Comparative Study of Different Steganographic Techniques

AKRAM M. ZEKI[1], ADAMU A. IBRAHIM[2] AZIZAH A. MANAF[3] AND SHAHIDAN M. ABDULLAH[4]

[1, 2]Faculty of Information & Communication Technology,
International Islamic University Malaysia, Malaysia, MALAYSIA

[3, 4]Advanced Informatics School (AIS),
University Technology Malaysia, MALAYSIA

[1]akramzeki@iium.edu.my, [2]adamuabubakar9@gmail.com [3]azizah07@ic.utm.my [4]mshahidan@utm.my

Abstract: - Steganography is the method of hiding data in such a way that no one, except the sender and the intended recipient, expects the existence of the hidden data. Thus the goal here is always to conceal the very existence of the secret data embedded in an innocent data in such a way that it will be undetectable, robust and the innocent data should be able to accommodate high capacity of the secret data. When it comes to the pro and cons of various Steganographic software, many have been designed; each of them has different features and capabilities for data hiding, hence, this makes it a wide and attractive field for further research, in which the establishment of innovative methods and techniques could be done. Different Steganographic techniques were studied; experiment was carried out using five Steganographic software. Finally comparison was done using benchmarking tool for identifying different performance aspects of the Steganographic techniques and Steganographic software like visual quality, performance indices, memory requirement and the evaluation of the maximum capacity for each software under this study. Experimental results show that all the software under this study performs above optimal level, although there are some differences of features and capabilities observed.

Key-Words: - Steganography, Steganographic Software, Information Hiding, Steganographic tools, PSNR

1 Introduction

Information is vital to human effort; indeed digital information offers wonderful opportunities and improvements to human life, especially with the advent of internet. The internet has become the most important source of information, which offers ubiquitous channels to deliver and exchange information.

The term Steganography which was earlier described as Steganographia first appears in a manuscript by Johannes Trithmius that started in 1499 [1]. The goal here is to hide data inside other harmless data in way that does not allow any suspicious present of the hidden data so that it can be used as a medium for transmission of secret information. Embedding secret data, into harmless data requires the presents of the two files. The first is the innocent-looking file that will hold the hidden information called the host file. The second file is the secret message. A message may be plaintext, cipher text, or any bit stream. When combined, the host file and the embedded message make a Stegofile.

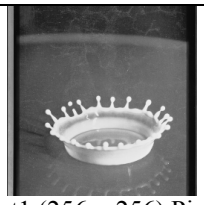
Although many information hiding techniques have been proposed by various authors, the specific requirements of each Information Hiding technique vary with the application. This study aims at providing a test to outline the best and current Steganographic software available, and the most outstanding Steganographic technique.

2 Research Methodology

This study starts with selecting the Steganographic software for the study and studying their features and capabilities. The parameters that will be used for the testing of their differences are also to be evaluated. Then next is the embedding and extracting using the selected software. Performance comparison of each software using the parameters

chosen is the next activity from the research framework.

Six standard Host Images have been selected in this study (Four gray scale images, with size of (256 × 256) Pixels 192 KB, see Figure 1) and (two colors images, with size of (512 × 512) Pixels 768 KB, see Figure 2). In addition one image to be hidden within the host images called logo (with size of (84 × 84) Pixels 20.7 KB see Figure 3) was selected here. All these images are BMP image format.


Host1 (256 × 256) Pixels 192 KB


Host2 (256 × 256) Pixels 192 KB


Host3 (256 × 256) Pixels 192 KB


Host4 (256 × 256) Pixels 192 KB

Figure 1 Gray scale Standard Images for Steganography.


Host5 (512 × 512) Pixels 768 KB


Host6 (512 × 512) Pixels 768 KB

Figure 2. Color Standard Images for Steganography


Logo (84 × 84) Pixels 20.7 KB

Figure 3. Image that will be hidden.

Steganographic algorithm is reliable when it embeds the secret message with little distortion so that it does not affect the quality of the underlying host file. The secret message should be truly undetectable, so that the host file cannot be distinguished from the Stego file. After embedding, distortion normally occurs which in turns affects the Stego file. To ensure that the distortion caused by embedding process is acceptable to Human Visual System (HVS), quality metrics are used to measure the difference between the host file and Stego file. Examples of such metrics are Mean Square Error (MSE), PSNR. The Mean Squared Error (MSE) is the averaged term-by-term squared difference between the input signal (the original image, P) and the output signal (the secret message,P'), as shown in below Equation.

$$\mathrm{MSE} = \frac{1}{\mathrm{N}}\sum^{N}\left(P_i' - p_i\right)^2$$

The PSNR is given in below Equation in which Ppeak is the peak value of the input signal.

$$PSNR(db) = 10\log_{10}\frac{p^2_{peak}}{MSE}$$

Usually 255 for 8 bit Gray scale images [2], [3], the larger the PSNR, the better the image quality will be. Some researchers considered the acceptable quality of Stego image, when the PSNR was greater than 30db [4], [5].

