MESSAGE CONCEALMENT TECHNIQUES USING IMAGE BASED STEGANOGRAPHY

by

Farhan Khan (G260214)

ABSTRACT

Image based Steganography is the most popular method for message concealment. In this paper, two techniques are proposed for enhancing the message secrecy using image based steganography. The first technique is based on the use of punctuation marks to encode a secret message before embedding it into the image file. The second technique is based on the use of modified scytale cipher to hide a secret message in an image file. Both of these techniques have been implemented and tested using the S-Tools software package. The original and stego-images both are shown for the purpose of comparison.

Keywords: *image based steganography, message concealment, LSB insertion*

1. INTRODUCTION

Steganography as defined in [1] is the art of hiding information in ways that prevent the detection of hidden messages. Steganography is a process that involves hiding a message in an appropriate carrier e.g., an image, an audio or video file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. [2] Literally meaning “covered writing”, it includes a wide range of secret communication methods like invisible inks, microdots, character arrangement, digital signatures, covert channels, spread spectrum etc. that conceal the very existence of

message. [1]. Cryptography and steganography are related to each other. The main difference between cryptography and steganography is that cryptography scrambles the message so that it becomes difficult to understand whereas steganography hides the very existence of a message. Steganography plays the central role in secret message communication. Several message hiding techniques have been developed and implemented in the past using digital images, audio/video files and other media. [1] [2]. These include least significant bit insertion, masking, filtering and algorithmic transformations to name a few.

In this paper, two new techniques are presented for hiding messages in image files using punctuation marks and modified scytale cipher.[3] These techniques are based on the simple idea of adding an extra layer of confusion before steganography by changing the representation of message and hiding it in the embedded message in different ways. These two methods are implemented using a popular steganography software S-Tools which is based on LSB insertion.[4]

In the following sections, first a brief description of concepts and available methods is presented followed by a detailed description of proposed techniques and their implementation results.

2. IMAGE BASED STEGANOGRAPHY

Embedding a message into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the *cover image*. The second file is the message—the information to be hidden. A message may be plain-text, cipher-text, other images, or anything that can be embedded in a bit stream. When combined, the

cover image and the embedded message make a *stegoimage*. A stego-key (a type of password) may also be used to hide then later decode the message. Most steganography software recommends the use of lossless 24-bit images such as BMP. The next-best alternative to 24-bit images is 256-coloror gray-scale images. The most common of these are GIF files. [1]

3. PREVIOUS WORK

[1] discusses three popular methods for message concealment in digital images namely LSB insertion, masking and filtering and algorithmic transformations. *LSB insertion* is a simple approach to embedding information in a cover file. It is vulnerable to even a slight image manipulation. Image conversion from a format like GIF or BMP which reconstructs the original message exactly (lossless compression) to a JPEG which does not (lossy compression) and then back could destroy the information hidden in the LSBs. LSB insertion can be performed in 24-bit, 8-bit or gray-scale images. *Masking and Filtering* usually restricted to 24-bit and gray-scale images, hide information by marking an image, in a manner similar to paper watermarks. Watermarking techniques may be applied without fear of image destruction due to lossy compression because they are more integrated into the image. Traditional steganography conceals information; watermarks extend information and become an attribute of the cover image. Digital watermarks may include such information as copyright, ownership, or license. *Algorithmic Transformation* techniques like redundant pattern encoding, encrypt and scatter etc. exist which use different approaches for concealing messages. In *redundant pattern encoding*, a small message may be painted many times over an image so that if the stegoimage is cropped, there is a high probability that the watermark can still be read.

In *encrypt and scatter* the data are hidden throughout an image. Scattering the message makes it appear more like noise. Proponents of this approach assume that even if the message bits are extracted, they will be useless without the algorithm and stego-key to decode them.

[2] analyzes and evaluates seven different image based steganography methods namely Steo1bit, Stego2bits, Stego3bits, Stego4bits, StegoColourCycle, StegoPRNG, StegoFridrich. *Stego1Bit* method involves utilizing a single least significant bit of one of the RGB bytes of a 24-bit image for message concealment. As the color value is not changed much, it will not considerably alter the visual appearance of color and image. *Stego2Bits* method involves utilizing two least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 2 times improved than Stego1Bit, the resulting image is degraded than Stego1Bit. *Stego3Bits* method involves utilizing three least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 3 times improved than Stego1Bit, the resulting image is much degraded than Stego1Bit. *Stego4Bits* method involves utilizing four least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 4 times improved, the resulting image is much degraded than Stego1Bit and color palette is restricted to only 16 variations. *StegoColourCycle* method involves cycling through the color values in each of the pixels in which to store the data. This means that the same color is not constantly changed e.g., the first data bit could be stored in the LSB of the blue value of the pixel, the second data bit in the red value and the third data bit in the green value. *Stego1BitPRNG* method involves using a pseudo random number generator

