EFFECTS ON QUALITY IN AUDIO STEGANOGRAPHY

HO MAN YEN

Thesis submitted in fulfillment of the requirement of the award of

Degree of Bachelor (Computer Science)

Faculty of Computer System and Software Engineering

UNIVERSITI MALAYSIA PAHANG

2014

EFFECTS ON QUALITY IN AUDIO STEGANOGRAPHY

HO MAN YEN

Thesis submitted in fulfillment of the requirement of the award of

Degree of Bachelor (Computer Science)

Faculty of Computer System and Software Engineering

UNIVERSITI MALAYSIA PAHANG

2014

UNIVERSITI MALAYSIA PAHANG
BORANG PENGESAHAN STATUS TESIS

JUDUL: Effects on Quality in Audio Steganography

SESI PENGAJIAN: 2014/2015

SAYA Ho Man Yen .

Mengaku membenarkan tesis/laporan PSM ini disimpan di Perpustakaan Universiti Malaysia Pahang dengan syarat-syarat kegunaan seperti berikut:

1. Tesis/Laporan adalah hakmilik Universiti Malaysia Pahang.
2. Perpustakaan Universiti Malaysia Pahang dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institut pengajian tinggi.
4. **Sila tandakan (√)

☐ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972) *

☐ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan) *

☑ TIDAK TERHAD

Disahkan Oleh

....

Alamat tetap: 11, Jalan Panchor Indah, Taman Panchor Indah, 14300 Nibong tebal. Pulau Pinang.

Penyelia: LIEW SIAU CHUIN

Tarikh: 26/12/2014

Tarikh: 26/12/2014

*Sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis/laporan ini perlu dikelaskan sebagai SULIT atau TERHAD.

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

STUDENT NAME : HO MAN YEN

STUDENT NUMBER : CA11085

Date : 22nd December 2014

SUPERVISOR DECLARATION

I hereby declare that I have read this thesis and in my opinion this thesis/ report is sufficient in terms of scope and quality for award of the degree of Bachelor of Computer Science (Computer Systems and Networking)

Signature : 

Supervisor Name : DR LIEW SIAU CHUIN

Date : 22nd December 2014

ACKNOWLEDGEMENT

I am grateful and would like to express my sincere gratitude to my supervisor, Dr Eric Liew Siau Chuin for his continuous encouragement, constant support and invaluable guidance in making this report. I am appreciated and thankful for his consistent support from the first day I report to him as my PSM supervisor to these concluding moments. I am truly grateful for his progressive vision about my training in writing progress, his tolerance for my naïve mistakes, and his commitment to my future career and studied. I am sincerely thankful for the time he spent correcting my mistakes throughout this research. Appreciate to all my friends and member staffs of the Faculty Computer System & Software Engineering UMP, who helped me a lot. I acknowledge my sincere thanks and gratitude to my parents for their love, support and sacrifice throughout my life. I cannot find the appropriate words that could properly describe my appreciations for their support, devotion and faith in my ability to achieve my goals.

ABSTRACT

This thesis focuses on effects on quality in audio steganography. Steganography is the science of hiding information, which is used to hiding the data from third party. Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. Embedding information into audio steganography is more secure due to less steganalysis techniques for attacking to audio. Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. Listening test and SNR will be carry out to test the quality between original file and embedded file. The payload can affect the quality of sound. Thus, it can said that LSB method can embed high payload of hidden message compare to other methods. Besides, different LSB position can also affect the quality of audio. The experimental result of this research is that the secret message can be hidden up to LSB position 3 to maintain imperceptible for the audio sound.

ABSTRAK

Tesis ini memberi tumpuan kepada kesan kepada kualiti dalam steganografi audio. Steganografi ialah sains maklumat bersembunyi, yang digunakan untuk menyembunyikan data dari pihak ketiga. Audio steganografi adalah teknik yang digunakan untuk menghantar maklumat tersembunyi dengan mengubah isyarat audio dengan cara yang tak kelihatan. Menerapkan maklumat ke dalam steganografi audio adalah lebih selamat kerana teknik steganalysis kurang untuk menyerang untuk audio. Kurangnya ketara sedikit (LSB) pengekodan adalah cara yang paling mudah untuk membenamkan maklumat dalam fail audio digital. Dengan menggantikan sedikit terkanan setiap titik pensampelan dengan mesej binari , LSB pengekodan membolehkan sejumlah besar data yang akan dikodkan. Mendengar ujian dan SNR akan menjalankan untuk menguji kualiti antara fail asal dan fail terbenam. Muatan yang boleh menjejaskan kualiti bunyi . Oleh itu , ia boleh berkata bahawa LSB kaedah boleh membenamkan muatan tinggi mesej tersembunyi berbanding dengan kaedah lain. Selain itu, berbeza LSB kedudukan juga boleh memberi kesan kepada kualiti audio. Hasil eksperimen kajian ini adalah bahawa mesej rahsia yang tersembunyi sehingga LSB kedudukan 3 untuk mengekalkan tak kelihatan untuk bunyi audio.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

WAV: Waveform Audio File Format

SNR: Signal- to- Noise Ratio

LSB: Least Significant Bit

CHAPTER 1

INTRODUCTION

1.1 AUDIO STEGANOGRAPHY

Steganography is the science of hiding information, which is used to hiding the data from third party. No one will suspect the existence of the hidden message except the sender and recipient. It is actually in a form of security through obscurity. Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". The hidden information can be in any format such as text file, images, or even audio. It has been widely used by people nowadays and in ancient time. Simple steganography techniques have been use for hundreds of years. The first recorded uses of steganography can be traced back to 440BC. Demaratus, King of Sparta from 515 until 491BC, who sent a warning about a forthcoming attack to Greece by writing the secret message on a piece of wooden backing of a wax tablet before applying its beeswax surface. Compare the technology with ancient Greece, the technology nowadays is very advanced. The software needed for steganography can be download everywhere and some of them are freeware version.

Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is used to hide secret message or audio file such as WAV, MP3, WMA, etc in a host message. There are few types of techniques of audio steganography and all of them have different embedding methods. Embedding information into audio steganography are more secure due to less steganalysis techniques for attacking to audio. Besides, natural sensitivity and difficulty

of working on audio and improvement in related techniques is needed. As consequence, audio steganography is necessary to keep the hidden information safe.

1.2 SECURITY IN AUDIO STEGANOGRAPHY

In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen to make sure the secured data transfer. Audio steganography is one of the solution and it is about conceal its very existence.

The goal of audio steganography is to hide a message in the audio file to obtain a new data so that no one will detect the presence of message in new data. Embedding secret message in audio file is actually more difficult process than embedding message in other media such as digital images as Human Auditory System (HAS) is more sensitive than Human Visual System (HVS). Multimedia data hiding techniques have developed a strong basic for steganography area with a growing number of applications. Multimedia data hiding have to satisfy two basic requirements which are object not containing any additional data and object containing secret message must be perceptually indiscernible, and another one is high data rate of the embedded data.

When hiding the secret message into the audio file, make sure the quality of the new data is still same or not much different with the original data. If the sound quality is change after embedded the secret message, then other people may have known there is something hidden in the audio file. It is quite difficult to avoid the hidden information reveal to others even the data is hidden very carefully. There are some methods used to test the effect of quality in audio steganography which will be discussed in the following section.

1.2.1 QUALITY OF AUDIO STEGANOGRAPHY

The audio steganography are widely used today, it can be used to embed hidden message into audio file to carry the information about the object or any other information. The way to evaluating quality of audio is to calculate the signal-to-noise ratio (SNR) between the original audio and audio after hiding data. SNR is most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal is the original data while the noise is come from the error introduces by compression.

The purpose to test the quality if the audio file is to ensure that the sound of the embedded file listen by human is no different to the original sound. Thus, different methods can be used to test the quality of audio steganography and to detect the hidden message.

1.3 EFFECTS ON QUALITY IN AUDIO STEGANOGRAPHY

Today, audio steganography is used to transmit hidden information in digital sound. It is a tool of embedded secret message into audio. The new data after embedded can be test by different methods. The hidden information will be detect and recovered without any error. Thus, audio steganography can be widely used by human to keep the secret information safe.

Based on the motivations mentioned above, the following are the research question:

i. What is the methods in audio steganography?
ii. What is the effects on audio quality in audio steganography?

1.4 PROBLEM STATEMENT

There have many methods to embedded hidden message into an audio file such as LBS (Least Significant Bit) coding, phase coding, parity coding and spread coding. By using these different methods, it is possible to embed the hidden message with the

change of the individual bits that make up an audio file. Any techniques which tries to improve the embedding payload or robustness should preserve imperceptibility. Different embedding payload may have different effects on audio quality. The longer payload or the bytes of the hidden message is bigger, then it will change the original audio quality and get different effects. Thus, several methods will be used to compare the effects on audio quality using different embedding payload.

1.5 RESEARCH AIM

The aim of this research is to facilitate the implementations of different methods to test the effects on audio quality using different embedding payload.

1.6 RESEARCH OBJECTIVES

There are three objectives of the research:

i. To study methods in audio steganography

ii. To test the method used in audio steganography

iii. To compare effects on quality in audio steganography

1.7 RESEARCH OUTCOMES

The following are the research outcomes:

i. Acquire the knowledge of method in audio steganography.

ii. Comparing the effects on audio quality in audio steganography.

1.8 SCOPE

The scope in this project is to find out the different in quality between original audio and the audio after hiding message by using audio steganography methods. The way to evaluating quality of audio is to calculate the peak signal-to-noise ratio (PSNR). The correlation between message to host size ratio and PSNR is studied. If the ratio of host size to message size is greater, obtained PSNR will be better. The format that will be conduct in this project can be hide text file, image, or audio file such as MP3, WAV, WMA and others.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter, the details of audio steganography and the previous works will be introduced. This chapter comprise of 6 sections. Section 2.2 is a introduction of audio steganography. In section 2.3, audio steganography embedded methods will be discussed, and section 2.4 is about the type of testing methods . Then the section 2.5 is the audio steganography testing. Finally, section 2.6 will be the summary of the literature review.

2.2 AUDIO STEGANOGRAPHY

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Hiding a message with Steganography methods is more secure because it can reduce the chance of a message being detected. If the message is also encrypted then it provides another layer of protection (Johnson, 2006). Steganography is not a new science; it dates back to

ancient times. It has been used through the ages by ordinary people, spies, rulers, government, and armies (Sellars, 2002).

All Steganography techniques have to satisfy two basic requirements:

I. The first requirement is perceptual transparency or noticeable perceptual distortion which means the original data which is object not containing any additional data and stego object which is object that containing secret message must be perceptually indiscernible (Anderson, R.J. & Petitcolas, F.A., 1998).
II. The second requirement is high data rate of the embedded data.

Generally, audio steganography started consider as attractive area that have viable application and space for development (Y,Z., ZM, L. & DN, Z., 2010; AA, A., X, S. & H,Y., 2010), this is because audio steganography is getting famous for hiding secret message in audio file format. There are several packages now exist for hiding data in audio files (Medani A, G, A. Z. O. Z. A., 2011). In the past few years, several techniques for data hidden in audio sequences have been presented. All of the developed techniques take benefit of the perceptual properties of the human auditory system (HAS).

