SilentSecrecy: Hiding in Image and Audio Using Spread Spectrum Technique with an Image Stenalysis Plug-In

Moo Chui Lih,
University of Kuala Lumpur, 1016, Jalan Sultan Ismail, Kuala Lumpur
moo.virgo13@gmail.com

Delina Beh Mei Yin
University of Kuala Lumpur, 1016, Jalan Sultan Ismail, Kuala Lumpur
delina@unikl.edu.my

Nurul Sharaz Azmanuddin
University of Kuala Lumpur, 1016, Jalan Sultan Ismail, Kuala Lumpur
nsharaz@unikl.edu.my

Abstract -This paper presents a proposed scheme which employs a steganography technique to hide and retrieve data or file along with steganalysis technique to analyse suspicious image file. Due to the growth of technology, people tend to keep information electronically. Private information can be obtained by unauthorised use without knowing. With the usage of both steganography and encryption method, the unauthorised user might have difficulty on getting user private information. On the other hand, steganalysis is an ill-posed problem. The original host data is unknown, the rate of hiding (if data is hidden) is not known and the number of steganography scheme is large. In this research, it will clarify what steganography is, the definition, the technique used in implementing steganography as well as steganalysis. This study focuses on the Spread Spectrum technique in hiding data or file in a media file (MP3 and JPEG) and statistical steganalysis technique that is Chi-Square attack. The proposed scheme is then analysed and evaluated the payload size, stego image resolution and the occurrence of hidden data in an image file. The significance of the proposed scheme is the user can embed and retrieve secret data from media file, while Chi-Square attack able to analyse the hidden message in an image.
Keyword: steganography, steganalysis, audio, chi-square attack, image, data hiding.

1.INTRODUCTION

Due to the availability of Internet throughout the world, in underdeveloped as well as developed countries, content security is playing a major role in multimedia communication. Since the commercial activities are used in the same Internet channels, the information has been coded before transmitting through the network has become one of a common practice to overcome the cyber illegal action which known as hacking. One of the reasons that intruders can be successful is that most of the information can obtain from the system that is in a readable form and can be comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. There are techniques that can be used to overcome this, which are by using steganography, cryptography and encryption. Steganography is a technique of hiding information in digital media file. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep the information invisible, while encryption encodes the information so that an unauthorized user cannot determine its intended meaning. A better private communication can be allows by combining encryption and steganography Although steganography can hide information but the hidden information can be analyse by using steganalysis techniques. Steganalysis is the detection of the existence of hidden information. Hence, like cryptography and cryptanalysis, the goal of steganalysis is to determine hidden information and to break the security of its carriers. It also can be explain that steganalysis serves a method to judge the security performance of steganography techniques

2.RELATED WORKS

Steganography is the art of invisible communication of messages which mean that hiding information in other information. The methods that being used in steganography can reduce the possibility of a message being detected. It provides extra layer of protection by encrypting the message. Thus, some steganography methods are combining with cryptography techniques. Sender has to encrypt the secret message first for the whole communication process, this way the attacker may have difficulties on detecting the embedded text in a cover [1].

The most common file formats used in steganography is image. Due to the possibility to access any pixel of the image at random, they are known for constituting a non-casual medium [2]. Image compression techniques are extensively used in steganography. Lossy compression and lossless compression are the two types of image compression. Example of lossy compression format is JPEG (Joint Photographic Expert Group) format files while lossless compression formats are GIF (Graphics Interchange Format) and BMP (Bitmap) formats [3]. Without changing its visible properties, message can be hide in an image. The cover source can be altered in “noisy” areas with many colour variations, so less attention will be drawn to the adjustments [4].

Other than image steganography, audio steganography is one of the types of digital steganography that can hides secret data into digital audio files such as WAV, WMA and MP3 files format etc. [5]. Human Auditory System (HAS) is being used in audio steganography. With the weakness of Human Auditory System, information can be hiding in the audio. That is, while using digital audio when it comes to low and high of sounds intensity, one can count on the different sensitivity of human ear. Lower sounds are less perceived than the high ones. Thus, it is easier to hide data among low sounds without the human ear become aware of the alteration [6].

Steganalysis is the science of detecting the presence of hidden data in the cover media files or also known as medium carries and is emerging in parallel with steganography. Since detection of hidden messages, whether in cipher text or plaintext, can lead to the prevention of disastrous security incidents [7]. Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message, while steganalysis generally begins with several suspect information streams but uncertainty whether any of these contain hidden message. This consider as the challenge of steganalysis [8].

2.1 CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

There are numerous approaches in classifying steganographic techniques. These approaches can be categorize according to the type of covers being used to a secret communication. It also according to the cover modifications applied in the embedding process. In this section, the second approach will be followed. The steganographic techniques are grouped in several categories, but only three categories will be discussed in this section.

