the more this alteration is likely to go unnoticed.

2.1 Steganography Characteristics

The goals of information concealment can change in a subtle way [5]. Classically, applications are sorted according to three criteria:

- Robustness ensures that secret information cannot be destroyed without severely degrading the image. It quantifies the resistance of the concealed message to the various attacks (transformations) made to the stego-medium.
- The invisibility aims to ensure that the stego-image is not disturbed by the inserted secret information.
- The insertion capacity of a steganography system is defined by the size in bits of the secret message which can be integrated into a medium of given size. The relative insertion capacity is the ratio between the size of the secret message to be concealed and the size of the medium used. Capacity therefore defines the amount of information that can be integrated into the medium without visible deterioration.

These three characteristics are closely related and inverse (Figure 1). For example, capacity improvement generally has a negative influence on invisibility

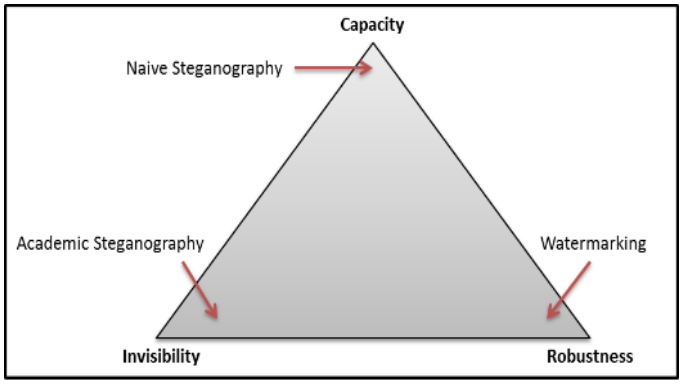

Figure 1: *Steganography characteristics*

2.2 Steganography protocols

Pure steganography: no prior agreement, other than choice of algorithm is necessary, A and B use the channel to exchange information [6] (Figure 2).

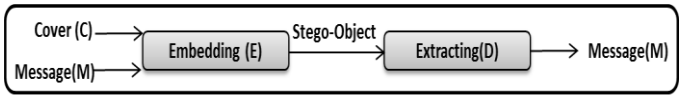

Figure 2: *Pure steganography process*

Steganography with secret key: A and B agree beforehand of a key used to insert and then extract the message of the stego-medium [7] (Figure 3).

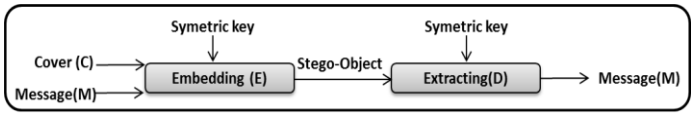

Figure 3: *Secret key steganography process*

Public key steganography: like in cryptography, A uses the public key of B when it wants to send a message to it. B extract with its private key [8] (Figure 4).

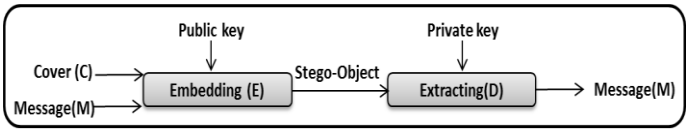

Figure 4: *Public key steganography process*

2.3 Areas of steganography

Steganography is divided into two domains, spatial and frequency. In the spatial domain, the secret message is inserted into the pixels of the carrier image, whereas in the frequency domain the pixels are transformed into coefficients, and the secret message is inserted in these coefficients [9].

Spatial domain: Spatial steganography involves changing bits of pixels in the image to insert the bits of the secret message. The LSB technique is one of the simplest and most common techniques. It consists in hiding a secret message in the least significant bits of the pixels of the image, so that the distortions brought by the insertion process remain non-perceptible. The reason is that for the human eye, variations in the value of the LSB are almost imperceptible. The insertion of secret message bits may be done sequentially or pseudo randomly.

Frequency domain: The message is inserted into the transformed coefficients of the image, which has the effect of bringing more robustness against the attacks. Frequency steganography is an essential technique for concealing secret information: nowadays most steganography systems operate in the frequency domain. The frequency steganography will thus make it possible to hide the information in areas of the image less sensitive to compression, cropping and various image processing.

2.4 Classification of Steganographic Methods (Image Format)

Before being able to establish our classification, it is essential to present the types of images chosen for our classification. We have chosen the most commonly used formats that are currently used and exchanged. Different representations of images must be distinguished. In a file, for storing and exchanging data, the image is usually compressed and stored in a graphic format. The main matrix formats are Windows bitmap (BMP), Graphics Interchange Format (GIF), Portable Network Graphics (PNG) and Joint Photographic Experts Group (JPEG). Each format has its own characteristics. To choose the one that corresponds to what we want to do with our images, it is essential to know the depth of the colors. Expressed in bits, it corresponds to the number of color values that each pixel of the image can take.

