P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2015, 9 (2) :80-84

New Stenographic method to hiding information in digital image

Falath M.Mohammed

University of Anbar - College of computer

ARTICLE INFO

Received: 19 / 5 /2022
Accepted: 28 / 5 /2022
Available online: 3/5/2017
DOI: 10.37652/juaps.2015.124504

Keywords:
Steganography,
Information hiding,
Least Significant Bit,
DCT.

ABSTRACT

Steganography is the art of hiding information in different cover media, then sending & displaying the hidden information especially in public places, Therefore, different methods have been proposed so far for hiding information. In this paper new method was proposed called keyboard method because it works in manner like the keyboard. It is insure that no change on image which must send to another side.

Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence [1].

The steganography can be considered as a branch of cryptography that tries to hide messages within others, avoiding the perception that there is some kind of message. To apply steganography techniques cover files of any kind can be used, although archives of image, sound or video files are the most used today. Similarly, information to hide can be anything: text, image, video, sound, etc. [2]. To a computer, an image is an array of numbers that represent light intensities at various points (pixels). These pixels make up the image's raster data. A common image size is 640 ´ 480 pixels and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data. Digital images are typically stored in either 24-bit or 8-bit files. A 24-bit image provides the most space for hiding information; however, it can be quite large (with the exception of JPEG images). All color variations for the pixels are derived from three primary colors: red, green, and blue [2]. Each primary color is represented by 1 byte; 24-bit images use 3 bytes per pixel to represent a color value. These 3 bytes can be represented as hexadecimal, decimal, and binary values. The best known steganography method that works in the spatial domain is the LSB (Least Significant Bit), which replaces the least significant bits of pixels selected to hide the information [2].

* Corresponding author at: University of Anbar - College of computer
.E-mail address:

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [3].

Background of the Problem

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered. Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [4], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [5]. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [6].

The basic model of steganography

The basic model of steganography consists of *Carrier*, *Message* and *Password*. Carrier is also known as *cover-object*, which the message is embedded and

serves to hide the presence of the message. Basically, the model for steganography is shown on Figure 1. Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *stego-object.*

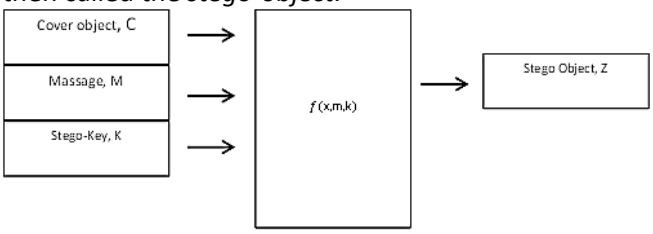

Figure 1 Basic Steganography Model

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message [9]. Modern steganography system attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes [20].

Different kinds 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 [7]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [6]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography

Text steganography

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message[9]. Alternately, hidden (e.g., control) characters, and redundant use of markup (e.g., empty bold, underline or italics) can add embedded within a body of text to hide information that wouldn't be visually apparent when displayed, but can be discovered by examining the document source. HTML pages can contain code for extra blank spaces and tabs at the end of lines, as well as different colors, fonts and sizes, which will not be visible when displayed. A more trivial example is white text on a white background, which can be revealed by "selecting"[8].

There are different methods to implement steganography over text[14]:

- Line Shift Coding Protocol
- Word Shift Coding Protocol
- Feature Coding Protocol
- White Space Manipulation
- Text Content

Image steganography

As stated earlier, images are the most important cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different stenographic algorithms exist.

Image definition

An image is a two-dimensional function f(x,y), where x and y are the spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x,y) is called the intensity of the image at that level. If x,y and the amplitude values of f are finite and discrete quantities, we call the image a digital image. A digital image is composed of a finite number of elements called pixels, each of which has a particular location and value [10]. Images have a finite set of digital values, called picture elements or pixels. The digital image contains a fixed number of rows and columns of pixels. Pixels are the smallest individual element in an image, holding quantized values that represent the brightness of a given color at any specific point. Typically, the pixels are stored in computer memory as a raster image or raster map, a two-dimensional array of small integers. These values are often transmitted or stored in a compressed form. [11]. Each pixel is assigned a total value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation.

