

Evaluation of Various LSB based Methods of Image Steganography on GIF File Format

Namita Tiwari
Asst.Prof. Deptt.of computer science
MITS, Gwalior,India

Dr.Madhu Shandilya
Professor,Deptt.of Electronics,
MANIT Bhopal,India

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. There have been many steganographic techniques available for hiding message in image having its own strength and weaknesses. Steganography can be carried out on any digital media. The chosen media for this system are GIF images. It is chosen due to wide use in web pages. In this paper we look at all the available image based steganography along with the cryptography technique to achieve security. This paper will focus on hiding the message in the least significant bits of the colors of the pixels of a GIF image. We discuss results obtained from evaluating available steganographic techniques and compare the different methods according to the vulnerability. In this paper we also discuss some application of steganography in network security

Keywords

Steganography, Cryptography, LSB, GIF image.

1. INTRODUCTION

As a society, humans have continually sought new and efficient ways to communicate. The earliest methods included cave drawings, smoke signals, and drums. Advancements of civilization introduced written language, telegraph, radio/television, and most recently electronic mail. As more and more communication is conducted electronically, new needs, issues, and opportunities are born. At times when we communicate, we prefer that only the intended recipient have the ability to decipher the contents of the communication. We want to keep the message secret. A common solution to this problem is the use of encryption. While encryption masks the meaning of a communication, instances exist where we would prefer that the entire communication process not be evident to any observer that is, even the fact that communication is taking place is a secret. In this case, we want to keep the communication hidden. Steganography can be used to hide or cover the existence of communication. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data.

A solution to this problem is steganography.

2. STEGANOGRAPHY AND CRYPTOGRAPHY

In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system has two stages:

1. The attacker can detect that steganography has been used.
2. Additionally, he is able to read the embedded message.

In our definition a steganographic system is insecure already if the detection of steganography is possible (first stage).

3. TYPES OF STEGANOGRAPHY

Steganography can be classified into various types, depending upon the cover medium used. Cover medium may be text, image or audio or video file. Hence steganography can be said to occur in three major types:

- i)Text Steganography
- ii)Image Steganography
- iii)Audio/video Steganography

3.1 Image Steganography

Image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image.

Image steganography has come quite far in recent years with the development of fast, powerful graphical computers. Digital image is the most common type of carrier used for steganography.

A digital image is composed of finite number of elements each of which has a particular location and value (gray scale). The processing of these digital images by means of a digital Computer is referred as digital image processing. Images are used for steganography in following ways.

The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. This results in the production of what is called a stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey.

The stego-image is then transmitted to the recipient. The recipient extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient.

This could be the algorithm for extraction or a special parameter such as a key. A stegoanalyst or attacker may try to intercept the stego-image. Computer based steganography allows changes to be made to what are known as digital carriers such as images or sounds. The changes represent the hidden message, but result if successful in no discernible change to the carrier. The information has nothing to do with the carrier sound or image. Information might be about the carrier such as the author or a digital watermark or fingerprint.

4. STEGANOGRAPHY APPLICATIONS

Steganography is very useful in the field of information technology because it used for the purpose of network security. Used for message authentication that means message is coming from a authorize person and will transmitted to an intended receiver. It keeps data integrity means there will be no modification in content of information during communication. Apart from that it keeps secrecy and privacy as well. Steganography techniques can be used for the purposes of watermarking.

Watermarking is the process of hiding information in a carrier in order to protect the ownership of text, music, films and art. Steganography can be used for example by civil rights organizations in repressive states to communicate their message to the outside world without their own government being aware of it.

Less virtuously, terrorists to communicate with one another without anyone else's knowledge can use it. In both examples the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to protect the courier.

5. IMAGE FORMAT

There are several types of image file formats that can be used for steganography and each has certain advantages and disadvantages for hiding messages. There are two types of images on the Internet available in a palette format GIF and PNG. GIF will be looked at in some detail.

5.1 GIF Graphics Interchange Format

GIF is used for the purpose of storing multiple bitmap images in a single file for exchange between platforms and images.

It is often used for storing multibit graphics and image data. GIF is not associated with a particular software application but was designed "to allow the easy interchange and viewing of image data stored on local or remote computer systems".

GIF is stream based and is made up of a series of data packets called blocks (which can be found anywhere in the file) and protocol information. GIF files are read as a continuous stream of data and the screen is read pixel by pixel. GIF is used also because it applies lossless file compression method.

6. METHODS OF STEGANOGRPHY

6.1 One Bit Stego

When images are used as the carrier in steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message can be stored in the LSB of one colour of the RGB value or in the parity bit of the entire RGB value. This process will most likely result in the formation of new colours for the palette. Therefore the image used must have a palette size of 128 pixels or less.