to choose random pixels in which to embed the message. This will make the message bits more difficult to find and reduce the existence of patterns in the image. *StegoFridrich* method involves searching for the closest color to the color of the pixel which has the correct parity for the bit to be hidden. The message is hidden in the parity bit of the RGB values of close colors. For the color of each pixel into which a message bit is to be embedded the closest colors in the palette are searched until a palette entry is found with the desired parity bit. This technique does not change the palette in any way either by ordering it or by increasing the colors in it.

[5] & [6] also present several methods for image based and multimedia based steganography.

4. MESSAGE CONCEALMENT TECHNIQUES

The message concealment techniques proposed in this paper are described below:

4.1 Use of Punctuation marks

Although punctuation marks are used in normal written English, they are seldom used in secretly embedded messages. The idea behind this technique is to utilize the presence of punctuation marks like , ; : “ etc. in the text for encoding a secret message. The message is encoded using any convenient character code like ASCII, Unicode. In all the examples in this paper, ASCII code has been used. The secret message to be communicated is hidden in any piece of text through binary encoding of punctuation marks. Two punctuation marks can be used to represent binary data or several punctuation marks can be used to represent binary combinations. The encoded message is embedded in an image file (BMP, GIF or grayscale) using any of the popular methods

like LSB insertion etc. [1] An additional layer of secrecy can be added by first encrypting the message and then encoding it through the use of punctuation marks before embedding it in the cover image file. Only the recipient who knows how to interpret the punctuations marks can retrieve the secret message.

Following are the steps for applying the above technique:

- Encode the given secret message using punctuation marks into the embedded message
- Embed the message in a cover image to create a stego-image using some transformation
- Extract the embedded message using the reverse transformation
- Decode the secret message from the embedded message

As an example of the above technique, consider the secret message “Pershing sails from NY June 1”. The embedded message whose punctuation marks represent our secret message is the following:

OFT, I had heard of Lucy Gray;
And, when I crossed the wild;
I chanced, to see, at break of day,
The solitary child,

No mate, no comrade; Lucy knew,
She dwelt, on a wide moor,
The sweetest thing; that ever grew,
Beside a human door;

You, yet may spy the fawn; at play,
The hare; upon the green,
But, the sweet face of Lucy Gray;
Will never more be seen,

"To-night, will be a stormy night--;
You, to the town must go;
And, take a lantern, Child to light;
Your mother through the snow";

"That, Father; will I gladly do,
'Tis scarcely afternoon--,
The minster-clock; has just struck two,
And, yonder is the moon!",

At this, the Father raised his hook;
And, snapped a faggot-band,
He plied his work;--and Lucy took,
The lantern, in her hand;

Not blither, is the mountain roe;
With, many a wanton stroke,
Her feet; disperse the powdery snow;
That rises up; like smoke,

The storm, came on before its time;
She wandered, up and down,
And, many a hill did Lucy climb;
But; never reached the town;

The wretched parents, all that night;
Went shouting, far and wide;
But, there was neither sound, nor sight;
To serve them for a guide;

At day-break, on a hill they stood;
That, overlooked the moor,
And, thence they saw, the bridge of wood,
A furlong from their door;

They wept,--and; turning homeward, cried,
"In heaven we all shall meet;"
--When in the snow, the mother spied,
The print of Lucy's feet;

Then, downwards from the steep hill's edge;
They tracked, the footmarks small,
And; through the broken hawthorn hedge;
And, by the long stone-wall,

And, then an open field they crossed;
The marks, were still the same;
They tracked them on, nor ever lost,
And; to the bridge they came;

They followed, from the snowy bank;
Those footmarks, one by one,
Into the middle, of the plank;
And; further there were none,

--Yet, some maintain; that to this day,
She is a living child;
That, you may see sweet Lucy Gray,
Upon; the lonesome wild,

O'er, rough and smooth she trips along;
And, never looks behind,
And; sings a solitary song;
That; whistles in the wind;

I WANDER'D, lonely; as a cloud,
That, floats on high o'er vales and hills;
When, all at once I saw a crowd;
A host, of golden daffodils;
Beside, the lake, beneath the trees;
Fluttering; and dancing; in the breeze,

Continuous, as the stars; that shine,
And; twinkle on the Milky Way;
They, stretch'd, in never-ending line;
Along, the margin; of a bay,
Ten thousand, saw I; at a glance,
Tossing their heads; in sprightly dance,

