EUSRM A Universe of Research ISSN(ONLINE) : 2319-3069

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7

Vol. 6 Issue 5
May 2014

A Study on Image Steganography Approaches in Digital Images

R.M. Yadav [1], Dr. Deepak Singh Tomar[2], Dr. R.K. Baghel [3]
Department of CSE&IT, ECE, MANIT, Bhopal, M.P., India
rmyyadav@rediffmail.com[1], deepaktomarmanit@gmail.com[2], rakbagh@yahoo.co.in[3]

Abstract

Steganography is the process of embedding information in a carrier in order to protect the secrecy in the terms of text, music, video and images. Steganography is the art of hiding information. Normally information are embedded in images it remain unvisible in the majority of commercial image databases, such as Getty (gettyimages.ie) or iStock Photo (istockphoto.com). Thus the advantage of using steganographic techniques for information hiding is that the existgence is resistant to detection and consequently to tampering. Robustness is a characteristic of critical importance. In this paper, we present the key concepts and the representation of steganography area is graphically & mathematically shown. Distinctions between steganography, cryptography and watermarking in terms of technique and intent are summarized. The common approaches used for embedding information into images are shown in detail. Methods applied for hiding messages are also explored. Steganography tools are highlighted.

Keywords

Steganography, Image processing, Security, Information Hiding

1 Introduction

Digital communication has become an essential part of infrastructure now-a-days. A lot of applications are internet- based and in some cases it is desired that communication be made secret. Internet and wireless networks make delivery and exchange of digital information possible. Software and devices have provided users worldwide with the ability to access, develop and modify objects [1]. In this respect, the governments and private companies often want to be privy to civilians who want to save the secret information from others [2]. Various motives are present to detect the steganography use and thus methods to do so are increasingly developed whereas methods for steganography are increasingly becoming advanced [3]. Steganography is the art and science of hiding the existence of the communication secrete through the concealment of the information within other information [4]. Varying carrier file formats are utilized, despite that images are widely being used due to their internet speed.

In security systems domain, information encryption and information hiding are the two common disciplines that are being used to protect information. Steganography is superior to cryptography in a sense that it is not by means to prevent others from being privy of the embedded message, but it is to prevent them from being privy to the existence of the information [2]. It is more inconspicuous to embed information in a image than to communicate an encrypted file [5].

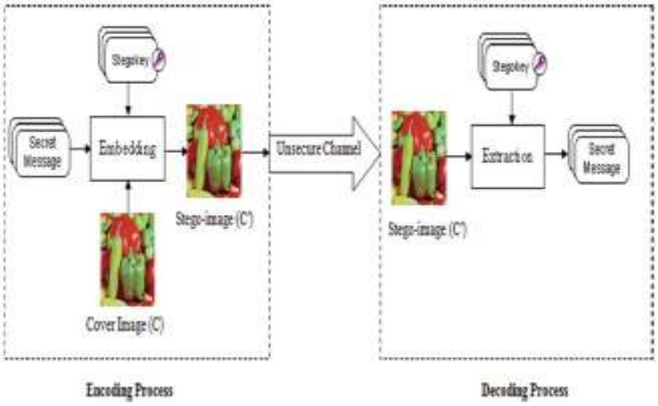


Figure : 1 The basic steganography model of the process of Hiding and Retrieval the message.

Let M denote to the set of embeddable messages.
Let C denote to the set of cover images.
Let K denote to the stego-key that is obtained from a set of stego-keys K.
Two mappings are included in a steganographic scheme, namely the hiding procedure (Hide) and the extraction procedure (Ext) [69].

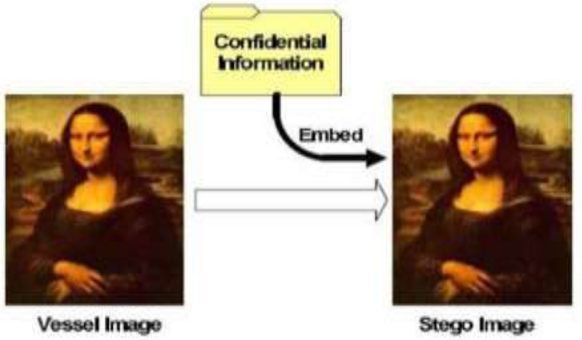
Hide: C x K x M------------C’ (1)
Ext: C’-----------M (2)

Where, Ext (Hide (c, k, m)) = m for all c ε C, k ε K, and m ε M. C' = Hide (c, k, m) is referred to as the stego-image.

In a steganographic communication, the sender and receiver agree on using the steganographic method [6], and for the prevention of information detection, it is convenient to use a secret key. In particular, this key is shared between the sender and receiver, and is utilized to control the message hiding and extraction.