6.2 Two Bits Stego

Using this method two LSBs of one of the colours in the RGB value of the pixels will be used to store message bits in the image. This will involve using a palette with a maximum of 64 colours allowing for the production of possible 192 new colours, i.e. two new colours for each existing colour. The advantage of this method is that twice as much information can be stored here than in the previous method

6.3 Three Bits Stego

Using this method three LSBs of one of the colours in the RGB value of the pixels will be used to store message bits. This will involve using a palette with a maximum of only 32 colours allowing for the production of a possible 224 new colours, three new colours for every existing colour in the image. The data hiding capacity is three times the storage capacity of One Bit change method but the image will be even more distorted than if a 128-colour palette was used.

6.4 Four Bits Stego

Using this method four LSBs of one of the colours in the RGB value of the pixels will be used to store message bits. This will involve using a palette with a maximum of only 16 colours allowing for the production of a possible 240 new colours. This is the smallest palette that could be used for an image using Jasc Paint Shop Pro. The colours are now very restricted but an area of one particular colour in the image may have 16 variations distributed through it which could result in a certain amount of texture mitigating the effects of such a restricted palette.

6.5 Colour Cycle Stego

In order to make the detection of the hidden data more difficult it was decided to cycle through the colour values in each of the pixels

in which to store the data. This also means that the same colour was not constantly being changed.

6.6 Cryptography – Knapsack

An encryption method will be investigated and will be provided as one of the final options for the user. The purpose here is not to use or develop a secure cryptographic method but to use a relatively simple method, which contains a key in order to more randomly distribute the message over the image. Knapsack was the first algorithm for generalized public key encryption.

7. EVALUATION

Three distinct but complementary methods of evaluation will be used. These are:

7.1 Pattern Analysis of Image Pixels

This detection method is based on looking for patterns in the bits that make up the pixel colours. For example if methods hide messages in the least significant bits of pixels then looking for patterns in the least significant bits of pixels is an easy way to detect the existence of messages.

There are many variations of this message hiding technique such as hiding the message bit in the least significant bit of either the red, green or blue value of the colour or the parity bit of the pixel.

This analysis will be carried out based on the literature survey rather than visual inspection of the images. The objective is to determine which of the methods being studied are vulnerable to this method of analysis and how vulnerable they are

7.2 Pattern Analysis of Image Palette

This detection method is based on looking for patterns in the images palette. For example some steganography methods require an image with a reduced number of colours.

The steganography methods then create new colours that are almost identical to the existing ones but have different least significant bits or parities. By ordering the palette by luminance such pairings may be visible.

The fewer original colours the steganography method allows the more obvious it should be in the palette. A colour reduced original image with a large message may have up to 256 colours in the palette half of which will be almost identical to the other half.

With a small message the number of new colours added to the original reduced set will be much smaller. In practice however the number of new colours created by the steganography process must be a maximum of 256 (GIF images) but is otherwise random.

Some methods do not however use colour-reduced images and rely entirely on existing colours. Palettes will be examined for colour images, which have had various forms of steganography, carried out on them.

In each case the palette will be ordered by luminance to make it more coherent. Of course when the palette is not ordered by luminance, patterns in the palette are much harder to see. It is assumed however that somebody attempting to carry out steganalysis would order the palette to make their job easier.

The palette from stegoed images will be compared with the palette of the original 256 colour image and the palette of a reduced colour unsteogoed image to see how much the palette has changed. Finally the palette will be examined to look at how it changes when hiding long and short messages.

7.3 Low Level Visual Inspection of Image Pixels

This detection method is based on carrying out a detailed inspection of selected sections of an image at a high degree of magnification to determine whether anomalous patterns become apparent.

As an inspection technique this might be problematical if the original cover image is not available for comparison. Under normal circumstances a person seeking to hide data in an image would be expected to use an image they have created themselves rather than a generally known image and therefore the original cover image would not be available for comparison with the stegoed image using this inspection method.

The tell tale distortions which would typically be looked for include a lack of continuity where continuity is expected (Fridrich method) and a lack of texture where texture is expected (colour reduction).

Table 1. Evaluation of different methods

	Rating	Stego1 Bit	Stego2 Bits	Stego3 Bits	Stego4 Bits	Stego Color Cycle
Pattern Analysis of the Bits	Not Vulnerable					
	Somewhat Vulnerable		X	X	X	X
	Very Vulnerable	X				
Pattern Analysis Of the Palette	Not Vulnerable					
	Somewhat Vulnerable					
	Very Vulnerable		X	X	X	X
Detailed Visual Inspection Of the Image Pixels	Not Vulnerable	X	X			
	Somewhat Vulnerable			X		X
	Very Vulnerable				X	

8. LSB in GIF

Since GIF images only have a bit depth of 8, the amount of information that can be hidden is less than with BMP. Embedding information in GIF images using LSB results in almost the same results as those of using LSB with BMP.

LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a gray scale image. GIF images are indexed images where the colors used in the image are stored in a palette. It is sometimes referred to as a color lookup table. Each pixel is represented as a single byte and the pixel data is an index to the color palette. The colors of the palette are typically ordered from the most used color to the least used colors to reduce lookup time.

Some extra care is to be taken if the GIF images are to be used for Steganography. This is because of the problem with the palette approach. If the LSB of a GIF image is changed using the palette approach, it may result in a completely different color. This is because the index to the color palette is changed. The change in the resulting image is noticeable if the adjacent palette entries are not similar. but the change is not noticeable if the adjacent palette entries are similar. some applications that use LSB methods on GIF images have low security because it is possible to detect even moderate change in the image. Solutions to these problems could be-

1. Sort the palette so that the color difference between consecutive colors are minimized.

2. Add new colors, which are visually similar to the existing colors in the palette.
3. Use Gray scale images- In a 8 bit Gray scale GIF image, there are 256 shades of gray. This results in gradual changes in the colors and it is hard to detect.

9. CONCLUSION

Steganography has its place in the security. On its own, it won't serve much but when used as a layer of cryptography, it would lead to a greater security.

Far fetched applications in privacy protection and intellectual property rights protection. Research is going on in both the directions One is how to incorporate hidden or visible copyright information in various media, which would be published. At the same time, in opposite direction, researchers are working on how to detect the trafficking of illicit material & covert messages published by certain outlawed groups. All methods suffer from an underlying weakness in that the requirement for colour reduction and replacement leaves a very strong steganography signature in the palette.

Stego1Bit is the most secure method in the order. The strengths of StegoColorCycle in terms of having a degree of resistance to pattern analysis of the least significant bits appears to be cancelled out by degree of colour reduction required. Finally despite the additional data hiding capacity of Stego2Bits, Stego3Bits and Stego4Bits the security of the steganography method being used decreases as the data hiding capacity increases making these progressively less desirable techniques

REFERENCES

- [1] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon "Image Steganography: Concepts and Practice" WSPC/Lecture Notes Series: 9in x 6in, Institute of mathematical sciences, Singapore April 22, 2004
- [2] Neil F Johnson & Sushil Jajodia, "Exploring Steganography: Seeing the Unseen" IEEE computer, february 1998 pp26-34
- [3] Lisa M. Marvel, "Image Steganography for Hidden Communication" Final rept. jan 1997-may 1999 2000.
- [4] R. Chandramouli, Nasir Memon, "Analysis of LSB Based Image Steganography Techniques" Proc. IEEE ICIP pp1019-1022, 2001.
- [5] Li Zhi, Sui Ai Fen, "Detection of Random LSB Image Steganography" IEEE pp2113-2117, 2004
- [6] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon "Performance study of common image steganography and steganalysis techniques" *Journal of Electronic Imaging* vol.15(4), pp 041104, Oct-Dec 2006
- [7] Hedieh Sajedi, Mansour Jamzad "Cover Selection Steganography Method Based on Similarity of Image Blocks" IEEE 8th International Conference on Computer and Information Technology Workshops pp379-384, 2008
- [8] Ismail Avcbas, Mehdi Kharrazi, Nasir Memon, Bulent Sankur "Steganalysis with Binary Similarity Measures" EURASIP Journal on Applied Signal Processing 2005:17, 2749-2757, 2005
- [9] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 (Published electronically)
- [10] Sanjeev Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Image Steganography Through Random Numbers Logic" *Signal Processing: An International Journal*, Volume 1 : Issue (1) 2007

- [11] Yanming Di, Huan Liu, Avinash Ramineni, and Arunabha Sen, "Detecting Hidden Information in Images: A Comparative Study", Department of Computer Science and Engineering Arizona State University, Tempe, AZ 85287, 2005.
- [12] Bret Dunbar, "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", As part of the Information Security Reading Room, SANS Institute 2002.
- [13] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB steganography in color and grayscale images" proc. ACM workshop multimedia security, Ottawa, ON Canada, Oct 5, 2001, pp 27-30.
- [14] K. Satish, T. Jayakar, Charles Tobin, K. Madhavi and K. Murali "Chaos Based Spread Spectrum Image Steganography" IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp 587-590 MAY 2004
- [15] Xiangwei Kong, Ziren Wang, Xingang You, "Steganalysis of palette images: Attack Optimal Parity Assignment Algorithm"
- [16] Rafael Gonzalez & Richard Woods, "Digital Image processing" prentice HALL 2002
- [17] Kurak C., J. McHugh, "A Cautionary Note on Image Downgrading", IEEE Eight Annual computer security. Applications Conference, pp. 153-159, 1992.