Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(3):117-122**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Steganography Uses and Various Techniques using Digital Images

Muhanad Faris Saleh, Akram Abdul Maujood Dawood

Computer Engineering Department, Mosul University, Iraq
muhanadfaris.83@gmail.com , akram.dawood80@gmail.com

Abstract In recent years, the rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. The art of information hiding has received much attention in the recent years as security of information has become a big concern in this internet era. Steganography – the art and science of hiding information into the other information so that the hidden information appears to be nothing to the human eyes has gained much attention. There are many ways to hide information inside an image, audio/video, document etc. But Image Steganography has its own advantages and is most popular among the others. This paper includes the important steganography methods and the main focus is on the review of steganography in digital images steganographic techniques in spatial domain such as least significant bit (LSB), pixel value differencing (PVD). The different aspects on which the steganography method depends are: robustness, capacity, undetectability.

Keywords Steganography, Least significant bit (LSB), Pixel value differencing (PVD), Capacity, Stego-image, cover-image

1. Introduction

Over the last two decades, the rapid development of internet requires confidential information that needs to be protected from the unauthorized users. This is accomplished through Data hiding. It is a method of hiding secret messages into a cover medium so that an unintended observer will not be aware of the existence of the hidden messages. This is achieved by steganography. The term steganography is retrieved from the Greek words *stegos* means *cover* and *grafia* meaning *writing* defining it as *covered writing.*[1].

Steganography is a technology that is used to hide secret information in digital media, thus hiding the fact that secret communication is taking place. By hiding secret information in less suspicious digital media, well-known channels, for example e-mail and social networking sites, are avoided, thereby reducing the risk of information being leaked in transit.

Steganography is a technology concerned with ways of embedding a secret message in a cover message also known as a cover object in such a way that the existence of the embedded information is hidden. A secret message can be plaintext, ciphertext, an image, or anything that can be represented as a bit stream. The embedding process is sometimes parameterised by a secret key, called a stego key, and without knowledge of this key it is difficult for an unauthorised party to detect and extract the secret message. Once the cover object has information embedded in it, it is called a stego object.

Steganography equation is 'Stego-medium = Cover medium + Secret message + Stego key. Theg eneral model of data hiding can be described as follows. The embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object.

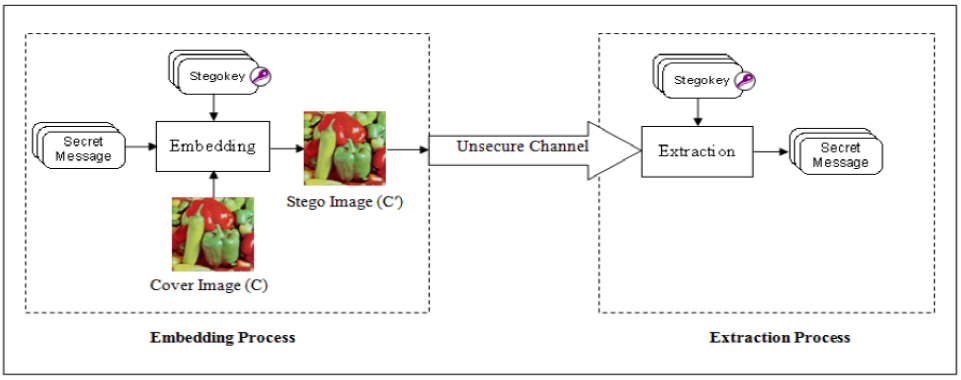

Figure 1: The General Steganography System

A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it [2]. When referring to computer-mediated communication, communication is defined as the means of sending and receiving information, specifically from one computer or device to another. In the context of this dissertation, secure communication is defined as sending and receiving information with the certainty that the information remains safe and protected against attacks.

In general, steganography is used by people who wish to communicate in secret and in complete freedom. The secrecy of the communication is especially important in censured or monitored environments.