This is an example of audio steganography shown in Figure 1 to see how the audio steganography work. (Malviya, S., Saxena, M. & Khare, A., 2012)

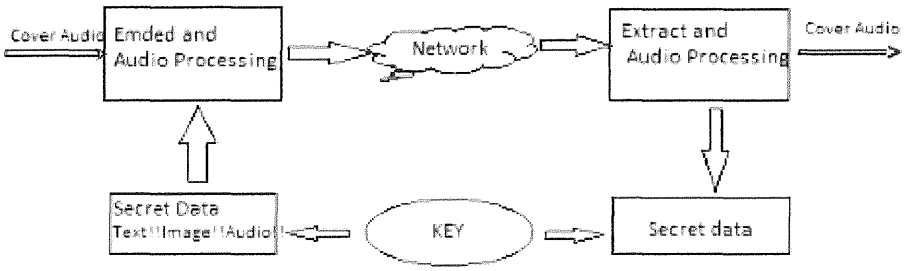


Figure 1: Blocks diagram for audio steganography

The sender embedded secret data of any type using a digital cover file to produce a stego file, in this way observer cannot detect the existence of the hidden message. Then the receiver processes the received stego-file to extract the hidden message. The cover file being used is a digital audio signal. An obvious application is a

covert communication using innocuous cover audio signal, such as telephone or video conference conversations.

2.3 AUDIO STEGANOGRAPHY EMBEDDED METHODS

This section presents some common methods used for hiding secret information in audio. When developing a data hiding method for audio, must first consider about the environments the sound signal will travel between encoding and decoding. There are two main areas of modification which is the storage environment, or digital representation of the signal that will be used, and the transmission pathway the signal might travel. (Malviya, S., Saxena, M. & Khare, A., 2012)

2.3.1 Least Significant Bit (LSB) Coding Method

In LBS coding method, least significant bit is modified to embed data. It is the simplest way to embed information in an audio file. LSB coding allow huge amount of data to be encoded by substitute the least significant bit of each sampling point with a binary message. This will not change the size of file even after encoding and also suitable for any type of audio file format. (Nehru, G. & Dhar, P., 2012)

The least significant bit substitution of a sample is to replaces with a message bit. The signal content should be consider first before deciding on the LSB operation to use. To extract a secret message from an LSB encoded sound file, the receiver need to access to the sequence of sample indices used in the embedding process. The length of the secret message to be encoded is smaller than the total number of samples in a sound file. It is important to choose the subset of samples that will contain the secret message and communicate that decision with the receiver at the beginning of the sound file and perform. (A, N. & K, G. A., 2012)

2.3.2 Phase Coding Method

The basic idea of phase coding method is to split the original audio stream or cover file into few blocks and embed the whole message data sequence into the phase spectrum of the first block.

Below will discuss the procedure for the phase coding done by Swati Malviya, Manish Saxena and Anubhuti Khare, 2012:

a. The original sound signal is break into few smaller segments whose lengths equal the size of the message to be encoded.

b. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform magnitudes.

c. Phase differences between adjacent segments are calculated.

d. Phase shifts between consecutive segments are easily detected. This can be say that the absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved. Therefore the secret message is only inserted in the phase vector of the first signal segment as follows

$$Phase_{new} = \begin{cases} \frac{\pi}{2} \; if \; message \; bit = 0 \\ \frac{-\pi}{2} \; if \; message \; bit = 1 \end{cases}$$

e. A new phase matrix is created using the new phase of the first segment and the original phase differences.

f. The new phase matrix and original magnitude matrix is using, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together. To extract the secret message from the sound file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information.

2.3.3 Spread Spectrum Method

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. The SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. (Venkateswaran, R. & V. Sundaram, 2011)

Zhou et al. proposed an algorithm embedding watermark in 0th DCT (Discrete Cosine Transform) coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal. The original signal is transformed into frequency domain using DCT. The process of generating embedded signal is shown as embedding procedure in Figure 1. Embedded signal will has some attacks, so noise is added to the signal. To extract the watermark the attacked signal is fed through extraction procedure. The procedure for extractions follows the same steps as that in embedding procedure as shown in Figure 1. The extraction process involves taking the attacked signal and applying DCT, framing the obtained components. And they obtain ned frames are used to obtain the watermark. Care is taken to replicate the procedure used for embedding process. (Malik, H. & Kang, S. S., 2013)

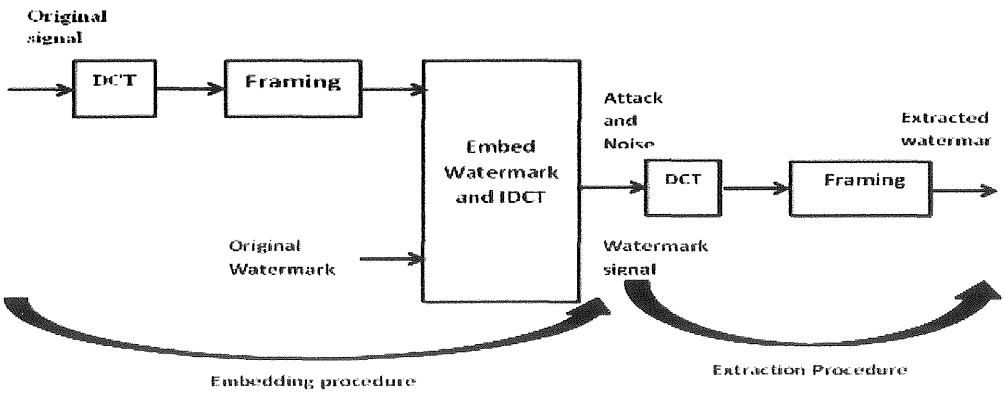


Figure 2: Example for spread spectrum technique

2.3.4 Parity Coding Method

The parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LBS of one of the samples in the region. So that the sender has more choice to encode the secret bit, and the signal can be changed in a more unobtrusive fashion. (Venkateswaran, R. & V. Sundaram, 2011)

2.4 TYPE OF TESTING METHODS

There are two types of methods to evaluate the sound quality of audio steganography. There are subjective evaluation to listen to the sound and objective evaluation such as using Peak-Signal-To-Noise Ratio (PSNR) and Mean Square Error (MSE) tests. Subjective listening test are indispensable and essential toward perceptual quality evaluation, because of the ultimate judgment that is made by human perception and the unreliability to the objective test. But, carrying out such listening tests is quite difficult and also not enough for manufacturing. Therefore, objective evaluation are useful to provide a convenient, consistent and fair measurement (Y, L. & WH, A., 2008).

2.5 AUDIO STEGANOGRAPHY TESTING

This steganography research will be test to find the level of quality stegofile after the message embedded to the carrier. For the bitmap carrier type file tested using the Peak Signal to Noise Ratio (PSNR) formula and the Signal to Noise Ratio (SNR) for wave stegofile which both of these formulas will be counted in decibel (dB). The aim of objective evaluation tests is to facilitate the implementation of subjective listening tests

(Kiah, M. et al., 2011). To achieve its goal, results of objective evaluation should related well with Subjective Different Grade (SDG) by Arnold, 2012.

Description of impairments	Difference grade
Very annoying	1
Annoying	2
Slightly annoying	3
Perceptible but not annoying	4
Imperceptible	5

Figure 3: Subjective Different Grade

The main full-reference objective test for audio quality metrics that have been appears in the literature are:

I. Peak Signal-to-Noise Ratio (PSNR)
II. Mean Square Error (MSE)
III. Signal to-Noise Ratio (SNR)

Nowadays, PSNR is widely used because it is simple to calculate, has clear physical meanings, and is mathematically easy to deal with for optimization purpose (Kiah, M. et al., 2011). PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs.

The value of PSNR is good if it is above of 20 dB with formula (Kriti, S. & Kumar, S. P., 2010):

$$\text{PSNR} = 10\ \text{Log}_{10}\left(\frac{255^2}{MSE}\right)$$

255 is the highest value of pixel intensity and MSE (Mean Square Error) is the average value of total square of Absolute Error between carrier file and stegofile.

MSE can be counted with the formula bellow:

$$\text{MSE} = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The SNR formula used to know the distortion ratio that happened after the message inserted to the carrier with the formula (Sujay, N. & Gaurav, P., 2010):

$$SNR = 10\ Log_{10}\left\{\frac{\sum_n X^2(n)}{\sum_n [X^2(n) - Y^2(n)]}\right\}$$

X(n) is the average of RMS (Root Mean Square) value from the carrier file and Y(n) is the average of RMS value from stegofile. The RMS value is the formula to know how big the sample audio out of any audio file. It can be known by using the audio editor application that provides information about quality of RMS audio. In audio signals for example, an SNR below 20 dB, generally denotes a noisy audio signal, while an SNR of 30 dB and above indicates that the audio signal quality is preserved (Djebbar, F., Ayad, B., Meraim, K. A. & Hamam, H., 2012).

2.6 SUMMARY

As a conclusion for this literature review, there are few audio steganography methods to embed secret data into audio file and being discussed. Besides, there are few testing methods to test the quality of audio steganography. It can be conclude that different payload capacity will have different effects on quality in steganography. So, there will have a limit to embed the secret message on an audio file.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter is going to describe the method have been used in this research on audio steganography. In section 3.2, is to discuss about the research methodology of proposed method to embed hidden message in the audio steganography. For the section 3.3, it is to discuss about the research methodology of testing method for the effects on quality in audio steganography. At last, 3.4 will be the conclusion for the proposed method.

3.2 RESEARCH METHODOLOGY OF AUDIO STEGANOGRAPHY

3.2.1 Challenges in Steganography

Like all multimedia data hiding methods, audio steganography has to satisfy three basic requirements to achieve in an effective audio steganography. The three basic requirements are also a challenge for audio steganography.

There are on below:

i. Perceptual Transparency: In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.

ii. Size of Payload: Steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory.

iii. Robustness: Steganography should increase the robustness to avoid unintentional attacks.

3.2.2 Least Significant Bit (LSB) Method

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. A novel method which increases the limit up to four bits by Nedeljko Cvejic, Tapio Seppben & mediaTeam Oulu. To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One

solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples.

When embedding the textual information in any audio file, first the audio signal is converted into bits. Then the message to be embedded is converted. By applying LSB algorithm, the message is embedded into 16 bits or 8 bits audio sample. The performance is evaluated by applying LSB algorithm at different position i.e 1LSB, 2LSB and so on. At the receiver side, the first five bytes are taken, if these bytes are same as our control symbols bytes then the next character case is defined.