2. Steganography Principle

The secret message is embedded inside the cover object by a hiding algorithm and is sent to a receiver. The The receiver then applies the reverse process on the cover data and reveals the secret data.



Figuer2: Simple presentation of the principle of steganography

The embedding i.e. steganography algorithm, tries to preserve the perceptive properties of the original image. A suitable image, called the cover/carrier, is selected. The secret message is then embedded into the cover using the steganography algorithm, in a way that does not change the original image in a human perceptible way. The result in new image, the stego-image, that is not visible different from the original.

3. Various categories of Steganography

Most of the 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 [4]. 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 3 shows specially the four types of file formats that can be used for steganography.

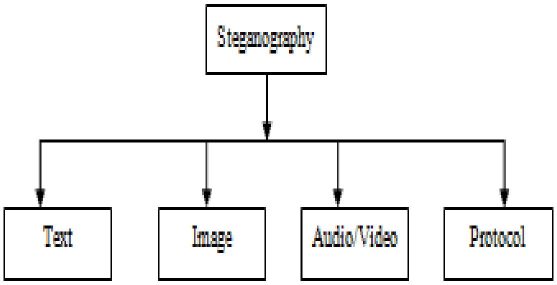


Figure 3: The categories of steganography

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. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance [8, 9]. Text steganography using digital files is not used very often since text files have a very small amount of redundant data [10].

Since, images are quite popular cover or carrier objects used for steganography. In the domain of digital images different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist, Here, in this paper, we will discuss about the image domain steganography methods.

In image domain methods, secret messages are embedded using the intensity of the pixels values directly. The image domain methods are relatively simple compared to the other methods and are sometimes characterized as the simple systems. However, they are generally more senstitive to small changes on the image such as filtering, resizing and squeezing.

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [10]. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images [11].

Protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [13].

4. Image Steganography

Images are the most popular 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 steganographic algorithms exist. Figure 4 shows Categories of image Steganography [12].

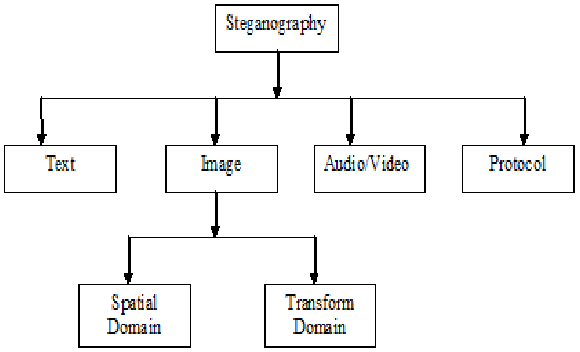


Figure 4 : Types of Image Steganography

5.Image Steganography Techniques

Image steganography techniques can be divided into two broad categories: Spatial domain based steganography and Transform domain based steganography.

5.1 Spatial Domain Technique\

In spatial domain method, the secret messages are embedded directly. Here, the most common and simplest steganography method is the Least Significant Bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding.

Least Significant Bit Insertion Technique

Most of the steganography software hide information by replacing only the least significant bits (LSB) of an image with bits form the file that is to be hidden. This technique works good for image steganography, is generally called LSB encoding. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels : 10010100 00001101 11001001 10010110 00001110 1100101 10011111 00010001 11001010

Secret Message i. e. A, the binary representation of A is : 01000001

Result : 10010100 00001101 1100100**0** 10010110 00001110 1100101**0** 1001111**0** 00010001 11001010

Here the letter A was embedded into the grid, only the 3 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

The three bold bits were actually replaced. Since the eight bit letter A only requires eight bytes to begin hiding the next character of the hidden messages. A slight variation of this technique allows for embedding the message in two or more of the LSB per byte. LSB insertion is easy to implement, it is also easily attacked . Slight modification in the color palette and simple image manipulations will destroy the entire hidden message. Some example of these simple image manipulations include image resizing and cropping. Since the steganalysis of LSb technique is easier. So, this is suggested that the image should be first manipulated before the embedding of the message into it.

Least Significant Bit Algorithm

Step 1. Select a cover image of size M*N as an input.
Step 2. The message to be hidden is embedded in RGB component only of an image.
Step 3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).

