ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 1, January 2013

Image Steganography

Rahul Joshi[1],Lokesh Gagnani[2] , Salony Pandey[3]
[1] PG Student,KIRC,Kalol
[2] Asst Prof,KIRC(I.T Department)
[3]PG Student,RK UNI,Rajkot

Abstract: **Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. This paper intends to give an overview of image steganography, its uses .**

I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" [1] defining it as "covered writing". In image steganography the information is hidden exclusively in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. 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 [2]. 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 [2]. The strength of steganography can thus be amplified by combining it with cryptography. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [4], forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [5].

Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

II. 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 [6]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [3]. 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.

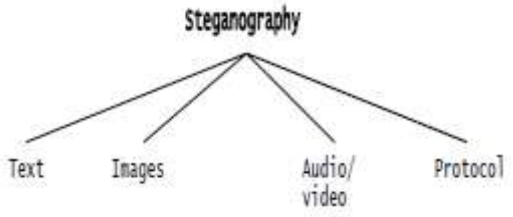


Figure 1: Categories of steganography

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 Text Images Audio/video Protocol Internet and all the different digital file formats that is has decreased in importance [1]. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

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 [1]. 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 [5].

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [8]. In the layers of the OSI network model there exist covert channels where steganography can be used [7]. An example of where information can be hidden is in the

header of a TCP/IP packet in some fields that are either optional or are never used. A paper by Ahsan and Kundur provides more information on this [8].

III. VARIOUS TECHNIQUES

A) LSB method [9]

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel. For example data bits 01100101 are tried to hide into an 8 bit colour image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may be like this:

00100101 11101011 11001010 00100011
11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become:

0010010**0** 1110101**1** 1100101**1** 0010001**0**
1111100**0** 1110111**1** 1100111**0** 1110011**1**

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

Advantages of LSB.

1. 100 % chances of insertion.
2. Easy to implement.

Disadvantages of LSB.

1) One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.

2). Not immune to noise and compression technique.

B) Local pixel adjustment technique [10]

Local Pixel adjustment process improves the image quality of the stego-image. Local pixel adjustment process only considers the last three significant bits and the fourth bit but not all bits. The local pixel adjustment method is not optimal. As the local Pixel Adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution.

C). Optimal pixel adjustment technique [11]

This is the technique given by Chan et. al in 2003. This is a data hiding scheme which uses simple LSB substitution with an optimal pixel adjustment process. This method provides less change in image quality as compared to the LSB Method and local pixel adjustment process (LPAP). The image quality of the stego-image is improved by using this method.

D). 6th, 7th and 8th bit method [12]

In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message.

E) Parity checker method [13]

In this method, Rajkumar et al gives the concept of odd and even parity. According to this method, 0 can be inserted at a pixel location if that pixel has odd parity i.e. the number of 1's in the binary value of the pixel should be odd. Similarly, 1 can be inserted at a pixel location if that pixel has even parity i.e. the number of 1's in the binary value of pixel should be even. If the corresponding parity does not exist at a pixel location either for 0 or 1, then we make corresponding parity at that pixel location (odd parity for 0 and even parity for 1) by adding or subtracting 1 to the pixel location such that the change in the image quality should not be visible to the human visual system (HVS).

F) PVD method [14]

The pixel value differencing (PVD) method proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification.

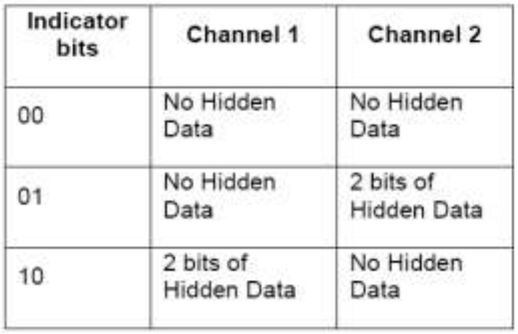
G) Tri-way PVD method [15]

This method is an improvement of the PVD method in terms of hiding capacity. In PVD method, only one direction is referenced whereas in this method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits. At first, the entire cover image is divided into a number of non-overlapping 2X2 blocks. Three pixel pairs of each block aroused for embedding purpose. The pixel pair that is taken into consideration is in the horizontal, vertical and diagonal directions. Data bits are embedded on the basis of the difference between the two pixel values of each pixel pair.

H) Pixel indicator technique [16]

The pixel indicator technique uses the least two significant bits of one channel from the Red, Green and Blue channel as an indicator for existence of data in other two channels. The indicator channels are chosen in sequence with Red being the first. Table 1 shows the relation between the indicator bits and amount of hidden data stored in the other. may prove too much for some.

Table 1



Indicator bits	Channel 1	Channel 2
00	No Hidden Data	No Hidden Data
01	No Hidden Data	2 bits of Hidden Data
10	2 bits of Hidden Data	No Hidden Data

IV.CONCLUSION

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness.
Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf

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

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

[4] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002

[5] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

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

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

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

[9] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34, February 1998.

[10] Chi-Kwong Chan, L.M. Cheng," Improved hiding data in images by optimal moderately significant bit replacement", IEEE Electron. Lett. 37(16)(2001)1017-1018.

[11] Chi-Kwong Chan, L.M. Cheng," Improved hiding data in images by simple LSB substitution ", Pattern Reorganization, Elsevier,37(2004)469-474

[12] Sudhir Batra, Rahul Rishi and Raj Kumar, “Insertion of Message in 6th, 7th and 8th bit of pixel values and its retrievals in case intruder changes the least significant bits of image pixels”, International Journal of Security and its application, Vol. 4, No. 3, July 2010.

[13] Yadav Rajkumar, Rishi, Rahul, Batra, Sudhir, “A new Steganography Method for Gray Level Images using Parity Checker”, International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.

[14] D.C. Wu and W.H. Tsai. “A steganographic method for images by pixel-value differencing”. Pattern Recognition Letters, 24: 1613-1626, 2003.

[15] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu,” A Novel Image steganographic Method Using Tri-way Pixel-Value Differencing”, *Journal of Multimedia*, VOL. 3, NO. 2, June 2008

[16] Adnan Abdul-Aziz Gutub,” Pixel Indicator Technique for RGB Image Steganography”, *Journal of Emerging Technologies in Web Intelligence*, VOL. 2, NO. 1, February 2010