3.2.3 LEAST SIGNIFICANT BIT (LSB) ALGORITHM

3.2.3.1 Embedding Algorithm

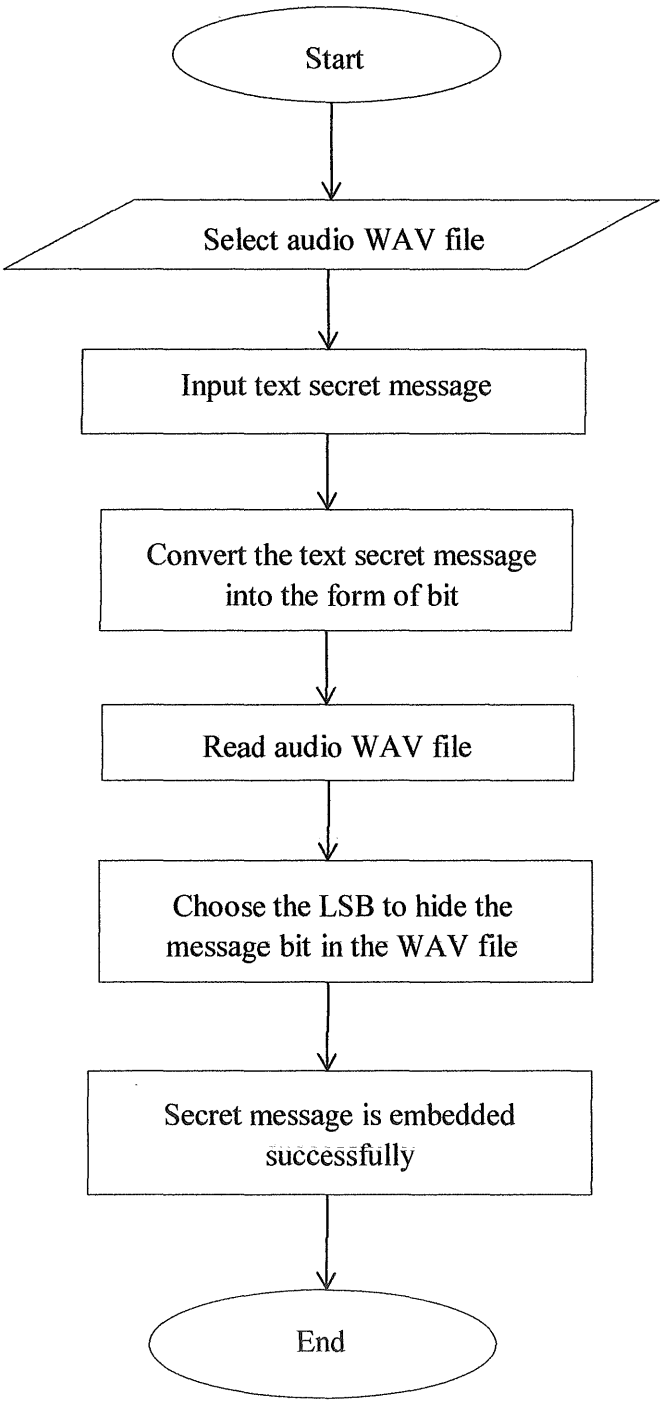
1. Select audio WAV file.
2. Input the text message to be embedded.
3. Convert the message into bit code.
4. Read WAV audio file as cover file.
5. Choose the LSB position for hiding text message.
6. Repeat till the whole message can be embedded in audio.

3.2.3.2 Retrieving Algorithm

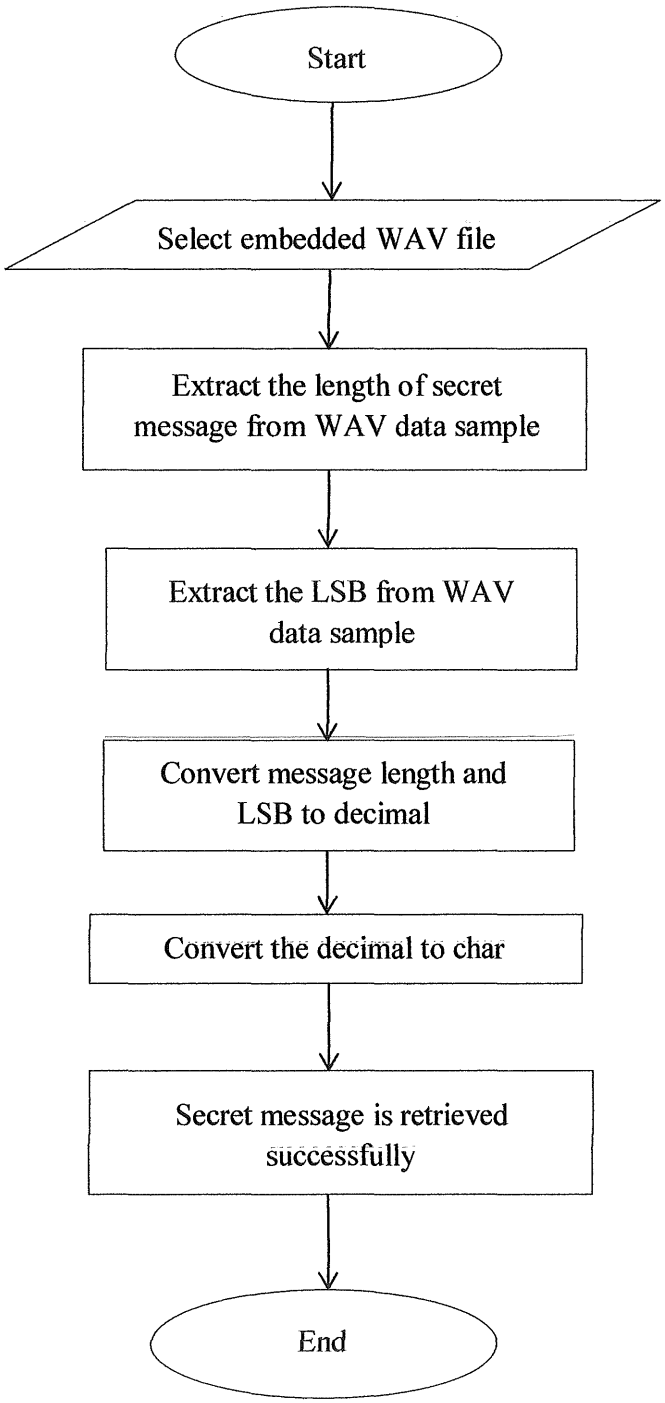
1. Read the embedded WAV file.
2. Extract the length of message from data sample.
3. Extract LSB position from WAV data sample.
4. Convert message length and LSB position to decimal.
5. Convert the decimal to char.
6. Display the secret message.

3.2.4 FLOW CHART OF LEAST SIGNIFICANT BIT (LSB) METHOD

The following steps show the steps for the proposed LSB method to embed text message.



The following steps show the steps for the proposed LSB method to retrieve text message.



3.3 RESEARCH METHODOLOGY OF TESTING METHODS

3.3.1 Subjective Evaluation – Listening Testing Method

Subjective listening tests by human's auditory perception, the subjects are asked to discriminate the differences between the stego file and original audio clips. The stego file signal is graded with respect to the host signal according to five- grade scare, the five- grade scale called Subjective Difference Grade, which is the difference between the subjective ratings given individually to the audio steganography signal and the original signal. Subjective listening tests are indispensable and essential toward perceptual quality evaluation, due to the ultimate judgment that is made by human perception and the unreliability of the objective test.

The survey will be done by giving 30 people to listen the audio file after embedded secret message and also the original audio file before embedded secret message. The 30 people will include senior citizen, adult, teenager and children. People will give the result by listen to the audio whether the audio sound is good or noise, can be accept or cannot be accept.

The result will grade by using the Subjective Difference Grade below :

Description of impairments	Difference grade
Very annoying	1
Annoying	2
Slightly annoying	3
Perceptible but not annoying	4
Imperceptible	5

3.3.2 Objective Evaluation – SNR (Signal- to- Noise Ratio)

The aim of objective evaluation tests is to facilitate the implementation of subjective listening tests. To achieve its goal, results of objective evaluation should relate well with Subjective Difference Grade.

SNR is a statistical difference metric which is used to measure the similitude between the original audio WAV file and the embedded audio WAV file. The SNR computation is done according to Equation, where X corresponds to the original audio signal and Y corresponds to the embedded audio signal.

The SNR formula used to know the distortion ratio that happened after the message inserted to the carrier with the formula:

$$SNR = 10\ Log_{10}\left\{\frac{\sum_n X^2(n)}{\sum_n [X^2(n) - Y^2(n)]}\right\}$$

X(n) is the average of RMS (Root Mean Square) value from the carrier file and Y(n) is the average of RMS value from embedded audio file.

3.3.3 Testing Algorithm

Follow the steps to testing the effect of audio steganography:

1. START

2. Calculate SNR for both original audio and embedded file

3. IF the result of original audio == result of embedded file, the SNR = ∞, no different between the original file and embedded file

4. ELSE get different result between original audio and embedded file

5. END

3.4 CONCLUSION

The main goal of steganography is to be unsuspected by the human eyes or human ear. For instance audio steganography is a great example for data protection and intellectual property. LSB method of steganography is very simple and easy to implement. The proposed method of the LSB method used as audio steganography combined with coding techniques gives high capacity. The key idea of the algorithm is steganography bit embedding that cause minimal embedding distortion of the host audio.

The effects on quality in audio steganography can be test by subjective evaluation and objective evaluation. Subjective listening tests are indispensable and essential toward perceptual quality evaluation, duo to the ultimate judgment that is made by human perception and the unreliability of the objective test. While the objective evaluation which is PSNR and SNR is widely used because it is simple to calculate, has clear physical meanings, and is mathematically easy to deal with for optimization purpose. Objective evaluations are also useful to provide a convenient, consistent and fair measurement The SNR ratio will be used to measure the ratio between original audio file and embedded file, and the result will be compare to see the different before and after embedded the hidden message.

As a conclusion, LSB method is very high steganography channel bit rate and a low computational complexity of the algorithm. It can embed high payload of hidden message compare to other methods.

CHAPTER 4

EXPERIMENTAL RESULT

4.1 INTRODUCTION

In this chapter, the experimental result is going to be illustrated and discussed. In section 4.2, the result of audio quality is shown in data tables, sample audio wave images and graphs. In 4.2.1, the testing result of audio quality by using SNR is shown in table for each sample of audio. In 4.2.1.1, the images of audio wave will be shown. The images will show the changes of audio wave of the song before embedded secret message and after embedded secret message. In 4.2.2, the result of subjective evaluation which is listening testing will be shown in pie chart. The retrieved process of the secret message will show at section 4.3. At last, the conclusion of this chapter is discussed in section 4.4.

4.2 EXPERIMENTAL RESULT

4.2.1 Audio Steganography Process

Two sets of 32- bit stereo WAV audio file with different audio size was embedded with different size of secret messages. Those secret messages were embedded in different LSB of the WAV audio file. The detail of the experiment results of audio steganography process is shown in table 1(a). The images of audio wave length of original and embedded audio for each LSB layer is shown in figure 4 to figure 13.

Audio (WAV file)		LSB	Audio Size (bit)	Message Size (bit)	SNR (dB)
Original	Embedded				
cat	cat1	1	4464	320	104.6563
	cat2	4	4464	320	86.4193
	cat3	8	4464	320	62.2398
	cat4	16	4464	320	14.0511
monkey	monkeyA	1	27475	6640	99.3993
	monkeyB	4	27475	320	93.7443
	monkeyC	8	27475	5760	58.3102
	monkeyD	16	27475	6720	9.3541

Table 1(a): The audio steganography experiment result for different LSB.

Image of wave length of cat.wav, cat1.wav,cat2.wav, cat3.wav and cat4.wav.