1.1. Types of Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display without the alteration being done [3].

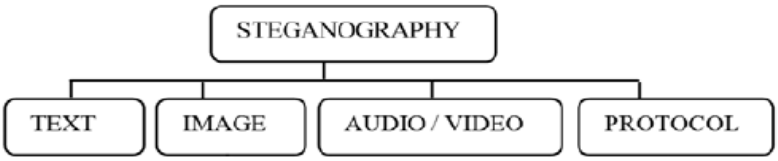

Figure 2: Types of Steganography

1.2. Classification of Steganographic Categories

Steganography is classified into 3 categories:

- Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication. This is most susceptible to interception.
- Public key steganography where a public key and a private key is used for secure communication.

2. Image Steganography Techniques

When image is used to carry the message to the receiver, then it is called image steganography. Image steganography is classified into two domains: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform Domain applies image transformation and manipulation of algorithm Image Domain applies bit insertion and noise manipulation of a covered image [1]. Spatial domains are those domains, where the secret data is embedded directly to pixels [4]. Image steganography is classified into two domains: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform Domain applies image transformation and manipulation of algorithm. Image Domain applies bit insertion and noise manipulation of a covered image. Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this

purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Grayscale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure [5].

Cover Media	Count	Percentage
Text	255	8.47%
Audio	445	14.78%
Video	86	2.86%
Images	1689	56.09%
Disk Space	416	13.82%
Network	39	1.30%
Other files	81	2.69%

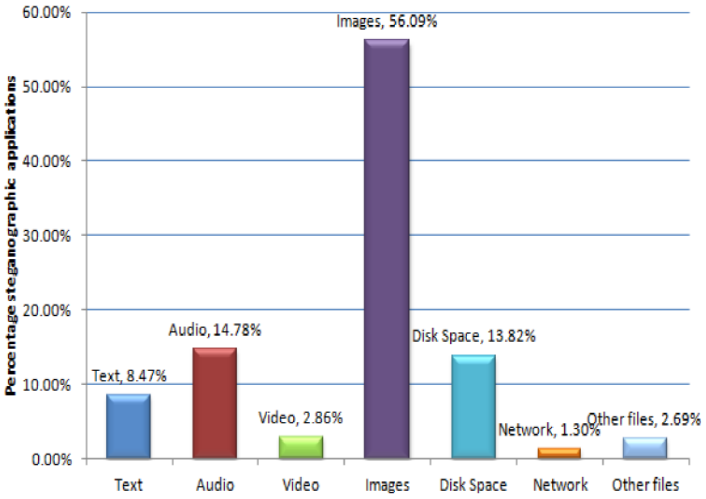

Figure 3: The number of steganographic applications that hide secret information in electronic media

The various parameters to find the efficiency of any image steganographic algorithm are:

Capacity: The hiding capacity is maximum amount of data an image can hide. It is represented in bits per byte, or bits per pixel.

Security: It is the ability to survive from different attacks. The more the security the better is the algorithm.

Invisibility – The first and foremost requirement for any steganographic algorithm is the invisibility that is the ability to be unnoticed by the human eye.

T**amper resistance**: The steganographic algorithms should be robust.

Imperceptibility: Any visual artifacts in the stego-image should not be noticeable to human eye. Peak Signal-to-Noise Ratio (PSNR), is used to find out whether the stego-image quality is acceptable or not.

2.1. Image Domain (Spatial Domain Technique)

2.1.1. Least significant bit (LSB)

Least Significant Bit Steganography is a simple way of embedding data in image. LSB technique directly embeds the secret data into the least significant bits of the pixel. Usually there are eight bit are there in a grayscale image.