For photographic purposes, there are two important types of digital images—color and black and white. A black and white image is made up of pixels each of which holds a single number represented by one byte corresponding to the gray level of the image at a particular location. These gray levels span the full range from black to white in a series of very fine steps,

normally 256 different grays. Since the eye can barely distinguish about 200 different gray levels, this is enough to give the illusion of a step less tonal scale.

A color image is made up of pixels each of which holds three numbers corresponding to the red, green, and blue levels of the image at a particular location. Red, green, and blue (sometimes referred to as RGB) are the primary colors for mixing light—these so-called additive primary colors are different from the subtractive primary colors used for mixing paints (cyan, magenta, and yellow). Any color can be created by mixing the correct amounts of red, green, and blue light. Assuming 256 levels for each primary, each color pixel can be stored in three bytes (24 bits) of memory. This corresponds to roughly 16.7 million different possible colors [12].

Audio and Video Steganography [17,18,19]

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. Some of them are as follows: -

• LSB Coding:

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence.

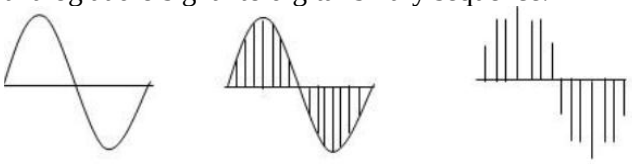

Figure 2: Sampling of the Sine Wave followed by Quantization process.

In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. For example if we want to hide the letter 'A' (binary equivalent 01100101) to an digitized audio file where each sample is represented

With 16 bits, then LSB of 8 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter 'A'.

Sampled Audio Stream (16 bit)	'A' in binary	Audio stream with encoded message
1001 1000 0011 1100	0	1001 1000 0011 1100
1101 1011 0011 1000	1	1101 1011 0011 1001
1011 1100 0011 1101	1	1011 1100 0011 1101
1011 1111 0011 1100	0	1011 1111 0011 1100
1011 1010 0111 1111	0	1011 1010 0111 1110
1111 1000 0011 1100	1	1111 1000 0011 1101
1101 1100 0111 1000	0	1101 1100 0111 1000
1000 1000 0001 1111	1	1000 1000 0001 1111

• Phase Coding:

Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.

Methods of steganography [15]

Steganography generally can be split into two types:

a) Fragile: This steganography involves embedding information into a file which is destroyed if the file is modified.

b) Robust: Robust marking aims to embed information into a file which cannot easily be destroyed.

The comparison of various methods of steganography according to its Embedding Technique and their advantages is as shown in the Table 1. Note all these methods used the same Cover Media but different techniques (Image Hiding) to embedding.

Table 1 COMPARISON OF VARIOUS METHODS OF STEGANOGRAPHY

Steganography Techniques	Cover Media	Embedding Technique	Advantages
LSB (Least Significant Bit)	Image	It works by using the least Significant bits of each pixel in one image to hide the most significant bits of another.	Simple & easiest way of hiding Information.
DCT (Direct Cosine Transform)	Image	Embeds the information by altering the transformed DCT coefficients	Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.
Wavelet Transform	Image	This technique works by taking many wavelets to encode a whole image	Coefficients of the wavelets are altered with the noise within tolerable levels

Direct Cosine Transform:Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants [9].

Combination of Steganography and Cryptography [13]

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques**.**

Steganalysis:

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information. Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message [21]. Steganographic attacks consist of detecting, extracting and destroying hidden object of the stego media. Steganography attack is followed by steganalysis. There are several types of attacks based on the information available for analysis. Some of them are as follows: -

・Known carrier attack:

The original cover media and stego media both are available for analysis.

・Steganography only attack:

In this type of attacks, only stego media is available for analysis.

・Known message attack:

The hidden message is known in this case.

・Known steganography attack:

The cover media, stego media as well as the steganography tool or algorithm, are known [16].

Visual detection [21]

Analyzing repetitive patterns may reveal the identification of a steganography tool or hidden information. To inspect these patterns an approach is to compare the original cover image with the stego image and note visible differences. This is called a known-carrier attack. By comparing numerous images it is possible that patterns emerge as signatures to a steganography tool. Another visual clue to the presence of hidden information is padding or cropping of an image. With some stego tools if an image does not fit into a fixed size it is cropped or padded with black spaces. There may also be a difference in the file size between the stego-image and the cover image. Another indicator is a large increase or decrease in the number of unique colors, or colors in a palette which increase incrementally rather than randomly.