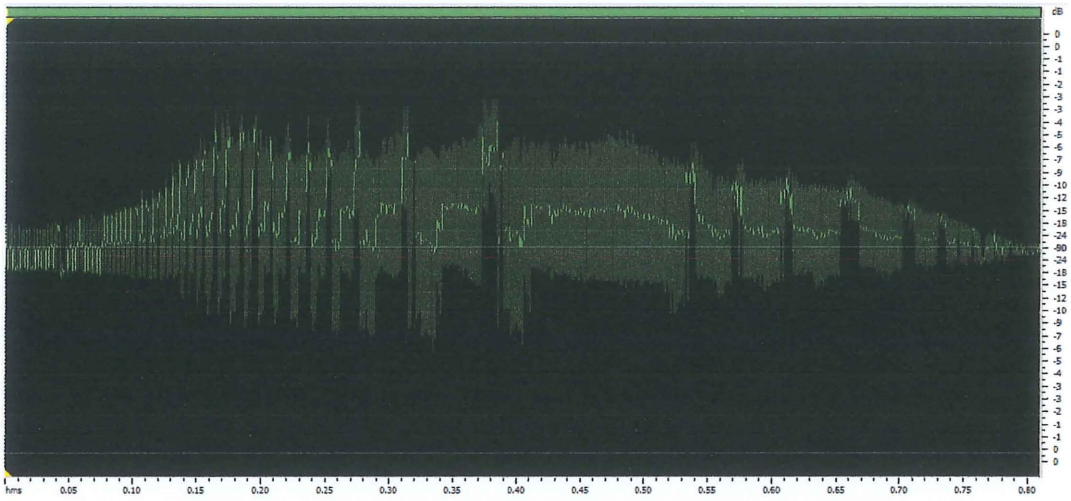


Figure 4 : The wave length of original WAV file, cat.wav.

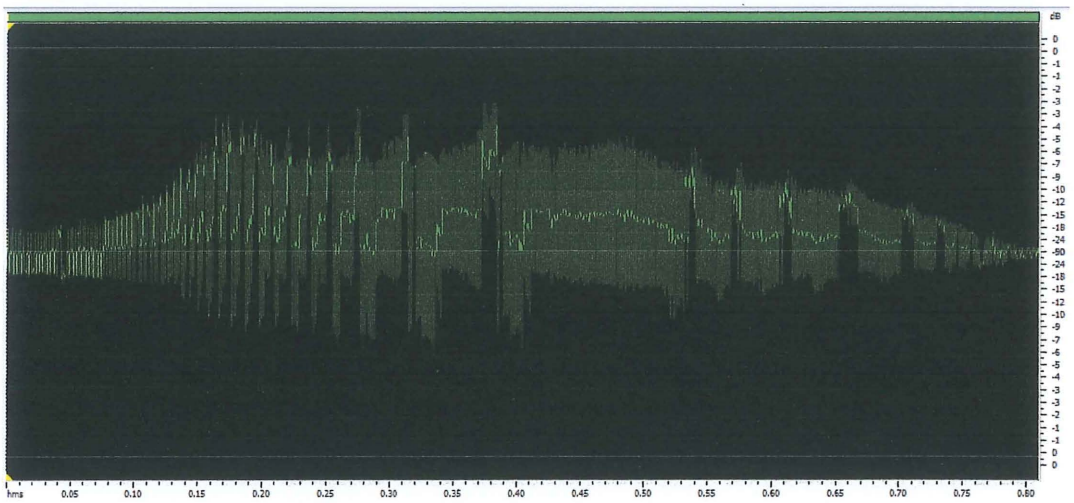


Figure 5 : The wave length of embedded WAV file, cat1.wav. Secret messages embedded in LSB 1.

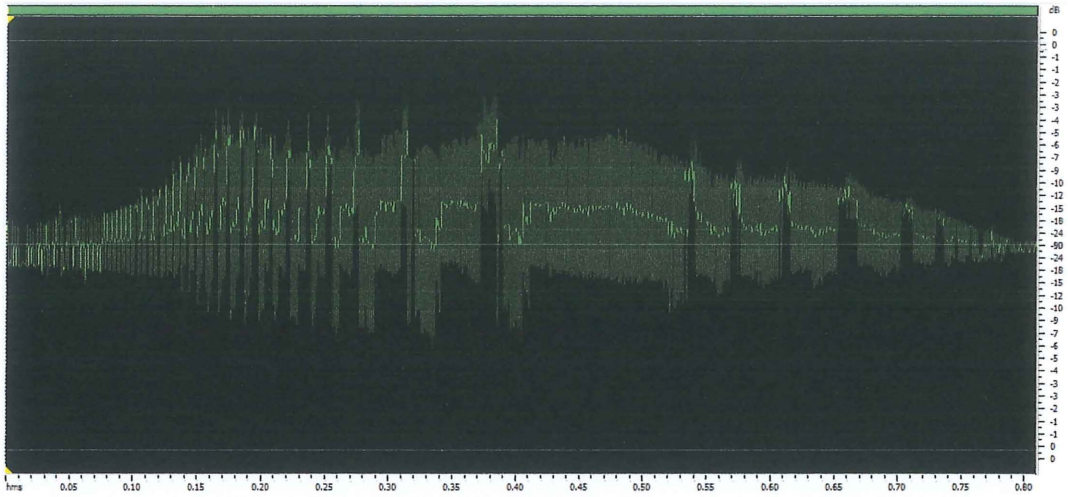


Figure 6: The wave length of embedded WAV file, cat2.wav. Secret messages embedded in LSB 4.

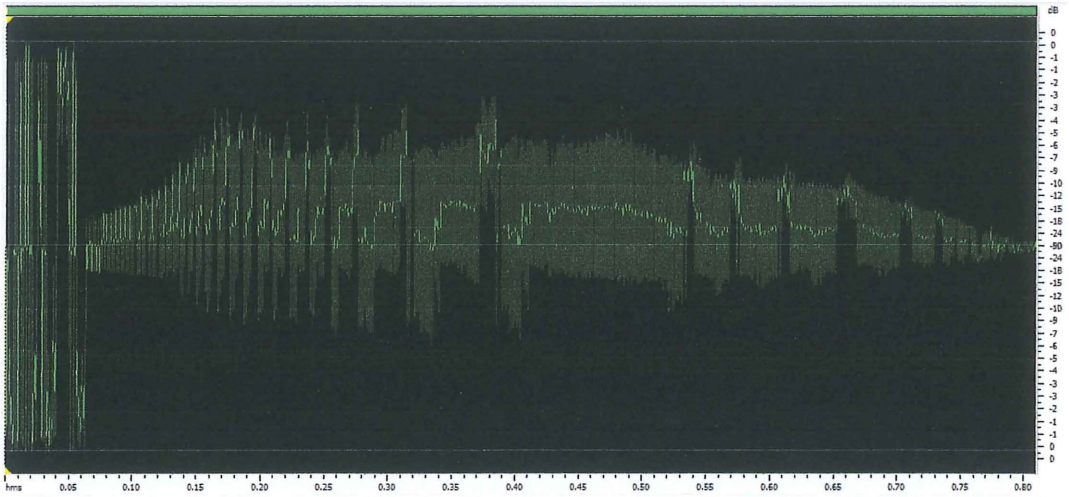


Figure 7: The wave length of embedded WAV file, cat3.wav. Secret messages is embedded in LSB 8.

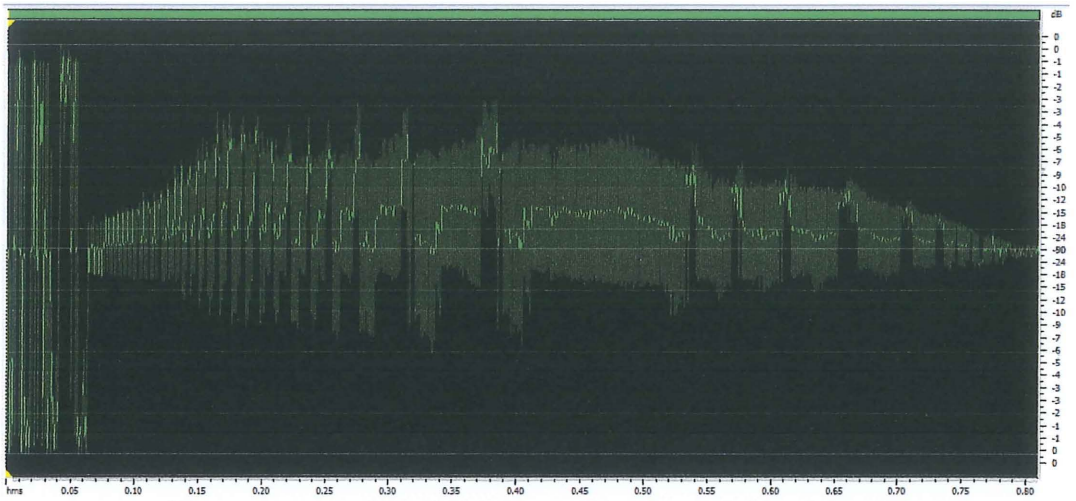


Figure 8: The wave length of embedded WAV file, cat4.wav. Secret messages is embedded in LSB 16.

Image of wave length of monkey.wav, monkeyA.wav, monkeyB.wav, monkeyC.wav, monkeyD.wav.

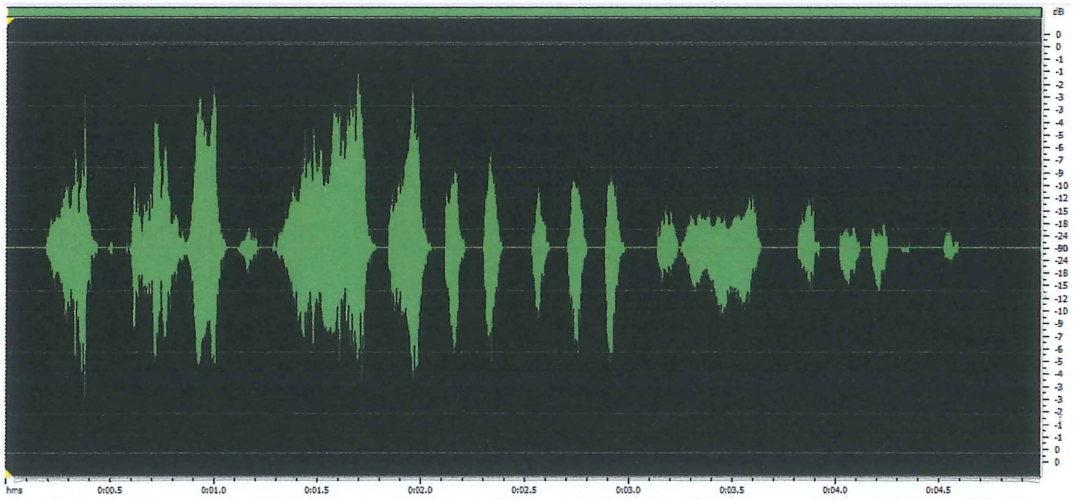


Figure 9: The wave length of original WAV file, monkey.wav.