- BMP (or Bitmap) format is a universal, uncompressed format developed by Microsoft and IBM. It allows a faithful reproduction of the colors of the original image; the counterpart is the high weight of the generated file.
- Graphics Interchange Format (GIF): Also widely used in the web, this proprietary format uses an indexed color scheme. It is thus possible to use only specific color values, which makes it possible to optimize as much as possible the weight of the visual. In contrast, the appearance of visuals displaying many colors is strongly degraded. This format also allows you to create frame-by-frame animations.
- The Joint Photographic Experts Group (JPEG) format: widely used in the web, this format was developed by a panel of experts that publishes compression standards for still images. This compressed format greatly alters the quality of the original images but allows a relatively accurate color reproduction and a relatively light weight.
- Portable Network Graphics (PNG) format: This format is standardized by the World Wide Web Consortium (W3C) and is designed to bypass the existing proprietary GIF format. The PNG thus has exactly the same characteristics as the GIF, and also allows the recording from 1 to 48 bits, and the management of transparency (alpha channels). On the other hand, it is not possible to make animations.

2.5 Classification of steganographic techniques

As we can see in the figure 5, the steganographic methods can be studied in five groups: Fusion methods, Statistical modification technics, permutation, substitution and additive marking technics.

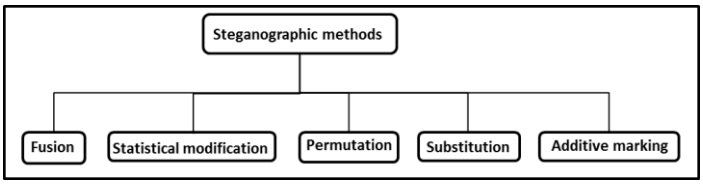

Figure 5: *Steganographic techniques classification*

Fusion: This technique, which can be considered as naive steganography [9], consists in adding the data to be hidden to the file. To do this, this method uses unused or unread slots by most image decoders. As we can see in "Figure 6" There are two operations: Adding data at the end of the file and adding to the file headers.

- The addition at the end of the file is made possible by the fact that most image decoders do not read the image file as a whole. For most available image formats, a certain bit string is set to mark the end of the image.
- The addition at the end of the image simply appends the hidden data after this string. No size limitations are imposed; however, a 20 Mbytes image file may not go unnoticed. As for adding to the header, some formats such as the bitmap define a field to specify the offset from which the image will start. By specifying a slightly longer offset it is possible to hide the data to be concealed between the two offsets.

Statistical methods: Statistical methods modify several support statistics (letter frequencies, pixel distribution) to hide the message [10] and retrieve it by testing these assumptions. In this technic, the generated mark is directly inserted into the original image. The process of detection and extraction, in this type of steganography (for blind techniques) is carried out using statistical methods. For example, a correlation measurement can be performed.

Additive Schemes: During insertion, the signal representing the mark is added to certain components of the medium. In order to do this, it is neither necessary to adapt the mark to the medium so that the signal it represents is not too low (risks of non-detectability) nor problems of robustness nor too strong (erasure of the initial signal and therefore too great degradation of it). Spectrum spreading [11] is a technique used in radio telecommunications, especially by the military, to disperse a signal over a wide frequency band to make it discreet and resistant to interference.