The Proposed Algorithm: There are many algorithms was used to hiding information in different digital files but in this paper simple algorithm was proposed. This research aims to study the case of hiding text in a digital image. This will be done by comparing the value of each letter of the text that we want to hide inside the cover image with the value of the pixels within the same image. The address of each pixel that match the letter's value will be stored in a file called map file. The map file then will be sent to the recipient in order to test the values of those titles to extract the message. As is well known that every digital color image is composed of pixels, which represents the smallest element in the image, each pixel in turn consists of three color compounds; those are red, blue and green. So all the three compounds will be compared in order to get a match.

Embedding algorithm:

1. For each pixel in the cover image, read the value of color components.
2. Convert each letter and symbol in the text that you want to hide turned into numbers using the ASCII code table.
3. Compare the value of the character (that is obtained in step 2) with the value of color component (that is obtained in step 1) within each pixel In order to find if the two values are equal. In this case the search stops and the address of that pixel in the image, as well as the sequence of composite color of that pixel which equal to the value of that character, will be stored in the map file.
4. This process will be repeated for each letter of the text, then the map file will be sent to the recipient in the addition to the picture in order to draw the message of this image. This process is done using the following steps:

a. Reading addresses (Sequences) within the map file and get the first address.
b. Go directly to the pixel's that is match the address taken from the map file (step a).
c. Search inside the color components of that pixel according to what is stated within the map file
d. Read the numeric value of that color component to be converted to corresponding character according to the ASCII table.
e. The process will be repeated for all the sequences in the map file.

Discussion:

There are many researches in the field of our paper and each one has its own way to hide the

information into the image at which the strength of the research depends on the amount of hided information and the distortion that can affect the image after the hiding.

So in our research, we focused on how to hide the information inside an image without any distortion as we will not do any real information hiding inside the image. One another advantage of our approach is in the case of the image being hacked by intruders then the information will be safe as there are no real information being hide inside it.

The only problem that can face the our approach is in the case of sending the map file (after encryption) via a secure connection will be with large size, so it can be suspicious and the intruders will try to get it, but this will not be a problem as the information is encrypted.

One another way of increasing the efficiency of the proposed approach is to encrypt the messages before hiding it.

References

[1].F.Johnson, SushilJajodia, Exploring Steganography Seeing the Unseen, George Mason University, IEEE, 1998.

[2]. J. Juan, M.Jesús, SLSB: Improving the Steganographic Algorithm LSB, Universidad Nacional de Educación a Distancia (Spain)

[3]. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[4]. Chandramouli, R., Kharrazi, M. &Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[5]. Chandramouli, R., Kharrazi, M. &Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003..

[6] Anderson, R.J. &Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areasin Communications, May 1998.

[7] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", *19th National Information Systems Security Conference*, 1996

[8]. Wikipedia,"Steganography", 2013.

[9]. MohamedAmin&Subariah Ibrahim, "Information hiding using steganographyApproach" , university technology Malaysia, 2003.

[10]. PhD. Hasan Demirel, "Digital Image Processing" , EE-583

[11].Wikipedia, "Digital image", ***2012.***

[12]. Jonathan Sachs, "Digital Image Basics", 1999.

[13]. Arvind Kumar, Pooja. Km, Steganography- A Data Hiding Technique International Journal of Computer Applications, Volume 9– No.7, November 2010.

[14].Jonathan Cummins, Patrick Diskin, "Steganography And Digital Watermarking", 2004.

[15]. Shashikala Channalli, "Steganography An Art of Hiding Data ", International Journal on Computer Science and Engineering Vol.1(3), 2009.

[16]. Das Soumyendu, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches ",

[17] MP3Stego: Hiding Text in MP3 Files - Mark Noto,The Information Security Reading Room, SANS Institute 2001
http://www.sans.org/reading_room/whitepapers/steganography/550.php

[18] Digital video steganalysis exploiting collusion sensitivity- Udit Budhiaa and Deepa Kundur Sensors, Command Control, Communications and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense, Edward M.Carapezza, ed., Proc. SPIE (vol. 5403), Orlando, Florida, April 2004.http://www.ece.tamu.edu/~deepa/pdf/BudKun04.pdf

[19] Methods of Audio Steganography, Internet Publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.html

[20]. Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[21]. Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Volume 9– No.7, November 2010