Step 4. After that Message is hidden using Bit Replacement method

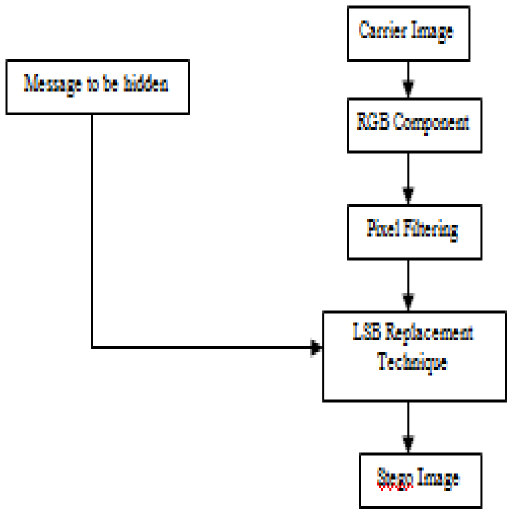


Figure 5 : Flow chart of Least Significant Bit

5.2 Transform Domain Technique

The transform domain Steganography technique is used for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The idea is to hide information in frequency domain by altering magnitude of all of discrete cosine transform (DCT) coefficients of cover image. The 2-D DCT converts image blocks from spatial domain to frequency domain. The carrier image is divided into non overlapping of size 8 x 8 and applies DCT on each of blocks of cover image using forward DCT [7].

It now perform Huffman encoding on the 2D secret image of size M2 x N2, to convert it into1D stream. Huffman code is decomposed in 8 bits blocks. The least significant bit of all of the DCT coefficients inside 8 x 8 block is changed to a bit taken from each 8 bit block from left to right. Now perform the inverse block DCT using inverse DCT and obtain a new image which contains secret image. At the receiver side, the stgo-image is received, which is in the spatial domain.

6. Statistical Analysis

There are two primary types of statistical analysis methods, which are : The image histograms and the peak-signal-to-noise ratio (PSNR) [15,16]. Histograms are considered as graphics that are utilized for data distributions display for quantitative variables. As for image, the variables or frequencies are considered as intensity values of image [16]. The PSNR is utilized as a performance measurement for the distortion of the image [15]. It is used to measure the image quality through a comparison between the cover image C and the stego-image S [17]. In particular, this method is defined as:

$$\mathrm{PSNR}(C,S) = 10\log_{10}\frac{(2^d-1)^2}{MSE}\ dB \qquad (3)$$

Where , d denotes the bit depth of the cover image, and is equal to 8 for gray-scale images. The MSE denotes the mean square error between the cover image and the stego-image, and is defined as:

$$\mathrm{MSE}\,(C,S) = \frac{1}{MN}\ \boxed{\sum_{i=1}^{M}\ \sum_{j=1}^{N}}\ (S_{ij}-C_{ij})$$

I=1 I=1

Where, Sij and Cij denote the pixel values of the cover image and the stego-iamge, respectively M and N represent the dimensions of the cover image.

The Large the PSNR, The better is the stego-image quality. The values of the PSNR that are lower than 30 dB imply a low quality, i.e., the embedding distortion can be obivoius, while 40 db and above imply a high quality stego-image [14]

Where, Sij and Cij denote the pixel values of the cover image and the stego-iamge, respectively M and N represent the dimensions of the cover image.

The Large the PSNR, The better is the stego-image quality. The values of the PSNR that are lower than 30 dB imply a low quality, i.e., the embedding distortion can be obivoius, while 40 db and above imply a high quality stego-image [14]

7. Steganography in Digital Image

The use of digital image steganography is increasing the interest in Internet development [18]. It is now a common place for individuals to put up their pictures, videos, and sounds to share with others. This type of objects have taken place a convenient place to hide secret information for the primary reason that idicates to typical digital media file comprising a huge number of pixels can be altered to hide a message.

The computer image files are shared by email, sites and other digital methods on the Internet [19]. The digital image is represented as a matrix of numeric values that represent the intensitites for various points which are called pixels. These pixels make up theraster data of the image. The bit depth is referred to the amount of bits in a color scheme, and is the amount of bits that is usilized for every pixel. The tiniest bit depth under the present color schemes is 8 bits are utilized to provide a description of every pixel's color. Images of digital colors are specially kept in 24 bit files, where the RGB color model is used by these images, referred to as a true color. Therefore, in a signle pixel, ar a total of 256 varying amounts of Red, Green, and Blue, totalling more than 16 million colors [6]. A pixel with 255 for red value and 0 for green and blue values renders the color red. A 24 bit color image with a resolution of 1024 x 768 can hide about 2.36 MBs of data.

8. Compression in Digital Image

For the purpose of digital image steganography, techniques must be included for the reduction of the file size of the image. There two kinds of compression in images, namely lossy and lossless, and both are storage space savers, although they differ in their implementation. The lossy compression method develops smaller files by getting rid of the original image's extra data. It gets rid of the details that are too tiny for the human eye to detect, which leads to the original image's close approximations. The image format using this compression method is JPEG (Joint Photographic Experts Group). This file format is the most widely existing image file format on the internet owing to its small size. Compression methods have significant roles in selecting steganographic algorithms; lossy compression maximizes the chance of losing part of the secret message as excess image data will be eliminated. On the other hande, lossless compression prevents the loss of even the slightest part of the message, but it cannot compress the file steganographic algorithms have been proposed [5].