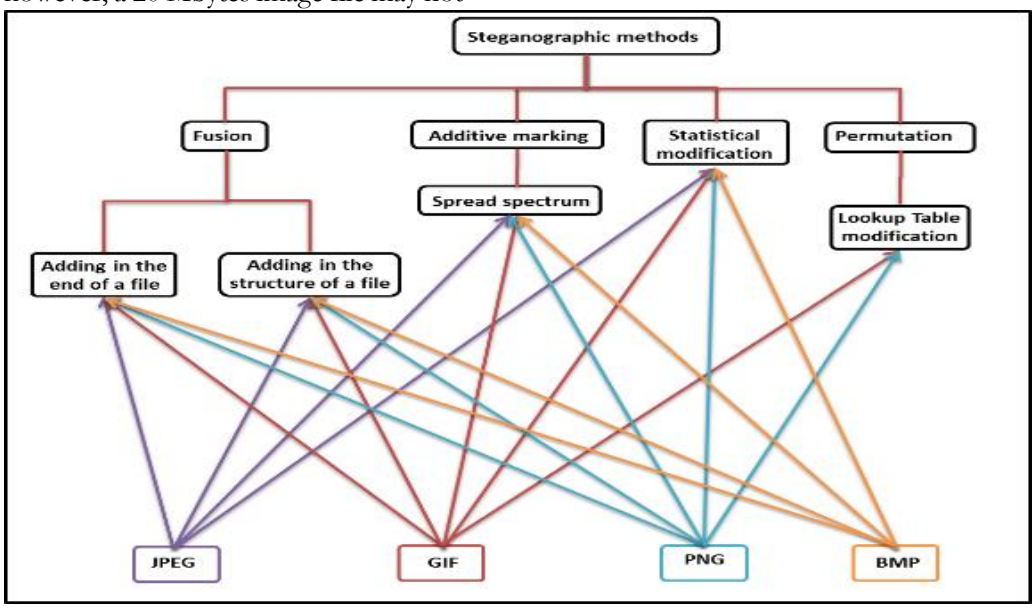

Figure 6: *Classification of steganographic techniques according to the image format*

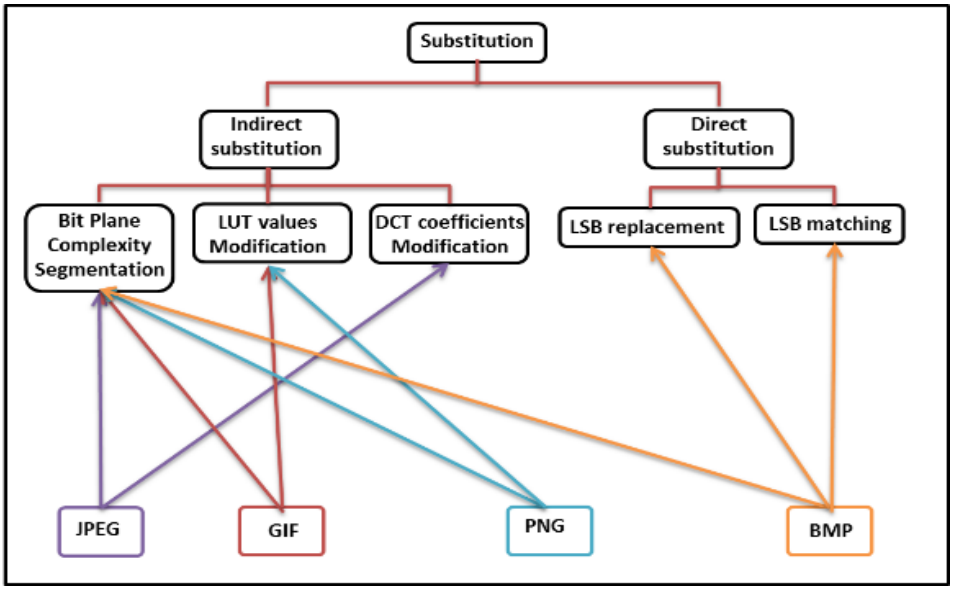

Figure 7: *Substitution technics classification*

Substitution technics: In substitution methods, the information to be hidden is not added but substituted in the components of the image (pixel, transform coefficient) selected using a secret key. As we can see in "Figure 7" substitution technics may be subdivided into two sub-categories, direct and indirect. In the direct substitution the cover values are modified without any transformation process. In the indirect substitution, a transformation of the cover is made before the concealment process.

- **Bit Plane Complexity Segmentation (BPCS):** The Human visual system has such a special property that a too-complicated visual pattern cannot be perceived as "shape-informative" [12] For example, on a very flat beach shore every single square-foot area looks the same - it is just a sandy area, no shape is observed. However, if you look carefully, two same-looking areas are entirely different in their sand particle shapes. BPCS-Steganography makes use of this property. It replaces complex areas on the bit-planes of the vessel image with other complex data patterns (i.e., pieces of secret files). This replacing operation is called "embedding." No one can see any difference between the two vessel images of before and after the embedding operation.
- **Modification of DCT coefficients:** This approach consists in extracting a certain number of squares of 8 × 8 pixels from the image, calculating the DCT transform of these blocks and marking a bit on the averages frequencies, the modification of the low frequencies of the image would not change it too much. The low frequencies corresponding to the largest homogeneous areas in the image, for example uniform black in the dark areas, and the high frequencies being removed by JPEG compression, corresponding to the smallest homogeneous areas of an image [13].
- **Least Significant Bit (LSB):** LSB gathers everything related to data concealment by modifying the low-order bit of an element [14]. Modification of the value of a pixel or the modification of the value of a DCT coefficient in the case of the JPEG standard. All are based on the insensitivity of the human visual system to a small change of colors. There are two LSB methods:
  - **LSB replacement**: This technique consists in substituting the least significant bits of the pixels for the message bits to be inserted. To insert a message, the last least significant bit of each pixel is replaced by a bit of the

message to be concealed. The path direction of the pixels is usually chosen by a pseudo-random path. To do this, the transmitter and the receiver must first exchange a key k, used as the seed of a pseudo-random number generator.