The waves, beside them danced; but they,
Out-did; the sparkling waves, in glee;
A poet, could not but be gay;
In, such a jocund company;
I gazed,—and gazed, —but little thought;
What wealth; the show to me; had brought,

For oft, when on my couch; I lie,
In, vacant, or in pensive mood;
They, flash upon that inward eye;
Which is, the bliss of solitude,
And; then my heart; with pleasure fills,
And, dances, with the daffodils;

In the above message, a comma(,) represents zero(0) and a semicolon represents one(1). Scanning the message and substituting a comma by 0 and semicolon by 1 gives the ASCII representation of the secret message. This prepared message is now embedded in an image file to create the stego-image using S-Tools software package. The original cover image is shown in Fig.1 and the stego image is shown in Fig. 2.

Figure 1. Original Cover Image (in BMP format)

Figure 2. Stego-Image containing secretly embedded message

The secret message is revealed by extracting the embedded message and applying the decoding as explained above. The decoding of the embedded message reveals the secret message “Pershing sails from NY June 1”.

4.2 Modified Scytale Cipher

In cryptography, a scytale (rhymes with Italy, and also transliterated as skytale, in Greek, a baton) is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of leather wound around it on which is written a message. The ancient Greeks and the Spartans in particular, are said to have used this cipher to communicate during military campaigns. The recipient uses a rod of the same diameter on which he wraps the paper to read the message. It has the advantage of being fast and not prone to mistakes, a necessary property when on the battlefield. [3]. Although Scytale cipher is easily broken, it can be used in combination with image based steganography to perform message concealment.

Following are the steps to carry out this technique of message concealment.

- Arrange a message on a rectangular array of some size e.g., 4x16 as shown in Figure 3.
- Fill the remaining cells of the grid with arbitrary letters or numbers and note down the row number and column number of the secret message.
- Embed this data array linearly in a cover image file.

A	E	I	M	Q	U	Y	**S**	**A**	1	5	9	D	h	l	p
B	F	J	N	R	V	Z	**e**	**r**	2	6	a	E	i	m	q
C	G	K	O	S	W	0	**n**	**m**	3	7	b	F	j	n	r
D	H	L	P	T	X	1	**d**	**y**	4	8	c	G	k	O	s

Figure 3. A rectangular grid containing a secret message “Send Army” at (row,col)=(1,8)

Only the recipient who knows the grid size, row and column number can retrieve the hidden message. In order to increase the level of confidentiality the message can be encrypted using some encryption algorithm like AES and the cipher text as well as the key can be arranged in different manner using two different grids. As an example of this technique, consider the linear representation of above grid data using ASCII Code.

4145494D5155595341313539646 86C7042464A4E52565A657232366165696D714347B

4F5357306E6D333762666A6E7244484C505458316479343863676B6F73

Figure 4. Cover image (GIF format)

Figure 5. Stego-image containing embedded message

The secret message is revealed from the above message by extracting the hidden message and applying the transformation as mentioned above.

5. S-TOOLS SOFTWARE PACKAGE

The software tool used in all the above experiments is S-Tools for Windows Version 4.[4] It allows processing of GIF and BMP images and audio WAV files. S-Tools applies the LSB method for image and audio files and also includes encryption routines. The message to be embedded is first compressed. The compressed output is then encrypted using IDEA using a stego-key and inserted into the low-order bits of each color value. As observed in the above stego-images, the existence of the message is almost invisible.

6. CONCLUSION

In this paper two techniques are described for message concealment using image based steganography. Both of these techniques add an additional layer of confusion before actually hiding the message into the cover image in order to make the message revealment difficult against steganalysis. They have smaller capacity of storing bits of message as compared to other image based steganography methods. The capacity of the above mentioned techniques can be increased by efficient encoding of data or using encryption. The advantage of these techniques is that they can be easily implemented using any available steganography software package without any modification. Also both of these techniques incorporate very simple ideas along with the use of available software.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography, Seeing the Unseen," *IEEE Computer Magazine*, 1998.

[2] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence*, Fall 2003 Voulme 2 Issue 2.

[3] Wikipedia, the Free Encyclopedia

http://en.wikipedia.org/wiki/Main_Page

[4] Andy Brown, S-Tools for Windows, Shareware, 1994

ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools3.zip

[5] Johnson Neil F., Zoran Duric, Sushil Jajodia, "Information Hiding, and Watermarking - Attacks & Countermeasures," Kluwer 2001.

[6] "Multimedia Security – Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, " Idea Group 2005.