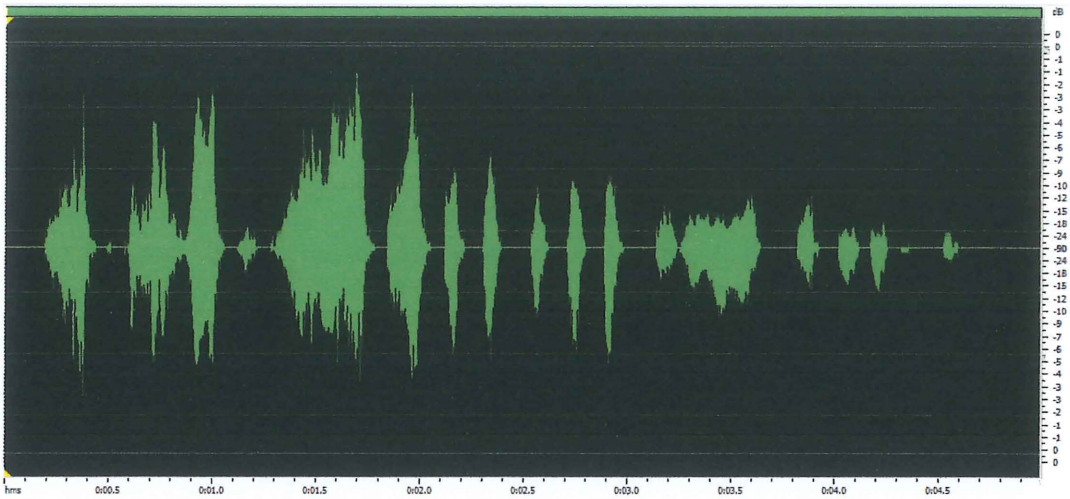


Figure 10: The wave length of embedded WAV file, monkeyA.wav. Secret messages is embedded in LSB 1.

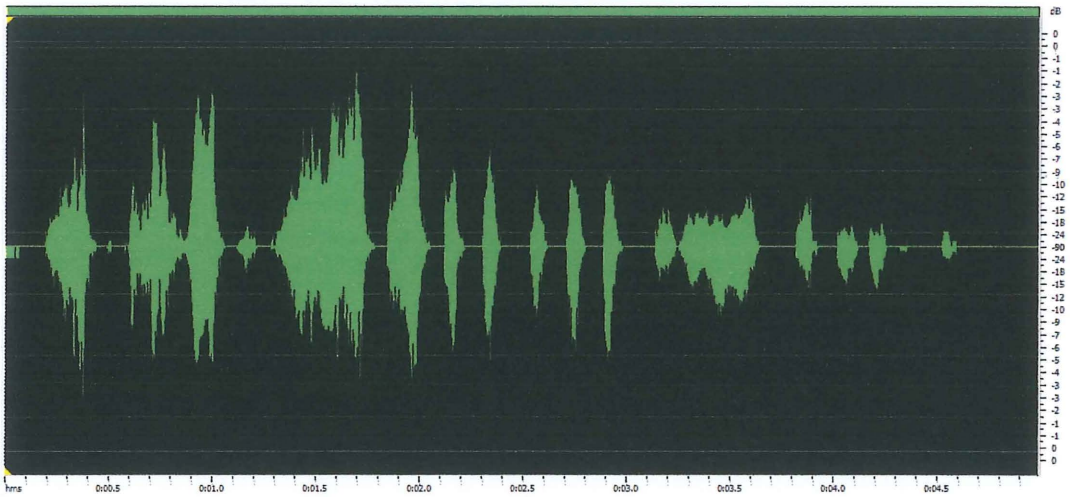


Figure 11: The wave length of embedded WAV file, monkeyB.wav. Secret messages is embedded in LSB 4.

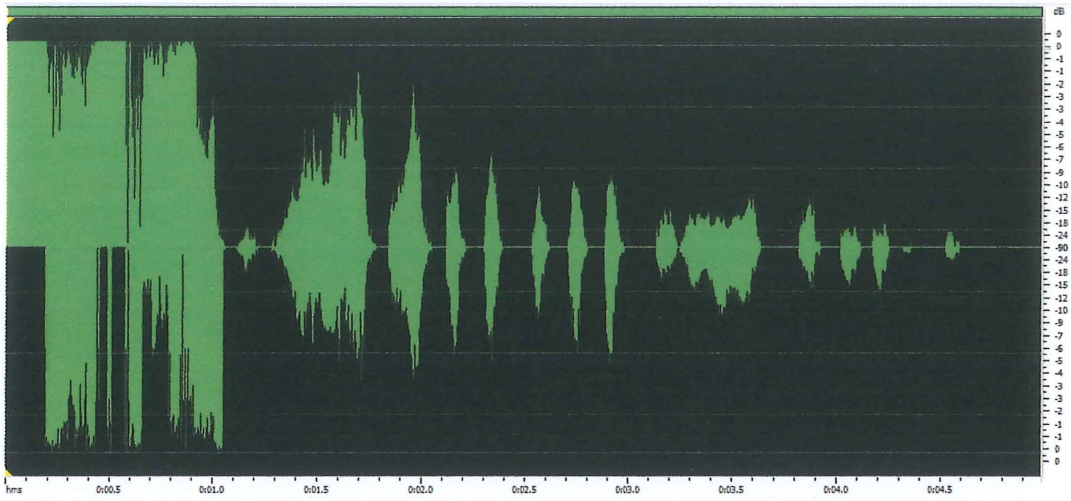


Figure 12: The wave length of embedded WAV file, monkeyC.wav. Secret messages is embedded in LSB 8.

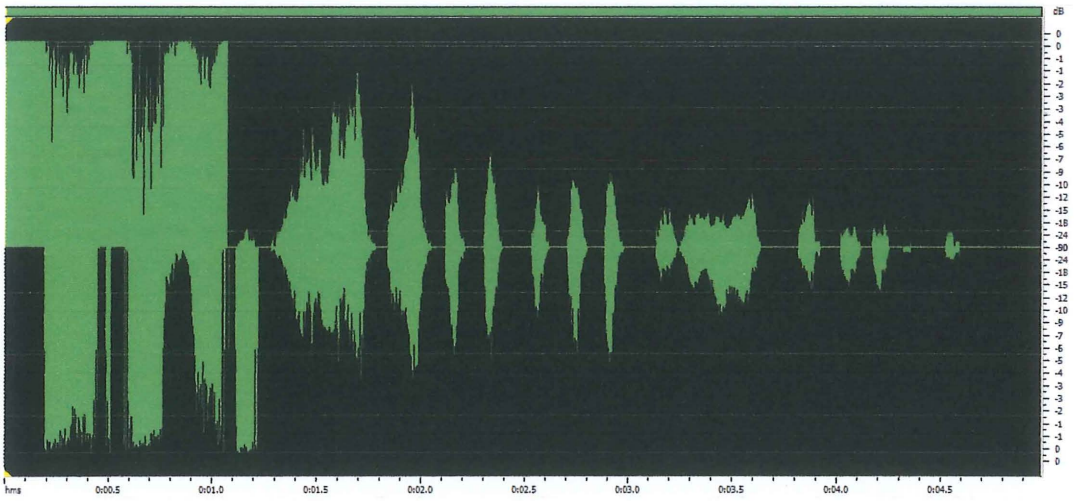


Figure 13: The wave length of embedded WAV file, monkeyD.wav. Secret messages is embedded in LSB 16.

A set of 32- bit stereo WAV audio file with 4464 bits of audio size were embedded with different size of secret messages. But those secret messages were embedded in same LSB layer which is LSB layer 1 of the WAV audio file. The detail of the experiment results of audio steganography process is shown in table 1(b). The images of audio wave length of original and embedded audio for each LSB layer is shown in figure 14 to figure 17.

Audio (WAV file)		LSB	Audio Size	Message	SNR
Original	Embedded	layer	(bit)	Size (bit)	(dB)
cat	catA	1	4464	2880	95.3651
	catB	1	4464	4160	93.7262
	catC	1	4464	960	100.0766

Table 1(b): The audio steganography experiment result for different message size.

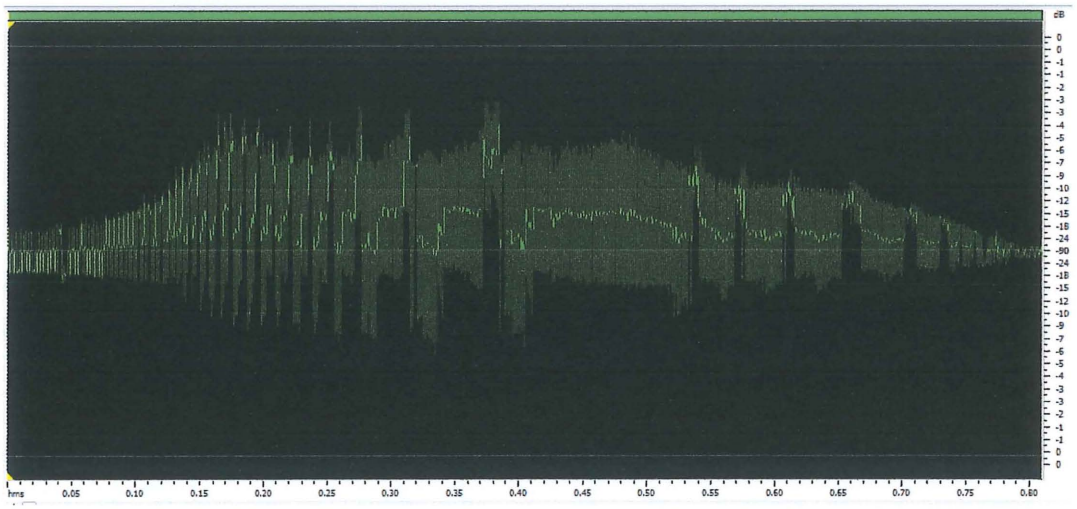


Figure 14: The wave length of original WAV file, cat.wav

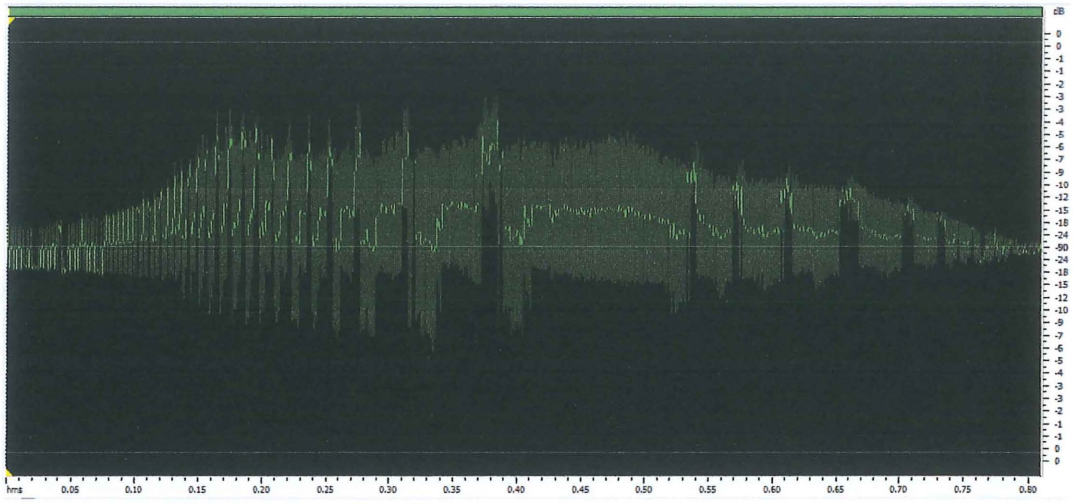


Figure 15: The wave length of embedded WAV file, catA.wav. Secret messages size is 2880 bits.

