Message Embedding In PNG File Using LSB Steganographic Technique

Wai Wai Zin

University of Computer Studies
Mandalay, Myanmar
waiwaizin.ucsmmdy@gmail.com

Abstract: ***Many types of Internet-based applications have been used for centuries to be secure important information and data. In some case, the communication is necessary to be secret. Consequently, the security of information has become a fundamental issue. In this paper, an image steganographic technique is presented by combining cryptographic and steganographic techniques. This system uses LSB-based data embedding technique to hide the encrypted message. Before embedding the secret message, RC4 algorithm is also used for message encryption. In this system, BBS (Blum Blum Shub) Pseudo Random Number Generator is used for generating the random sequences and then the secret messages can be hidden in PNG image file by using random sequences. This system is intended to emphasis on digital applications, focusing on hiding information under PNG image file.***

Keywords: Image Steganography, Data Hiding, LSB technique, RC4.

1. Introduction

The security of information can be achieved by using encryption and information hiding. In cryptography, encrypted data is transmitted after transforming the other form instead of the original data. Contrast cryptography, information hiding process can be extended for protecting from the interesting of any attacker. This paper proposes the security system by combining these two techniques. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker detects the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message [1].

There are many encryption algorithms but RC4 encryption algorithm is used for data confidentiality in this system. In RC4 algorithm, encryption is about 10 times faster than DES and a particular RC4 key can be used only once. After enciphering the plaintext (original message), these encrypted messages are embedded in PNG image file by using LSB steganographic technique. Least Significant Bits (LSB) insertion is a simple approach to embed secret information in image file. Altering the LSB will only cause minor changes in color, and thus is not usually noticeable to the human eye. This system improves the security of the data by embedding the encrypted text (ciphertext) and not the plaintext in an image.

This paper is organized as follows. Section 2 contains the related works. Section 3 gives the background theory about LSB steganographic technique. Section 4 describes the steganographic method in PNG image file. Design and Implementation for this system is illustrated in section 5. Finally, conclusion is described in section 6.

2. Related Works

Nowadays security has become one of the most significant problems for information technology. Many users want their information to be secure. Cryptography and steganography can solve this issue. In [6], Mamta Juneja , et al presented a technique for LSB steganographic insertion. They described a technique to embed data in an 8 bit color image. The 24 bit bitmap file was compressed by 8 bit colormap. They discussed that this 8 bit color insertion technique provide a good starting point for anyone interested in learning about steganography.

In [7], Neha Sharma et al. proposed a system that combines the effect of two methods such as cryptography and steganography to enhance the security of data. The authors also used MD5 hashing algorithm to provide the integrity of message contents. They can't evaluate their system by steganographic tools. Allam Mousa and his partner predicted the performance of the RC4 algorithm in [8]. To predict the performance they used various encryption key length and file size. In [9], the authors explained LSB embedding technique and presented the evaluation for various file formats. They don't analyze their techniques with other steganographic techniques.

3. LSB Steganographic Technique

This technique is to embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in a human perceptible difference because the amplitude of the change is small. The implementation of LSB method is quite easy and it is a popular method. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. Digital image steganography is accomplished by using a common principle called least significant bit insertion. Each pixel contains a number of bytes that describe the color and appearance of the pixel. Depending on the resolution of that image, there are a set number of bytes for each pixel. When the LSB are removed from an image, it can be viewed as a gradient of redundant bits that resembles a black and white star burst. These bits are not really necessary for the integrity

of the photography so these are the bits that are manipulated [2].

There are many insertion techniques in LSB. They are 1-bit insertion, 2-bit insertion, 3-bit insertion and 4-bit insertion [3]. In this paper, 1-bit LSB insertion algorithm has been used. This 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 [3].

In this system, a PNG image file is used as a carrier to hide message. Least Significant Bit (LSB) insertion [4] is a simple approach for embedding information in image file. LSB technique is the most popular steganographic technique employed with graphics image files.

3.1 Pros and Cons of LSB Insertion

The advantages of LSB embedding are its simplicity and many techniques use these methods. It is easy to understand and comprehend to employ. LSB embedding is also allowed the high perceptual transparency. It gives the low degradation in the image quality and growingly commercial software is available which follow this approach.

However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc [9]. Furthermore, an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [4].

4. LSB Data Hiding Technique in PNG

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 [5].

In this system, PNG image file is used as a container file. PNG, the Portable Network Graphics, format was designed to replace the older and simpler GIF format. PNG supports for indexed colors, gray-scale, and RGB (millions of colors). An image in a lossless PNG file can be 5%-25% more compressed than a GIF file of the same image. PNG does not support animation like GIF does. PNG is designed to work well in online viewing applications, such as the World Wide Web.

4.1 Structure of PNG Image File

A PNG file starts with an 8-byte signature. The hexadecimal byte values are 89 50 4E 47 0D 0A 1A 0A [10].