Pi = (b7 b6 b5 b4 b3 b2 b1 b0)2

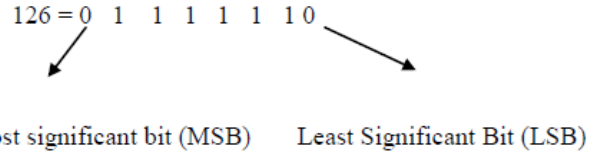

Figure 4: MSB & LSB of a pixel

If we will change the MSB bit to hide another bit, i.e. we can hide either 0 or 1. Suppose we want to hide a 0 bit, then there I no change to the pixel value but if you hide a 1 bit, then the new value becomes 11111110 i.e. 254. It means there is a change in 254-126=128 of the pixel value. This much of change to the pixel values can easily

identified to a normal eye. So data should not be inserted or embedded in the MSB of any pixel. In the other side if we embed 0 in the LSB of the pixel then there is no change to the pixel value but if you hide a 1 bit, then the new value becomes 01111111 i.e. 127,and change in only 1 to the pixel value. This small change to the pixel value will not be noticed by a normal human eye. This technique is called simple 1-LSB technique. The LSB embedding approach has become the basis of many techniques to hide secret data. LSB such as 1-LSB, 2-LSB, 3-LSB and combining LSB with other image steganographic techniques such as Pixel value differencing (PVD) [4].

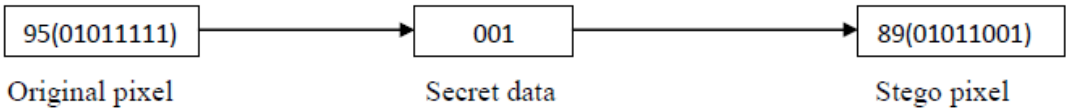

Figure 5: Simple 3-LSBs technique

2.1.2. Pixel value differencing (PVD)

The pixel-value differencing (PVD) scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Besides, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding.

In PVD method, gray scale image is used as a cover image with a long bit-stream as the secret data. At first the cover image is partitioned into non-overlapping blocks of two consecutive pixels, pi and pi+1. From each block the difference value di is calculated by subtracting pi from pi+1. The set of all difference values may range from -255 to 255. Therefore, |di | ranges from 0 to 255. The blocks with small difference value locates in smooth area where block with large difference values are the sharp edged area.

2.2. Transform Domain (Frequency Domain)

In steganography, data is embedded in the transform domain. There are different file formats available in transform domain but JPEG file format is most popular among the others. The reason is that the size of the JPEG image is very small. Transform domain is more robust when compared to the image domain [1].

Transform Domain Techniques (Discrete Cosine Transform)

The DCT technique plays a vital role in JPEG compression technique. For example, an image is split into 8X8 squares. Each square is transformed through DCT which produce 63 coefficients multi-dimensional array of outputs. Now, the coefficient is rounded by quantized value. By using the Huffman encoding schemes the further compression can be done**.**

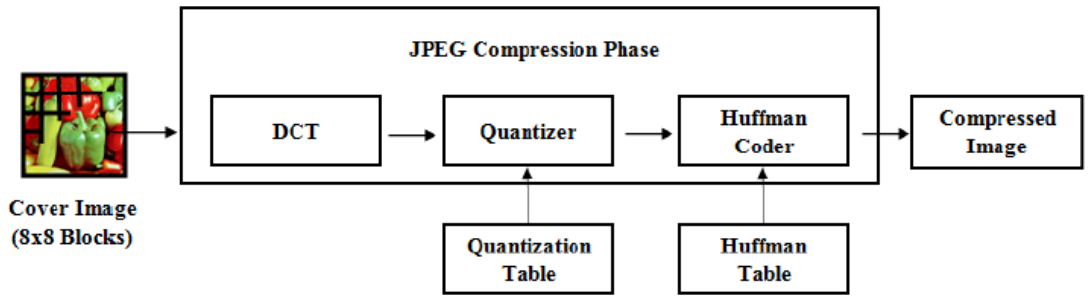

Figure 6: The JPEG image compression phase

3. Applications of Steganography

Steganographic technologies are very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the

cryptographic systems on their own and the desire to have complete secrecy in an open systems environment [6].