A. SPATIAL DOMAIN

This techniques also known as substitution techniques. Which is a group of relatively simple techniques that make a covert channel in the parts of the cover image. When compared to the human visual system (HVS), the changes are likely to be a bit scant [2]. In audio, these techniques hide information on the basis of geometric characteristics of audio signal [9]. The popularity of this techniques is derived from their simple algorithmic nature and ease of mathematical analysis. It is easy to implement, even it provide high payload capacity yet the robustness is weaker than the counter part [10].

B. TRANSFORM DOMAIN

This techniques also known as frequency domain techniques. Information being hide along the frequency distribution of the carrier signal [9]. This techniques often use in compression algorithms and transformation involve hiding secret message in transform space of the cover image [11]. The techniques always work with JPEG images where message is embedded in the transform coefficients of the image [12]. It have an advantage over LSB techniques because it hide information in areas of the image that are less exposed to compression, cropping and image processing [2].

C. SPREAD SPECTRUM

Spread Spectrum is a new technology that can grant better levels of security over other steganographic techniques. The transmitted data signal is being spread over a wide frequency range [5]. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image [2]. The Signal-to- Noise Ratio (SNR) in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely [8]. Spread signals tend to be difficult to remove, embedding methods based on spread spectrum should provide a considerable level of robustness [1]. This technique is similar to LSB but it is more robust against steganalysis techniques [13].

Table 2.1: Comparison of Various Steganography Techniques

METHOD		**ADVANTAGE**	**DISANVANTAGE**
Spatial Domain	Least significant Bit (LSB)	-High embedding rate -simple and easy	-Noticeable to human ear. -Hudden data can easily contaminated even is a small format changes.
	Eco Hiding	-Recover easily from lossy data compression algorithms. -The problem of HAS sensitivity	-Low capacity -Low security
Transform Domain	JPEG Stegnography	-More secure embedding -Difficult to detect visually.	-Difficult to embed the message because of the harsh compression applied.
	Phase coding	-Robus against signal distortion. -phase components of sound are not as perceptible to the human ear as noise is.	-low capacity
Spread spectrum		-offer moderate data transmission rate while maintaining a high level of robustness	-can introduce noise unto a sound file -more vulnerable to time scale modifications.

2.2 Classification of Steganalysis Techniques

Steganalysis is the science of attacking steganography and also the science of detecting hidden information. The main objective of steganalysis is to break steganography and the detection of stego image is the goal of steganalysis [14] [15]. Steganalysis can be classified into two categories: Signature Steganalysis and Statistical Steganalysis

ASIGNATURE STEGANALYSIS

Hiding information within any electronic media using steganography methods requires alternations of the media properties. It may introduce some form of degradation or patterns. These patterns may act as signatures that convey the existence of embedded message [15] [16]. Therefore, a methods to detect the existence of secret message in a suspicious image is by looking for these patterns-signatures of a steganography tool. Such specific signatures will automatically exploit the tool used in embedding the messages [16].

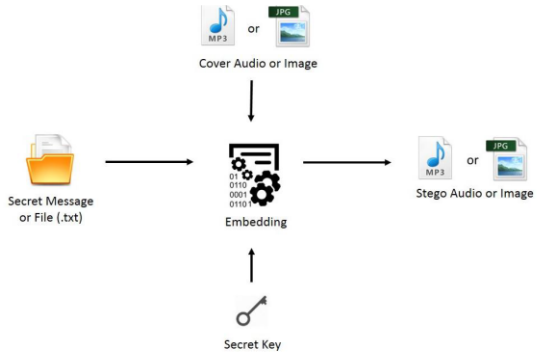
B. STATISTICAL STEGANALYSIS

Statistical steganalysis is more powerful than signature steganalysis, since statistical steganalysis is applied in mathematical techniques and it is more sensitive than visual perception. The secret message that embedded into cover image by using LSB embedding, LSB matching, JPEG compression and other transform domain can be detected by statistical steganalytic tools [15] [16]. Chi-Square Attack developed is based on Pair of Value (PoV). L-bit colour channel can have $P=2L$ possible values. Splitting into $2L-1$ pairs, which differ

only in LSBs gives all possible patterns of neighbouring bits of LSBs. Each of these pair is called PoV. The distribution of odd and even values of PoV is same as 0/1 distribution of secret bit if all available LSB fields are to be used. Chi-square test works well for sequential embedding [15

3. PROPOSED SYSTEM

The proposed system is a standalone two-in-one application, which has two main part which consists both steganography (audio and image) and image steganalysis. In steganography section, there are two processes, which are hiding and retrieving. Basically, the proposed system will work as shown in Fig. 1, 2 and 3.



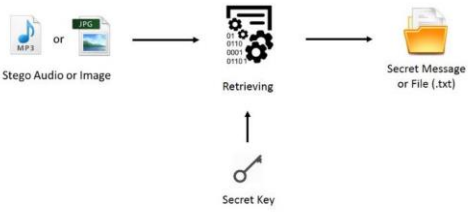


Fig. 2: System diagram on how retrieve process works

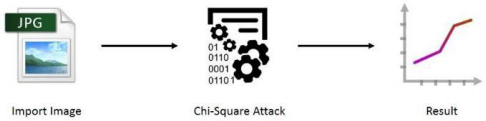


Fig. 3: System diagram on how image steganalysis process works

The application can hide and retrieve mesage or file into media file. Media file such as MP3 audio format and JPEG image format. Password are required to hide and retrieve message or file. Secret message or file, cover audio or image and password will be the input in the hiding process. While the stego audio or image will be the input for the retrieving process. In image steganalysis, a random image (it may contain secret message) will be the input. Image will be analysed by using Chi-Square Attack. Chi-Square attack is one of the statistical steganalysis. Therefore, the result will be shown in line graph.