- **LSB matching steganography:** Least Significant Bit (LSB) matching steganography, also named ±1 embedding, is a slightly more sophisticated version of LSB embedding. The LSB correspondence steganography method does not alter the first order statistical distribution of the host support. So All first-order statistical attacks are ineffective.

As we can see in the figure 7, a steganographic technique cannot always be applied to all image formats. It is not possible, for example, to modify the DCT coefficients of a BMP image since this format is not compressed, it is also not possible to modify the LUT in a BMP image because the colorimetric representation in a BMP image does not use Lookup table. For JPEG, PNG and GIF images, direct substitution cannot be performed as both types require processing to access pixel values (DCT for JPEG and LUT for GIFs).

3 Conclusion

The need for secret or discrete communication is not a new quest: since antiquity, human beings have always sought to protect and disguise their data with different methods. With the advent of the Internet, adapted digital methods were then put in place. In this paper, we are interested in steganography which is a secret communication process. In our work we have presented the most used steganographic techniques, we have also tried to classify these techniques according to the types of images on which they are applied. In our classification we also distinguish steganography techniques depending on the way the message is inserted into a host document, either additively known by additive techniques, or alternatively known by substitution techniques. Insertion in the spatial domain has logically been the first to be considered. But, if the methods used are quite simple, they often show their limits fairly quickly. The spatial domain has the advantage of being inexpensive in computing time, since it is not necessary to perform transformations. However, this domain does not easily handle invisibility. In addition, it is natural to think that steganography is incompatible with lossy compressions. In reality, it is much more advantageous to use the JPEG format, which is much more used and allows more discretion, even if it is done at the expense of the insertion capacity. We note in our classification that there are no methods applicable to all image formats, each format has its characteristics, this classification could be useful because it gives an overall view of the existing methods and applicable to digital images and it allows delimiting the fields of application of each technique. The extension of this work could lead to a wider classification by integrating all possible digital media (audio and video).

4 Competing Interests

The author declared that no conflict of interest exists in the publication of this work.

How to Cite this Article:

A. Khaldi, “Steganographic Techniques Classification According to Image Format”, *Int. Ann. Sci.*, vol. 8, no. 1, pp. 143-149, Nov. 2019. doi: 10.21467/ias.8.1.143-149

References

[1] S.Kaur, S.Bansal, R. K. Bansal, “Steganography and classification of image steganography techniques”, *International Conference on Computing for Sustainable Global Development*, India, 2014.

[2] A. Abd EL-Latif, B.Abd-El-Atty, E. Venegas-Andraca, “A novel image steganography technique based on quantum substitution boxes”, *Optics & Laser Technology*, Volume 116, August 2019, Pages 92-102.

[3] M.Hussain, A.Wahid Abdul Wahab, Y.Idris, S. Ho, K.Jung, “Image steganography in spatial domain: A survey”, *Signal Processing: Image Communication*, Volume 65, Pages 46-66, July 2018.

[4] K.Gaurav, U.Ghanekar, “Image steganography based on Canny edge detection, dilation operator and hybrid coding”, *Journal of Information Security and Applications*, Volume 41, August 2018, Pages 41-51.

[5] S.Kumar, A.Singh, M.Kumar, “Information hiding with adaptive steganography based on novel fuzzy edge identification”, Defense Technology, Volume 15, Issue 2, April 2019, Pages 162-169.

[6] B.Feng, W.Lu, W.Sun, “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”, *IEEE Transactions on Information Forensics and Security*, Volume 10, Issue 2, April 2015, Pages 243 - 255.

[7] S.Dagar, "Highly randomized image steganography using secret keys", *International Conference on Recent Advances and Innovations in Engineering*, India, 2014.

[8] Z.Li, Y.He, "Steganography with pixel-value differencing and modulus function based on PSO", *Journal of Information Security and Applications*, Volume 43, December 2018, Pages 47-52.

[9] A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", *Computers & Electrical Engineering*, Volume 70, August 2018, Pages 380-399.

[10] A.Shaik, V. Thanikaiselvan R.Amitharajan, "Data Security Through Data Hiding in Images: A Review", *Journal of Artificial Intelligence*, Volume 10, 2017, Pages 1-21.

[11] M.Nutzinger, C.Fabian, M.Marschalek, "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Germany, 2010.

[12] S.Bhattacharyya, A.Khan, A.Nandi, A.Dasmalakar, S.Roy, G.Sanyal, "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography", *World Congress on Information and Communication Technologies*, India, 2011.

[13] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Third International Conference on Intelligent Sensing and Information Processing, India, 2005.

[14] G.Swain, "Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function", *Optik*, Volume 180, February 2019, Pages 807-823.