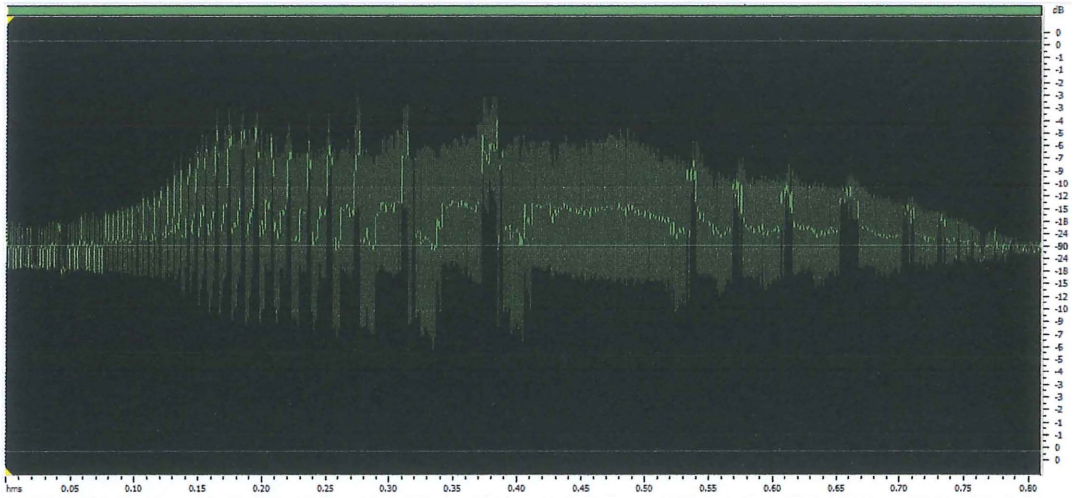


Figure 16: The wave length of embedded WAV file, catB.wav. Secret messages size is 4160 bits.

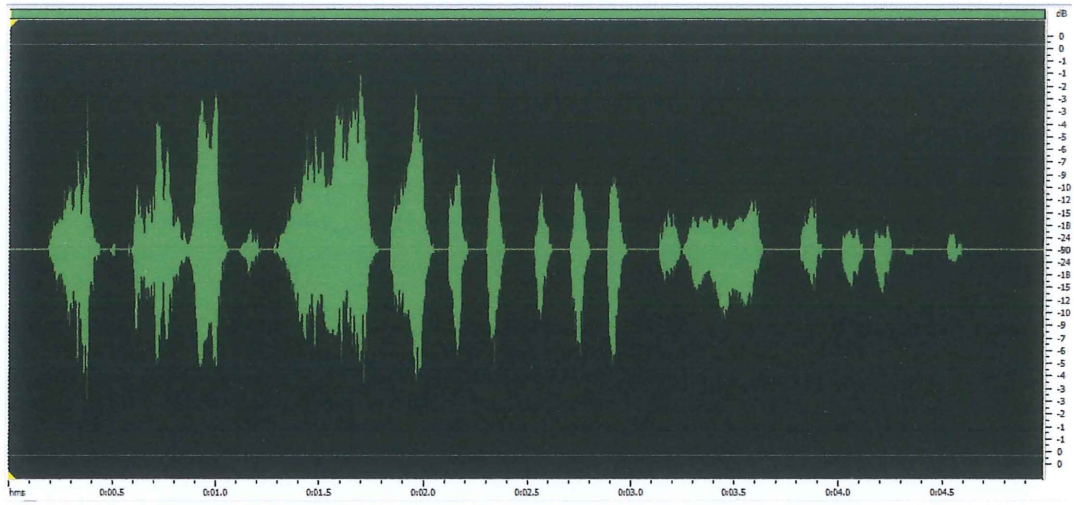


Figure 18: The wave length of original WAV file, monkey.wav.

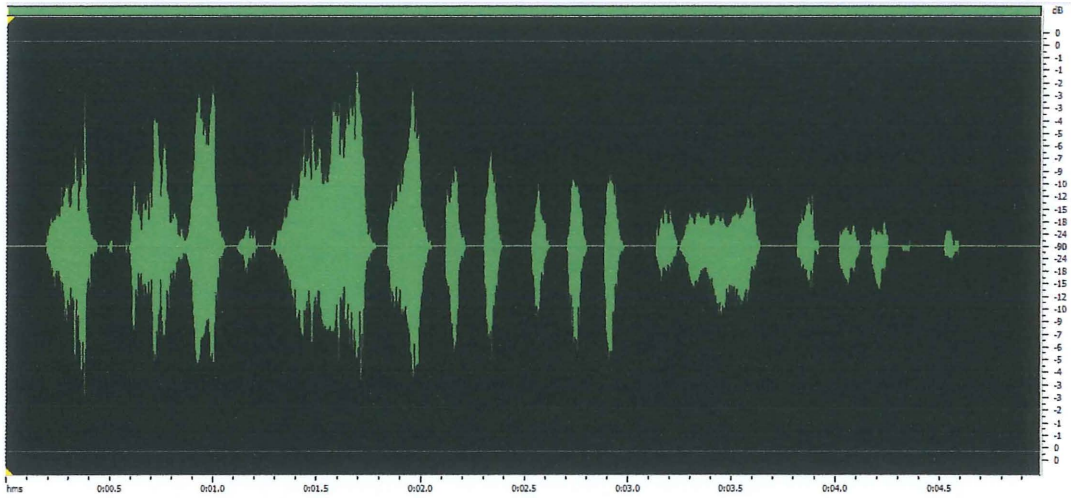


Figure 19: The wave length of embedded WAV file, monkey1.wav. Audio size is 27475 bits.

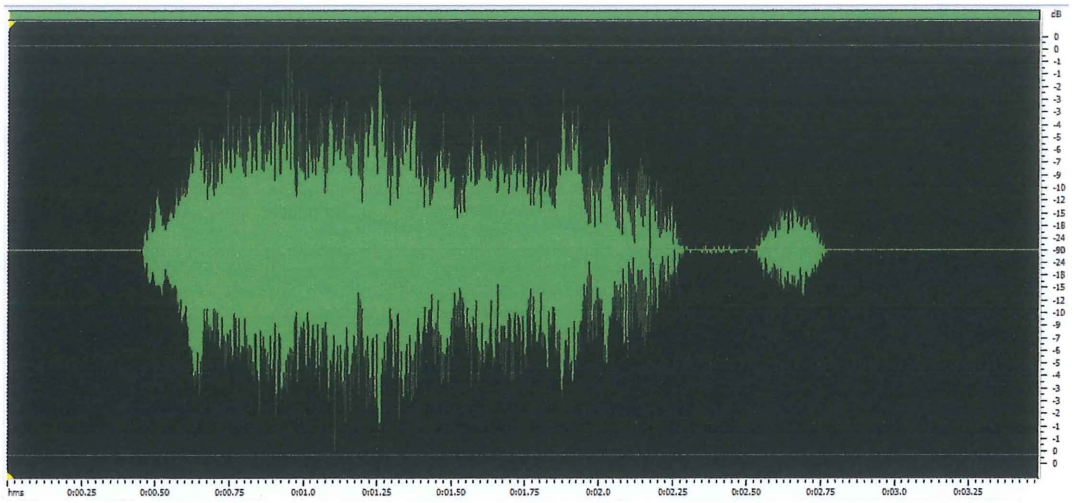


Figure 20: The wave length of original WAV file, horse.wav.

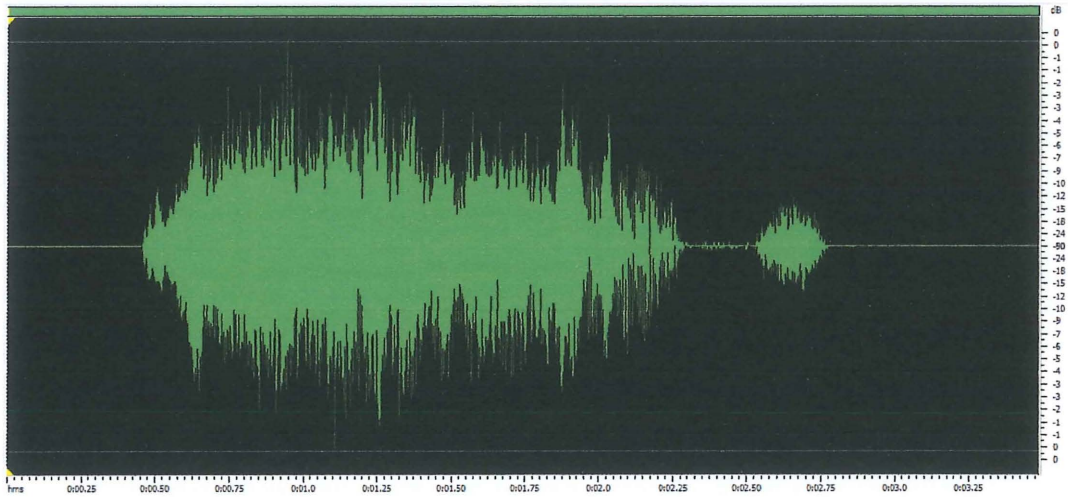


Figure 21: The wave length of embedded WAV file, horse1.wav. Audio size is 19227 bits.

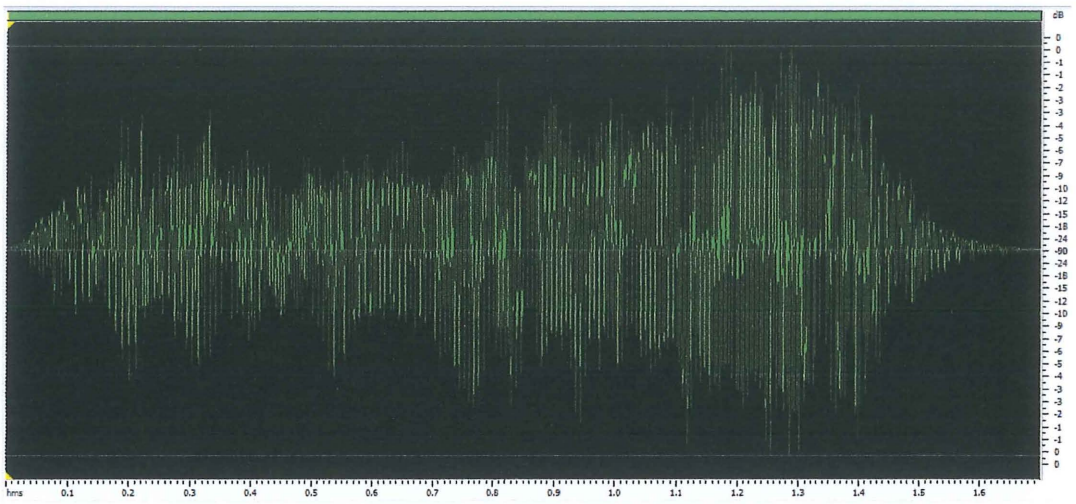


Figure 22: The wave length of original WAV file, cow.wav.