3 Steganographic Software

Almost all Steganographic software comes with their strengths and weaknesses, and they are mostly based on different techniques and algorithms. It's a fact that each Steganographic software has been designed by different company, and developed by different programming language. Some are available in the internet free for academics purposes, while some are for home use or businees use, and other comes as part of security suite software.

This study aimed at comparing the features and capabilities of most popular and current Steganographic software available. Five Steganographic software have been selected. Six host images, four gray scale images and two color images are the images considered for this research as indicated in Figure 2 and 3. The host images are the standard images for Steganography and they were downloaded from the internet. They can be found in many websites. The software selected for the comparisons are: Invisible Secrets 4, Hermetic Stego 8.04, Puffer 4.04, Xiao Steganography 2.6.1, and S-Tools

Invisible Secrets 4 is a powerful security suite that can hide and encrypt files, also can destroy internet traces, shred files, make secure IP-to-IP

ISBN: 978-1-61804-039-8

password transfer and even lock any application on the computer. It is an easy to use with a powerful wizard interface. It was first released in 1999; the latest version is "Invisible Secrets 4" that was released in 2009 by NeoByte Solutions. It accepts five hosts file formats Steganography applications, which are: JPG, PNG, BMP, HTML and WAV.

Puffer version 4.04 was released as a revised version of Puffer 4.03 in 2009. It is a general purpose encryption and Steganographic software that is used to protect most sensitive data from unauthorized viewing to securely exchange message or email with other Puffer users. It hides data among the pixels of image, and distributes self-decrypting archives to non-Puffer users. Extensive wiping options are also available to permanently erase sensitive data. Puffer runs on all 32-bit versions of Windows from 98 through Vista. Puffer 4.04 has displayed the ability to hide encrypted archives among the pixels of 24-bit color image, specifically PNG and BMP files.

Xiao Steganography 2.6.1 is developed by nakasoft (www.nakasoft.net) in Venezuela. It is easy to use and powerful wizard interfaced. It was released in 2005; it offers an impressive and unique art of hidden writing. It accepts many different types of file. The security level use RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA Algorithms through using password protected.

Hermetic Stego 8.04, is part of Hermetic applications under Hermetic system which was released on 2009. Hermetic Stego is able to hide any type of file within BMP images, with an encryption key, so that the presence of the hidden file is undetectable, if a Stego key has been used when hiding the data then that data can be extracted only by someone who knows that Stego key. The Stego key is used not only to facilitate random selection of bytes for hiding data file bits but also is used to encrypt the data file.

S-tools, was developed by Andy brown in 1996. S-Tools is a Steganography tool that hides files in BMP, GIF, and WAV files. It can hide multiple files in one sound/picture and the data is compressed before being encrypted and then hidden. Multi-threaded operation means that the user can have many hide/reveal operations going simultaneously without fear of them interfering with other work. The user can even close the original picture/sound with no ill effects to ongoing threads. S-Tools uses the spatial domain technique and works by spreading the bit-pattern of the file that will be hidden across the least significant bit. S-Tools uses four encryption options (IDEA, DES, Triple DES and MDC) that give an additional security level to its operation. After embedding the message, normally distortion occurred which in turns affect the Stego image. Table 1 shows the software's features.

Table 1. The Steganographic software features used in this study.

Steganograp-hic Software	Software Size	Software Description	Software Creator	Software Sources
Invisible Secrets 4	2.7 MB	Security suite software that can hide files, encrypt files, destroy Internet traces, shred files, make secure IP to IP password transfer and even lock any application on the computer	NeoByte Solutions	1. http://www.invisiblesecrets.com/download.html
Hermetic Stego 8.04	2.30MB	Uses encryption and hiding technique to hide files of any type and of any size in BMP images, with or without the use of a user-specified Stego key	Hermetic system	1. http://www.hermetic.ch/hst/hst.htm
Puffer 4.04	1.90MB	It a security is general purpose encryption and Steganographic software; with Extensive wiping opti ons are also available to permanently erase sensitive data.	Briggs Softwors	1. http://www.soft32.com/download_7842.htm
Xiao Steganography 2.6.1	2.14MB	It is security software that implements cryptography/Steganography. It offers unique art of encry pting and hidden files. It can Includes attach any file, doesn't matter the type of file (limited by the size of host image)	Nakasoft	1. http://download.cnet.com/XiaoSteganography/30002092_410541494.html
S-Tools	561 KB	It is a Steganography that hide files in BMP, GIF, and WAV files. And also uses some encryption technique as an added layer of security.	Andy brown	1. http://www.jjtc.com/Security/Stegtools.htm

ISBN: 978-1-61804-039-8

The features of the software under this study were represented in table 2; they all come with Graphical User Interface (GUI), some come in collection of security applications while others are specifically for Steganographic use only. The capabilities of the software (The Image format, Capacity, Cryptographic algorithm and Steganographic techniques).

