Salony Pandey, Prof. Amit.M.Lathigara / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1295-1297

Hiding Text behind Image for Secure Communication

Salony Pandey[1], Prof. Amit.M.Lathigara[2]
[1]PG Student,RK UNI,Rajkot
[2] C.E Dept. R.K 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 exist 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.CATEGORIES 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.

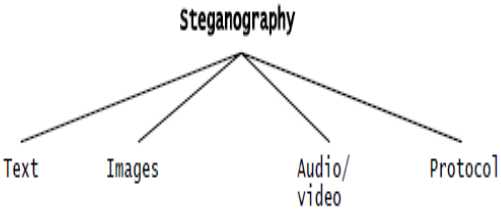


Figure 1: Categories of steganography

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.

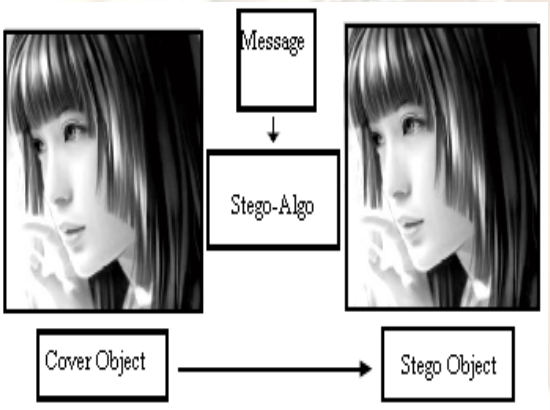
Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

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. IMAGE STEGANOGRAPHY PRINCIPAL



IV.IMAGE STEGANOGRAPHY TERMS

- Carrier File – A file which has hidden information inside of it
- Steganalysis – The process of detecting hidden information inside of a file.
- Stego-Medium – The medium in which the information is hidden.
- Redundant Bits – Pieces of information inside a file which can be overwritten or altered without damaging the file.
- Payload – The information which is the be concealed.

V. HIDING A MESSAGE INSIDE IMAGES

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in news groups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster, which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit(LSB).

VI. LEAST SIGNIFICANT BIT METHOD

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:
00100100 11101011 11001011 00100010
11111000 11101111 11001110 11100111
The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise

.

LSB - Uses

- Storing passwords and/or other confidential information
- Covert communication of sensitive data
- Speculated uses in terrorist activities
- Being widely used to hide and/or transfer illegal content

VII. REASONS FOR USING DIGITAL IMAGES

- It is the most widely used medium being used today
- Takes advantage of our limited visual perception of colors
- This field is expected to continually grow as computer graphics power also grows
- Many programs are available to apply steganography

VIII. IMAGE ATTRIBUTES

- Digital images are made up of pixels

- The arrangement of pixels make up the image's "raster data"
- 8-bit and 24-bit images are common
- The larger the image size, the more information you can hide. However, larger images may require compression to avoid detection

IX. STEGANALYSIS

For hiding information, an equal number of clever techniques have been designed to detect the hidden information [9]. These techniques are collectively known as 'steganalysis'. As introduced earlier, the Laplace formula is one such steganalytic method. Attacks on steganography can involve detection and/or destruction of the embedded message. A stego-only attack is when only the stego-image is available to be analysed .

A known cover attack is when the original cover image is also available. It involves comparing the original cover image with the stego-image. As hiding information results in alterations to the properties of a carrier which may result in some sort of degradation to the carrier. Original images and stego-images can be analyzed by looking at colour composition, luminance and pixel relationships and unusual characteristics can be detected. If a hidden message is revealed at some later date the attacker could analyse the stego-image for future attacks. This is called known message attack.

The chosen stego attack is used when the steganography algorithm and the image are known. A chosen message attack is when the stegoanalyst generates stego-images using a given steganography algorithm using a known message. The purpose is to examine the patterns produced in the stego images that may point to the use of certain steganography algorithms. Most steganographic algorithms embed messages by replacing carefully selected pixels bits with message bits.

Any changes to the data associated with the image through embedding will change the properties of the image in some way. This process may create patterns or unusual exaggerated noise.
Two other popular techniques are RS Analysis and Sample Pairs Analysis. RS Analysis makes small modifications to the least significant bit plane in an image then uses these modifications and a discrimination function to classify groups of pixels. The counts of the groups based on the modifications allow the calculation of an estimated embedding rate. Images that do not contain steganography often have a natural embedding rate of up to 3%, whereas images containing hidden information usually have estimated embedding rates which accurately reflects the amount of hidden information. RS Analysis is a special case of Sample Pairs Analysis, which also uses least significant bit modifications to help calculate an estimated embedding rate.
Sample Pairs Analysis utilizes finite state machines to classify groups of pixels modified by a given pattern. Both steganalysis techniques are very accurate at predicting the embedding rate on stego-images using least significant bit embedding

X.CONCLUSION

Image Steganography as a whole has existed in many forms throughout much of history.
Lossless compression of images with a great deal of color variation work best as a cover image to embed a message. Image Steganography can be used as beneficial tool for privacy

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] M. Wu and B. Liu, Multimedia Data Hiding. New York: Springer-Verlag, 2003