The Steganography can be used for wide range of applications such as The educational sector for hiding question papers or important confidential memos, In the military for hiding important operational procedures as the case may be, In the financial sector for hiding financial records and the like, In government for hiding specialized government documents and a host of other areas of application, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost, in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviors [7].

4. Classification of Steganographic Methods

Steganography methods can be classified mainly into six categories, although in some cases exact classification is not possible.

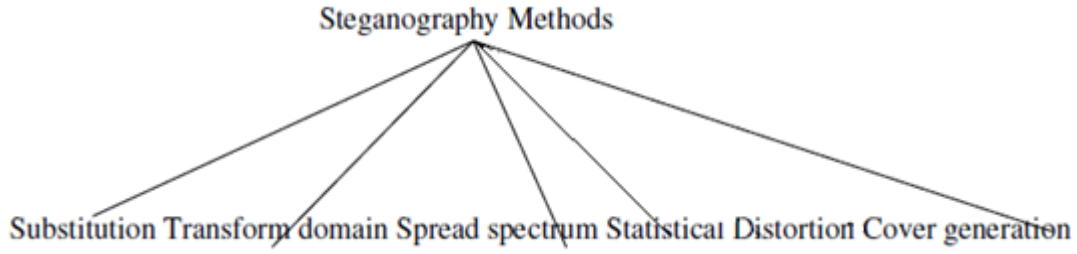

Figure 7: Classification of Steganographic Methods

- Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).
- Transform domain techniques embed secret information in a transform space of the signal (frequency domain)
- Spread spectrum techniques adopt ideas from spread spectrum communication.
- Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
- Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.

3. Evaluation Of Different Techniques

There are several parameters to measure the performance of the steganographic system:-

- **Undetectability (imperceptibility):** this parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.
- **Robustness:** it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique (out of the scope of this paper).
- **Payload capacity:** it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye.

Table 1: A comparison of Image Steganography Techniques

	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques
Imperceptibility	High*	High	High	Medium*	Low
Robustness	Low	High	Medium	Low	Low
Payload Capacity	High	Low	High	Low*	Low

4. Conclusion

This paper provides the novel approaches for implementing Digital Image Steganography, that is to conceal secret information inside an image so that it invisible to the eyes. The main image steganographic techniques to hide information were discussed in this paper in the Image Domain, LSB and PVD. Also in the Transform Domain, DCT. Each of Steganography techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and Robustness).

References

[1]. R. Poornima, R.J.I. (2013). An Overview of Digital Image. *International Journal of Computer Science & Engineering Survey*, 4(1): 23-31.

[2]. C.P. Sumathi, T. Santanam, G.U. (2013). A Study of Various Steganographic Techniques. *International Journal of Computer Science & Engineering Survey*, 4(6).

[3]. Pallavi K., Jaikaran S., Mukesh T. (2011). Digital Image Steganography. *Journal of Engineering Research and Studies*, 2(3): 101-104.

[4]. Aditya K. S., Monalisa S. (2016). Digital Image Steganography Techniques in Spatial Domain: A Study. *International Journal of Pharmacy & Technology*, 8(4): 5205-5217.

[5]. Ravi K. S., Rashmi M. T., Image Steganography Techniques. *International Journal of Computer Engineering and Sciences*, 1(2): 1-15.

[6]. Amaobi U. M., Amadi E. C., Nwokonkwo O. C. (2017). A Cost Effective Image Steganography Application for.*Management Science and Information Technology*, 2(2): 6-13.

[7]. Babloo S., Shuchi S. (2012). Steganographic Techniques of Data Hiding using Digital Images. *Defence Science Journal*, 62(1): 11-18.

[8]. Rahul J., Lokesh G., Salony P. (2013). Image Steganography. *International Journal of Advanced Research in Computer Engineering & Technology*, 2(1): 224-227.

[9]. Odai M. Al-Shatanawi, Nameer N. El. Emam, (2015). A New Image Steganography Algorithm Based. *International Journal of Network Security & its Applications*,7(2): 37-53.