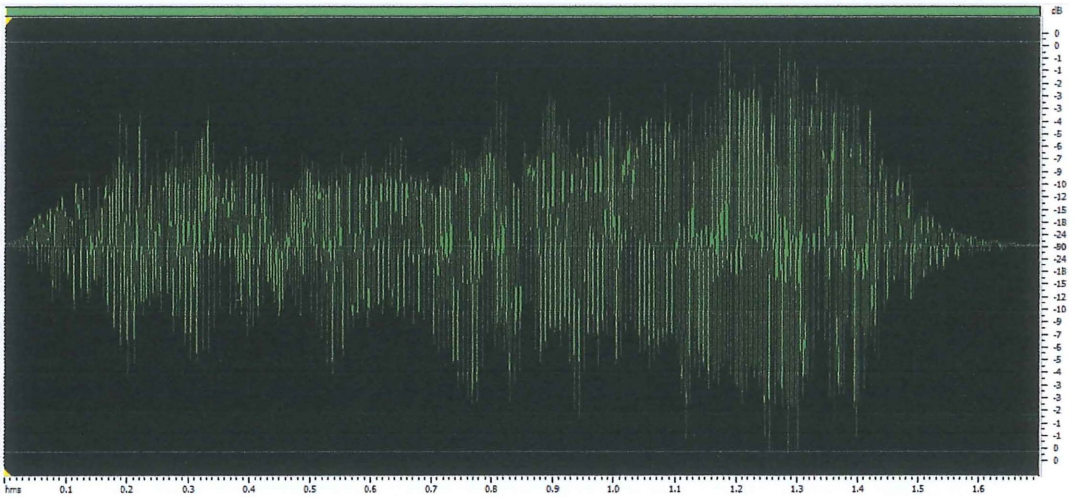


Figure 23: The wave length of embedded WAV file, cow1.wav. Audio size is 6798 bits.

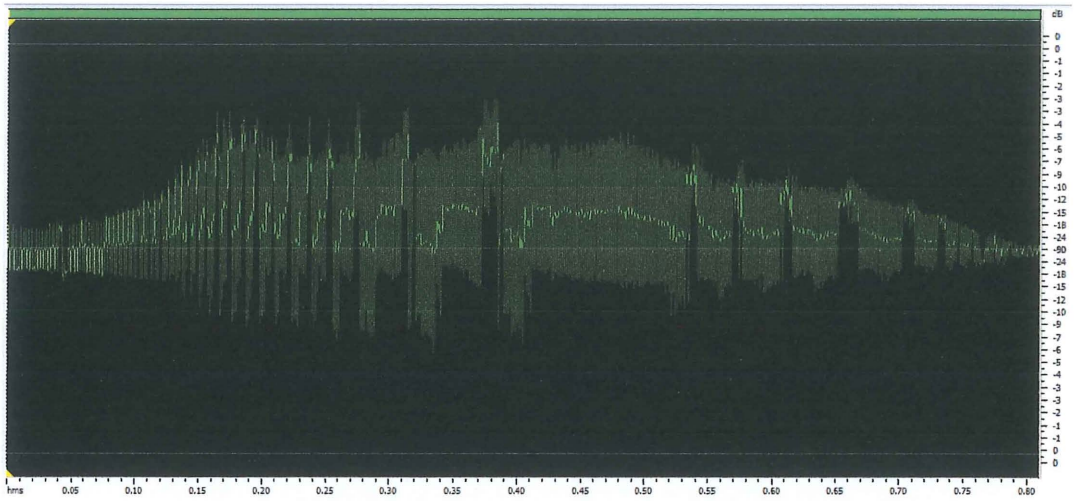


Figure 24: The wave length of original WAV file, cat.wav.

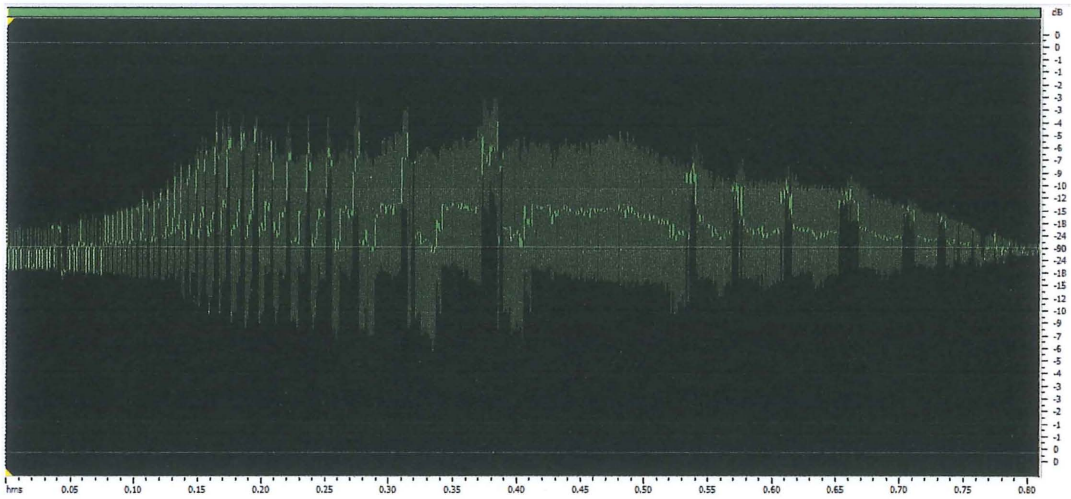


Figure 25: The wave length of embedded WAV file, cat0.wav. Audio size is 4644 bits.

4.2.2 Subjective Evaluation – Listening Testing Survey

The survey is done by giving 30 people to listen the original audio file and the audio after embedded secret message. The 30 people come from different social group which include senior citizen, adult, teenager and children. People will give the result by listen to the audio whether the audio sound is good or noisy, can be accept or cannot be accept.

The result will grade by using the Subjective Difference Grade below :

Description of impairments	Difference grade
Very annoying	1
Annoying	2
Slightly annoying	3
Perceptible but not annoying	4
Imperceptible	5

4.2.2.1 Survey Process

There are 2 sets of original audio WAV file, that is cat.wav and monkey.wav. Each WAV file will be embed the secret message in different LSB, which is LSB 1, 4, 8 and 16. Therefore, an original audio WAV file will have 4 different songs which mean secret messages embed in different LSB. Total 8 songs will be listen by each people. The survey is carry on between 30 people of male and female. They are from different social group which is senior citizen, adult, teenager and children. Below is the information of the survey songs, which is listen by those 30 people.

Audio (WAV file)		LSB	Audio Size (bit)	Message Size (bit)	SNR (dB)
Original	Embedded				
cat	Song 1	1	4464	3200	94.9825
	Song 2	8	4464	3200	52.7107
	Song 3	16	4464	640	11.4464
	Song 4	4	4464	320	86.4193
monkey	Song 5	8	27475	5760	58.3102
	Song 6	1	27475	6400	99.3994
	Song 7	4	27475	320	93.7443
	Song 8	16	27475	6720	9.3541

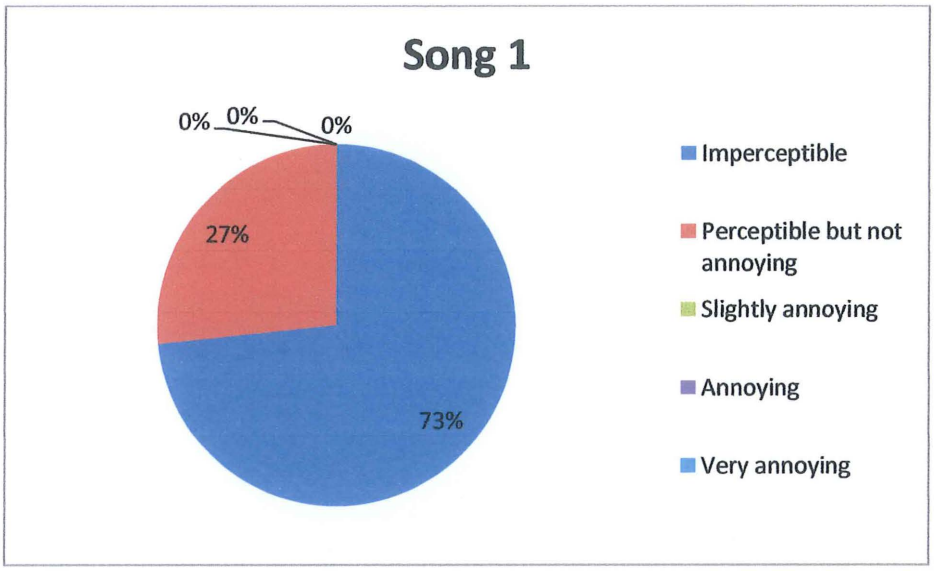
Table 2: The audio steganography SNR result for survey songs.

Audio (WAV file)		Very annoying	Annoying	Slightly Annoying	Perceptible but not annoying	Imperceptible
Original	Embedded					
cat	Song 1	0	0	0	8	22
	Song 2	23	7	0	0	0
	Song 3	3	7	12	8	0
	Song 4	0	0	0	15	15
monkey	Song 5	20	9	1	0	0
	Song 6	0	0	0	11	19
	Song 7	0	0	9	15	15
	Song 8	24	6	0	0	0

Table 3: The audio quality survey result for survey songs by 30 people.

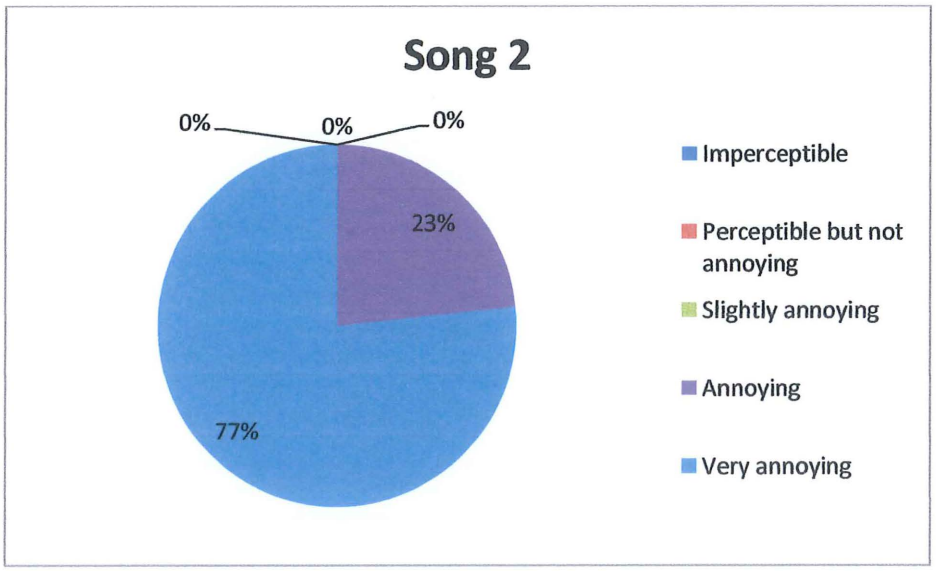
The survey result will be sketch in pie chart. Total 8 songs will sketch in pie chart with the result.

Figure 26: Pie chart of the Song 1. Secret messages embedded in LSB 1.