After the header comes a series of *chunks*. A chunk consists of four parts: length (4 bytes), chunk type/name (4 bytes), chunk data (length bytes) and CRC (cyclic redundancy code/checksum; 4 bytes).

Table 1: File Header of PNG

Bytes	*Purpose*
89	Has the high bit set to detect transmission systems that do not support 8 bit data and to reduce the chance that a text file is mistakenly interpreted as a PNG, or vice versa.
50 4E 47	In ASCII, the letters PNG, allowing a person to identify the format easily if it is viewed in a text editor.
0D 0A	A DOS-style line ending (CRLF) to detect DOS-Unix line ending conversion of the data.
1A	A byte that stops display of the file under DOS when the command type has been used—the end-of-file character
0A	A Unix-style line ending (LF) to detect Unix-DOS line ending conversion.

Table 2: Chunks within the PNG File

Length	*Chunk type*	*Chunk data*	*CRC*
4 bytes	4 bytes	Length bytes	4 bytes

PNG images can either use palette-indexed color or be made up of one or more channels. Since multiple channels can affect a single pixel, the number of bits per pixel is often higher than the number of bits per channel, as shown in the illustration at figure-1.

Bits per pixel						
Color option	Channels	Bits per channel				
		1	2	4	8	16
Indexed	1	1	2	4	8	
Grayscale	1	1	2	4	8	16
Grayscale & alpha	2				16	32
Truecolor	3				24	48
Truecolor & alpha	4				32	64

Figure 1. PNG color options

The number of channels will depend on whether the image is grayscale or color and whether it has an *alpha channel*. PNG allows the following combinations of channels, called the *color type*. The color type is specified in the color type field, which is a *bit field*, as explained in the following figure-2.

Color type	Name	Binary				Masks
			A	C	P	
0	Grayscale	0	0	0	0	
1	(Indexed grayscale)	0	0	0	1	palette
2	Truecolor	0	0	1	0	color
3	Indexed	0	0	1	1	palette
4	Grayscale & alpha	0	1	0	0	alpha
5	(Indexed grayscale & alpha)	0	1	0	1	palette
6	Truecolor & alpha	0	1	1	0	color
7	(Indexed & alpha)	0	1	1	1	color | palette

Figure 2. PNG color types

5. Design and Implementation of Proposed System

5.1 Overview System Design

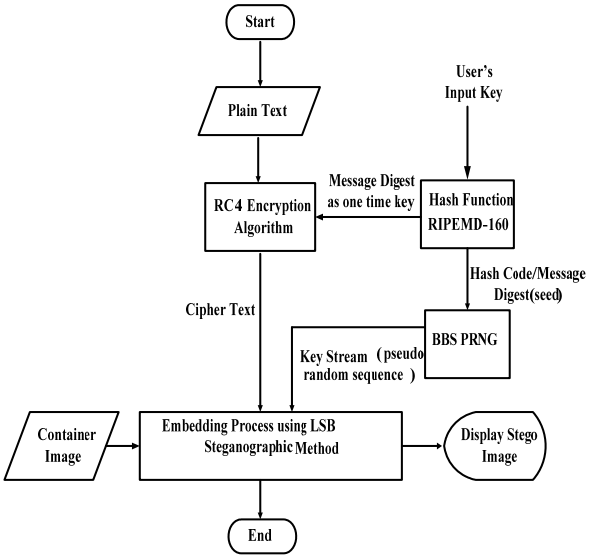

Figure 3. Overview of Data Embedding Process

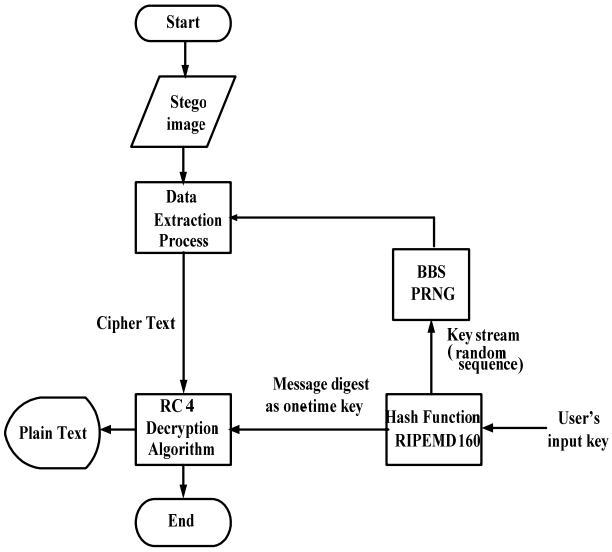

Figure 4. Overview of Data Extraction Process

By combining cryptography and steganography, this system can support to develop the information security. There are many encryption algorithms but RC4 encryption algorithm is used in this system for data confidentiality. After encrypting the plain text (original message), these encrypted messages are embedded in PNG image file by using LSB method. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. The embedding process is based on pseudorandom number generator. Blum Blum Shub (BBS) generator is used in this system to generate the random sequences. According to these random sequences, encrypted messages are embedded in PNG image file. In this method, message may be embedded to 1-LSB of container image if random sequence generates "1" as PRNS. In contrast, the message can be embedded to 2-LSB of container image.