9. Steganography approaches in Digital Image

The digital image steganography has mainly two approaches : Spatial Domain Steganography and Frequency Domain Steganography. In spatial domain, LSB is easy but not robust as compared with Frequency Domain Steganography.

Least Significant Bit Steganography

The several variations of the LSB steganography are available today with different levels os susceptible to detection. The LSB steganography can be used with a gray-scale or 24 bit images to embed the secret message bits in the LSBs of sequentially or randomly selected pixels of the cover image. For example, here, a new LSB algorithm that embeds a secret message in a 24 bit image is show how it is easy to manipulate the pixels of an image. The cover 24 bit image is virtually divided up into disjoint blocks with each block's size being equal to the size of the secret message. Here, a secret message is a gray-scale image of the size M x N. Each pixel from the secret image is to be embedded in the best pixel's byte among the corresponding pixels in the the blocks of the cover image. Best byte of the pixel is the one that gives minimum differences between it and the pixel to be embedded. The pseudo code below shows the embedding process

```
For i = 1 to M;
For j = 1 to M;
Endfor;
Endfor;
```

10. Advantages and disadvantages of the steganography methods

Steganography method	Advantage	Disadvantage
spatial domain	1. High embedding capacity 2. There is less chance for degradation of the original image. 3. Moreinformation can be stored in an image.	1. Less robust, the hidden data can be lost with image manipulation. 2. Hidden data can be easily destroyed by simple attacks. 3.Typically depend on the image format.
Frequency domain	1.Less prone t lossy compression and common image processing techniques. 2. Typically independent of the image format.	1Low embedding capacity 2.Embedding message happens in the co-efficient ofthe transformed image; more computations are required. 3. Less robust against second order statistical analysis.

12. Conclusion

This paper presented a background of Steganography and a comprehensive study of some Steganographic software. Steganography as information security system can have some useful applications, like other seemingly related system (cryptography). Steganography aims at creating covert channels for secret or private communications. All the techniques under the image domain methods are focus which mostly works on the least significant bits of the pixel values. The tool for measuring the quality of image after embedding is the PSNR. The selections of the cover images impacts the security of steganography systems. Advantages and disadvantages of steganography method are shown The success of this study is to identify the reliable steganography approaches in digital images.

Reference :

[1] M.Wu. and B.Liu. "Data Hiding in image and video.I.Fundamental issues and solutions." IEEE Transactions on Image Processing. Vol.12,pp.685-95, 2003

[2] M.M. Amin. M. Shalleh, S. Ibrahim, M.R. Katmin, and M. Shamsuddin, "Information Hiding using steganography" in 4th National Conference on Telecommunication Technology (NCTT) 2003), Shah Alam, Malaysia, pp. 14-15 Jan. 2003.

[3] R. Krenn. " Steganography and steganalysis" An Article, Santa Barbara, California, Jan. 2004, available from :http/www.krenn.nl/univ/cry/steg/article.pdf

[4] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998.

[5] T.Morkel, J.H.P. Eloff, and M.S. Olivier, "An overview of image Staganography" in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, pp.1-12, 2005.

[6] N. Provos, and P. Honeyman, "Hide and Seek: An inftroduction to steganography." Security and Privacy, IEEE, Vol. 1, pp. 32-44, 2003.

[7] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", *Proceedings of the Workshop on Multimedia Security at ACM Multimedia*, 2002.

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

[9] Handel, T. & Sandford, M., "Hiding data in the OSI network model", *Proceedings of the 1st International Workshop on Information Hiding*, June 1996.

[10] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", *Proceedings of the 2nd Information Hiding Workshop*, April 1998.

[11] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", *Proceedings of the International Conference on Information Technology: Coding and Computing*, 2004.

[12] N. Jacobsen, K. Solanki, U. Madhow, B. S. Manjunath a, and S. Chandrasekaran, "Imageadaptive high-volume data hiding based on scalar quantization," *in Proceedings of IEEE Military Communications Conference (MILCOM), Anaheim, CA, USA*, October 2002.

[13] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", *Proceedings of the IEEE*, 87:07, July 1999.

[14] A. Cheddad, J. Condell, K. Curran, and P.Mc Kevitt, "Digital image steganography, survey and analysis of current methods" signal processing. Vol 90, pp 727-52, 2010.

[15] A. Cheddad, J. Condell, K. Curran, and P.Mc Kevitt, "Enhancing Steganography in Digital images in Canadian Conference on Computer and Robot Vision, Windsor, Ontario, pp. 326-32, May 2008.

[16] A. Cheddad, J. Condell, K. Curran, and P.Mc Kevitt, "A Comparative Analysis of Steganography Tools" in the 7th Information Technology and Telecommunication Conference, Ireland, pp. 43-51, Oct. 2007.