4.PRELIMINARY RESULT AND ANALYSIS

A. Payload Size

This section shows a comparative for the size of the payload in stego audio and image. In order to observe the size of the stego file, a payload testing has been carried out with two types of secret data that consists of message (plain text) and .txt file. The size of the audio and image file remain unchanged after being embedded with secret data (refer to Fig. 4 and

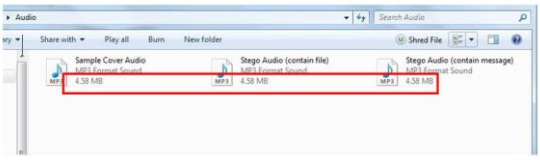


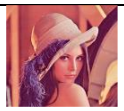
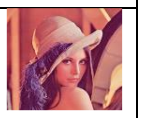
Fig. 4: The Comparison of Capacity between the Cover Audio Used and the Stego Audio Produced

Fig. 5: The Comparison of Capacity between the Cover Image Used and the Stego Image Produced

A. Image Resolution

This section shows the comparison of cover image and stego image resolution. Table 1 shows the resolution between cover image and stego image remain the same.

Table 1: The Comparison of Image Resolution between Cover Image and the Stego Image

Secret data	Cover image	Stego image	Results
Message (plain text)			Appears identical in human eye
.txt file			

5. CONCLUSION AND FUTURE ENHANCEMENT

SilentSecrecy has been introduced in this paper. It is a standalone application, which consists of both steganography and steganalysis. Due to the growth of technology, people tend to keep information electronically. Private information may obtained by unauthorized user without knowing. By using SilentSecrecy, user private data or files can be protected. For future enhancement, it is best enhancement to improve the limitation of SilentSecrey. Which is add more media file format for steganography processes along with audio steganalysis plug-in.

REFERENCES

[1] Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., & Alanazi, H. (2010). Overview: Main fundamentals for steganography. *arXiv preprint arXiv:1003.4086*.

[2] Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, *6*(3), 168-187.

[3] Reddy, V. L., Subramanyam, A., & Reddy, P. C. (2011). Implementation of LSB steganography and its evaluation for various file formats. Int. J. Advanced Networking and Applications, 2(05), 868-872.

[4] Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. World Applied Programming, 1(3), 191-195.

[5] Sharma, A., & Singh, P. (2014). *Semantic Analyzer for Audio Steganography*, *3*(1).

[6] Kekre, H. B., Athawale, A., Rao, S., & Athawale, U. (2010). Information hiding in audio signals. International Journal of Computer Applications (0975–8887) Volume.

[7] Meghanathan, N., & Nayak, L. (2010). Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *international journal of Network Security & Its application (IJNSA)*, *2*(1), 43-55.

[8] Bhattacharyya, S., & Sanyal, G. (2012). Audio Steganalysis of LSB Audio Using Moments And Multiple Regression Model. *International Journal of Advances in Engineering & Technology, IJAET*, *3*(1), 145-160.

[9] Bilal, I., Roj, M. S., Kumar, R., & Mishra, P. K. (2014, December). Recent advancement in audio steganography. In Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on (pp. 402-405). IEEE.

[10] Huayong, G., Mingsheng, H., & Qian, W. (2011, October). Steganography and Steganalysis based on digital image. In Image and Signal Processing (CISP), 2011 4th International Congress on (Vol. 1, pp. 252-255). IEEE.

[11] Kaur, S., Bansal, S., & Bansal, R. K. (2014, March). Steganography and classification of image steganography techniques. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 870-875). IEEE.

[12] Subba Rao, Y. V., Brahmananda Rao, S. S., & Rukma Rekha, N. (2011, April). Secure image steganography based on randomized sequence of cipher bits. In Information Technology: New Generations (ITNG), 2011 Eighth International Conference on (pp. 332-335). IEEE

[13] Wheeler, D., Johnson, D., Yuan, B., & Lutz, P. (2012). Audio Steganography Using High Frequency Noise Introduction. Kuala Lumpur Undergraduate IT Exhibition and Conference (KLTEC 2015)

[14]Bhattacharyya ,S. (2011). A survey of steganography and steganalysis technique in image,text,audio and video as cover carrier. *Journal of global research in computer science*,2(4).

[15] Chanu, Y.J,Singh, K . M., & Tuithung, T . (2012). Image steganography and steganalysis: A survey. International Journal of Computer Applications,52(2).

[16] Nissar,A.,&Mir,A.H. (2010). Classification of steganalysis technique: A study. Digital Signal Processing,1758-170.