5.1 Implementation of the Proposed System

This system has two main parts: Hide and Reveal. Hide process is shown the following figure-5. Firstly, we choose container PNG image file and then select message file. This system uses RIPEMD-160 hash algorithm for data encryption and message digest. Message Digest is used for hiding message process. After hiding, data is hidden in the previous choosing image file.

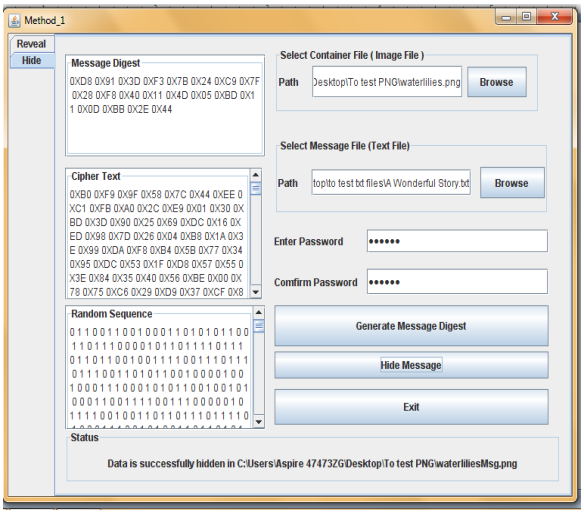

Figure 5. Hiding Process

Revealing process is shown in figure-6. To extract hidden data from image, message digest and random sequences are used. The result of this system can be seen by figure-7. The original image and stego image are similar. Therefore, any attacker can't know easily hidden data is embedded in image file.

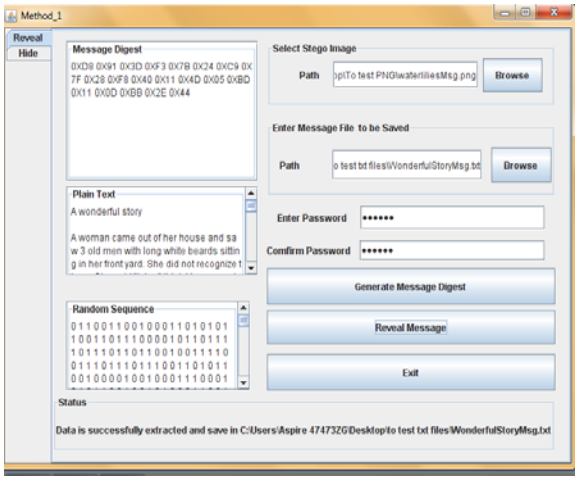

Figure 6. Extraction Process

Waterlilies.png WaterliliesMsg.png

Figure 7. Original Image and Stego Image

6. Conclusion

By combining cryptographic and steganographic techniques, we tried to enhance the security of this system. In this paper, we described well known steganographic techniques used to hide secret messages in stego objects that use the least significant bit insertion method. For message encryption, RC4 algorithm is used before embedding the message. This system uses BBS generator to generate random number sequences. According to these sequences, secret messages can be hidden in PNG image file. If an attacker wants to get the original messages, he must know secret key and random sequences. This system can be used for many applications in computer science and other related fields.

References

[1] D.Stinson, "Cryptography: Theory and Practice", second edition, CRC Press, Boca Raton, 1995.

[2] P.Singh, Balkrishan, "Java implementation of Least Significant Bit Embedding for Hiding Data", IE(I) Journal-CP

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

[4] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh, Mohd Rozi Katmin, " Information Hiding Using Steganography", Department of Computer System & Communication Faculty of Computer Science and Information System, University Technology Malaysia, 2003

[5] Namita Tiwari, Dr.Madhu Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, September 2010

[6] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Inssertion and Encryption", 2009 IEEE

[7] Neha Sharma, Mr.J.S.Bhatia, Dr (Mrs) Neena Gupta, "An Encrypto Setgo Technique based secure data transmission system", PEC, Chandigarh, May, 2005

[8] Allam Mousa, Ahmad Hamad, "Evaluation of the RC4 Algorithm for Data Encryption", International Journal of Computer Science & Applications vol-3, No.2, June 2006.

[9] V. Lokeswara Reddy, Dr .A. Subramanyam, Dr .P. Chenna Reddy, " *Implementation of LSB Steganography and its Evaluation for Various File Formats*", Int.J.Advanced Networking and Applications, Volume: 02, 2011

[10] "PNG Image File Format": http:// en.wikipedia.org/wiki/Portable_Network_Graphics

Author Profile

Wai Wai Zin received the B.C.Tech anad M.C.Tech degrees from University of Computer Studies, Mandalay in 2002 and 2006, respectively. From 2006, she served at Computer Univesity (Myitkyina) as an Assistant Lecturer. Now she is a PhD candidate at University of Computer Studies, Mandalay. Her interested fields are cryptography and steganography.