Table 2. Capabilities of the Steganographic software under this study

Steganographic Software	Host Image Formats	Software Capacity	Memory Usage	Encryption Support	Steganographic Algorithm
Invisible Secrets 4	BMP, JPG, PNG	12.80%	10.104 KB	AES-Rijndael, Twofish, RC4, Cast128, GOST, Diamond 2, Sapphere II, and Blowfish	least significant bits (LSB) algorithm
Puffer 4.04	BMP, JPG, PNG, GIF	38.40%	4.512 KB	AES encryption algorithm	least significant 3 bits (Intermediate bit)
Xiao Steganography2.6.1	BMP	12.50%	6.256 KB	RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA	least significant bit (LSB) substitution
S-Tools	BMP, GIF, WAV	12.80%	1.224 KB	IDEA, DES, Triple DES and MDC	least significant bit (LSB)

Notice that the capacity refers to the amount of information being able to be inserted into a particular image. In general, increasing the capacity will make the hidden image more obtrusive in viewing.

Measuring the embedding capacity can be done directly by dividing the size of the embedded information on the size the host image.

4 Results

The image quality measure after embedding process, high image quality reflects the success of Steganographic system. PSNR has been used for measuring the quality of image. All host images were converted to BMP format before embedding process for comparison purposes. Table 3 shows the PSNR values after embedding the logo image within the host images using the selected software.

Table 3. PSNR of the software

HOST IMAGES	Invisible Secrets 4	Hermetic Stego 8.04	Puffer 4.04	Xiao Stegano-graphy2.6.1	S-Tools
Host1	51.14	50.81	43.21	51.7689	56.39
Host2	51.14	50.07	49.15	57.7948	62.43
Host3	51.14	50.81	43.15	51.7704	56.40
Host4	51.14	50.85	43.06	51.7911	56.38
Host5	51.14	50.81	43.17	51.7508	56.41
Host6	51.14	50.07	49.15	57.7956	62.43

This study uses a single watermark file to be embedded within all host images using the five different software. Invisible secret 4 reveals that the PSNR were all the same.

The above results, indicates that S-Tools shows better performance, while Puffer 4.04 is the least. While though, all the software's PSNR were above 40 dB, which is above the benchmark for the most high quality Stego image, it still reveals that Hermetic Stego 8.04, Invisible secrets 4, and Xiao Steganography 2.6.1 performance were relatively the same.

The results show that all the software possesses the ability to hide data without noticing changes in their properties, more especially the image size which logically is the second character to be considered to ensure efficiency of hiding system apart from visual inspection of the Stego image. The entire extracted images were clear without any distortion.

ISBN: 978-1-61804-039-8

5 Conclusion

This research presented a background of Steganography and a comparative study of some Steganographic software. Steganography as information security system can have some useful applications, like other seemingly related system (cryptography). The success of this study is to identify the reliable and best software available in the market for Steganography. Some of the software available in the market were selected based on the recent deployment, that is five recently deployed software, these software were tested using the same input on all of them. The tools used in our experiment are images. Specific image was embedded within all host images for each of the five software selected. The results of the experiment reveal that all the five software were relatively performing at the same level, though some software performs better than others. The image quality measure after embedding usually reflects the success of Steganographic system. The tool for measuring the quality of image after embedding is the PSNR. The values of PSNR are obtained using the software under this study were all above the bench mark for the high quality image.

References:

[1] Arnold, M. K., Schmucker, M., & Wolthusen, S.D. (2003). Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Norwood, Massachusetts.

[2] Joachim, J., Eggers, J. & Bernd, G. (2000). Robustness of a blind image watermarking scheme. ICIP 2000, Special Session on WM. Sep. 10–13. Canada.

[3] Stefan, W., Elisa, D. & Gelasca, T. (2002). Perceptual quality assessment for video watermarking. Proceedings of International Conference on Information Technology: Coding and Computing (ITCC). April 8-10. Las Vegas, NV.

[4] Wu, N. (2004). A Study on Data Hiding for Gray-Level and Binary Images. Master Thesis. Chaoyang University of Technology, Taiwan.

[5] Bennour J. Dugelay J. L. & Matta, F. (2007). Watermarking Attack: BOWS contest. Proceedings of SPIE.