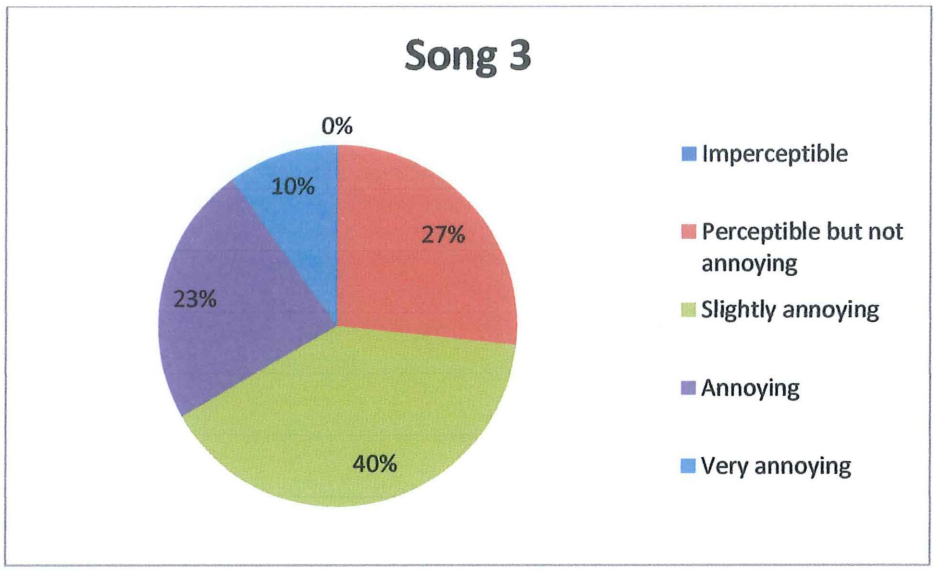
Conclusion: 22 people found that the audio sound is imperceptible.

Figure 27: Pie chart of the Song 2. Secret messages embedded in LSB 8.



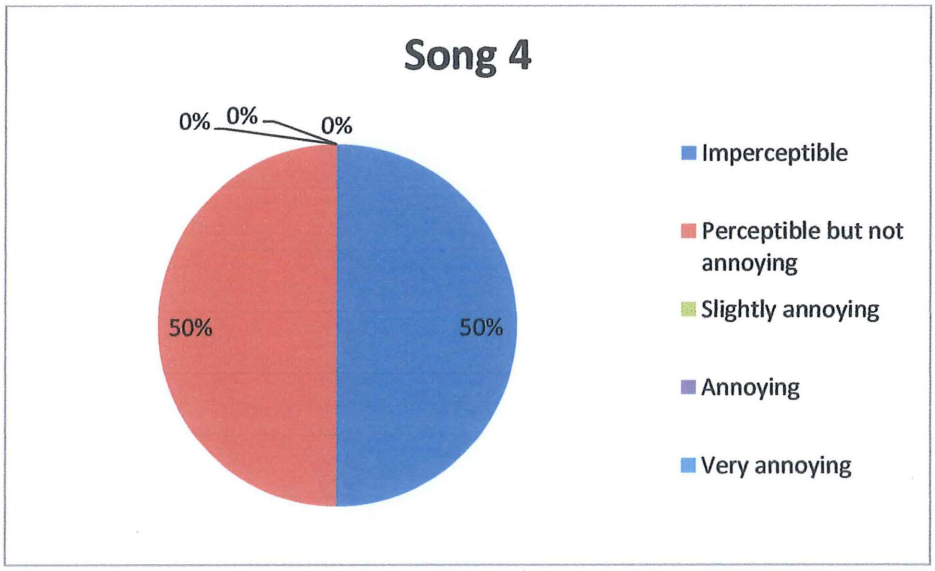
Conclusion: 23 people found that the audio sound is very annoying.

Figure 28: Pie chart of the Song 3. Secret messages embedded in LSB 16.



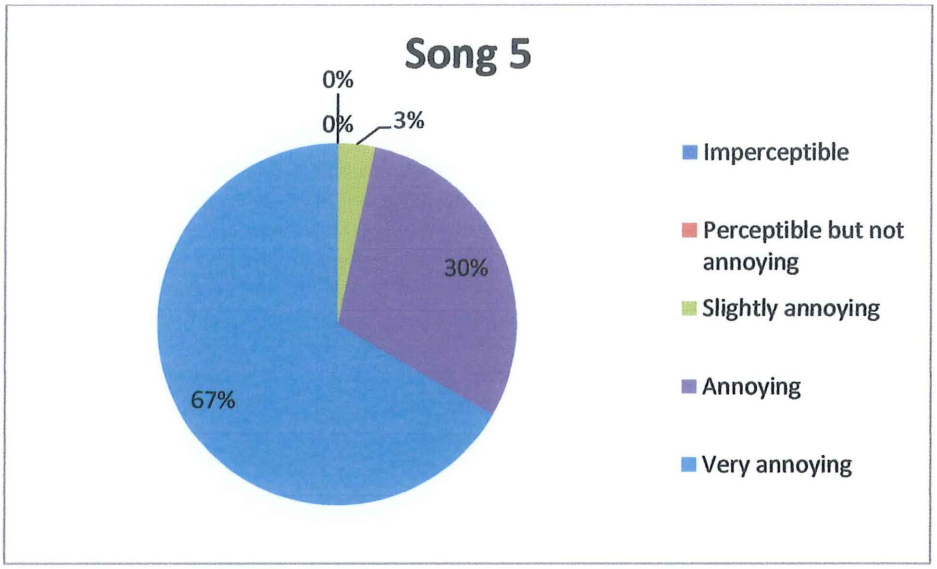
Conclusion: 12 people found that the audio sound is slightly annoying.

Figure 29: Pie chart of the Song 4. Secret messages embedded in LSB 4.



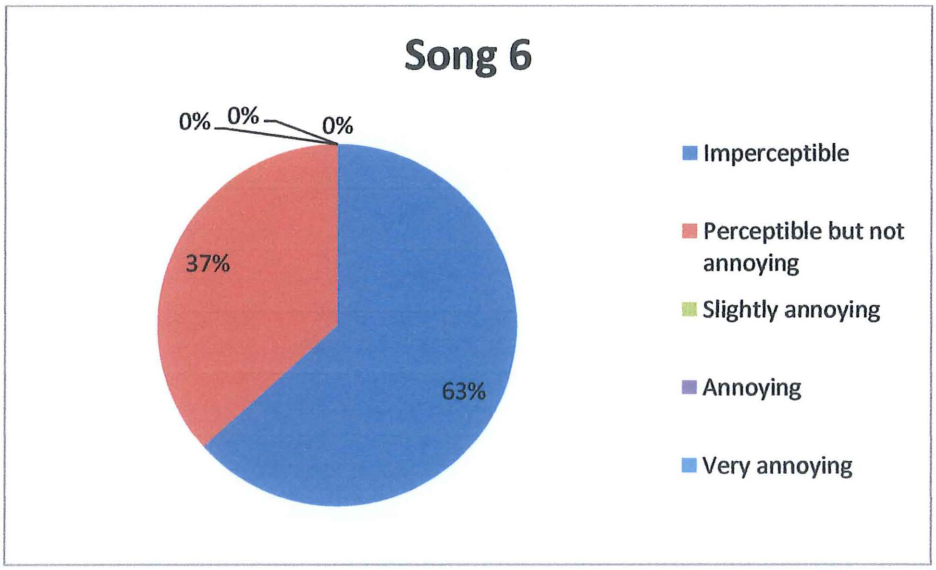
Conclusion: 15 people found that the audio sound is imperceptible and another 15 people found that the audio is perceptible but not annoying.

Figure 30: Pie chart of the Song 5. Secret messages embedded in LSB 8.



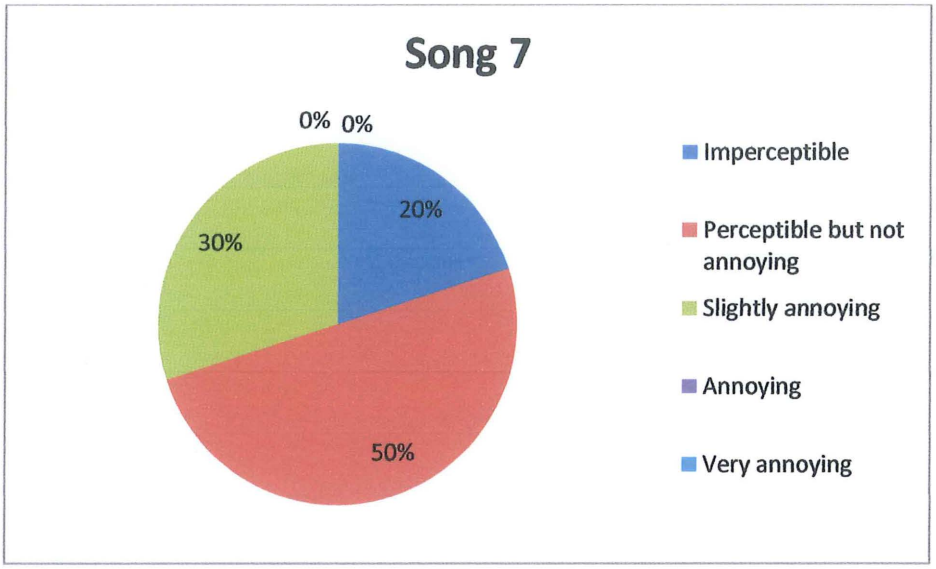
Conclusion: 20 people found that the audio sound is very annoying. Only 1 people found that the audio sound is slightly annoying.

Figure 31: Pie chart of the Song 6. Secret messages embedded in LSB 1.



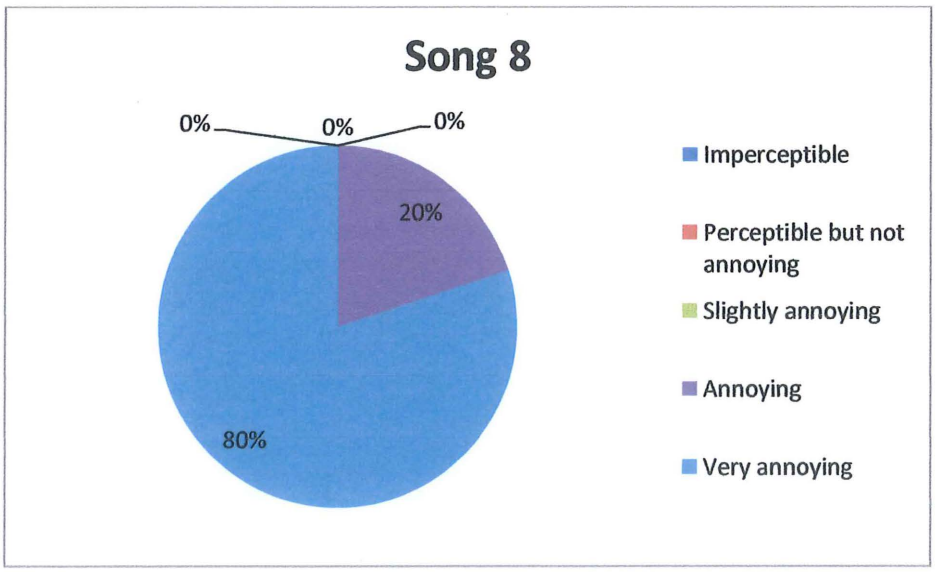
Conclusion: 19 people found that the audio sound is imperceptible. Another 11 people found that the audio sound is perceptible but not annoying.

Figure 32: Pie chart of the Song 7. Secret messages embedded in LSB 4.



Conclusion: 15 people found that the audio sound is perceptible but not annoying. But have 6 people found that the audio sound is imperceptible and 9 people found that the audio sound is slightly annoying.

Figure 33: Pie chart of the Song 8. Secret messages embedded in LSB 16.



Conclusion: 24 people found that the audio sound is very annoying.

4.3 RETRIEVED PROCESS

The secret messages were embedded into an audio WAV file by using the LSB method. Once the secret messages is success to embed in the audio file, which mean the secret massages can also be retrieve from the embedded file. The process of retrieve will be show below.

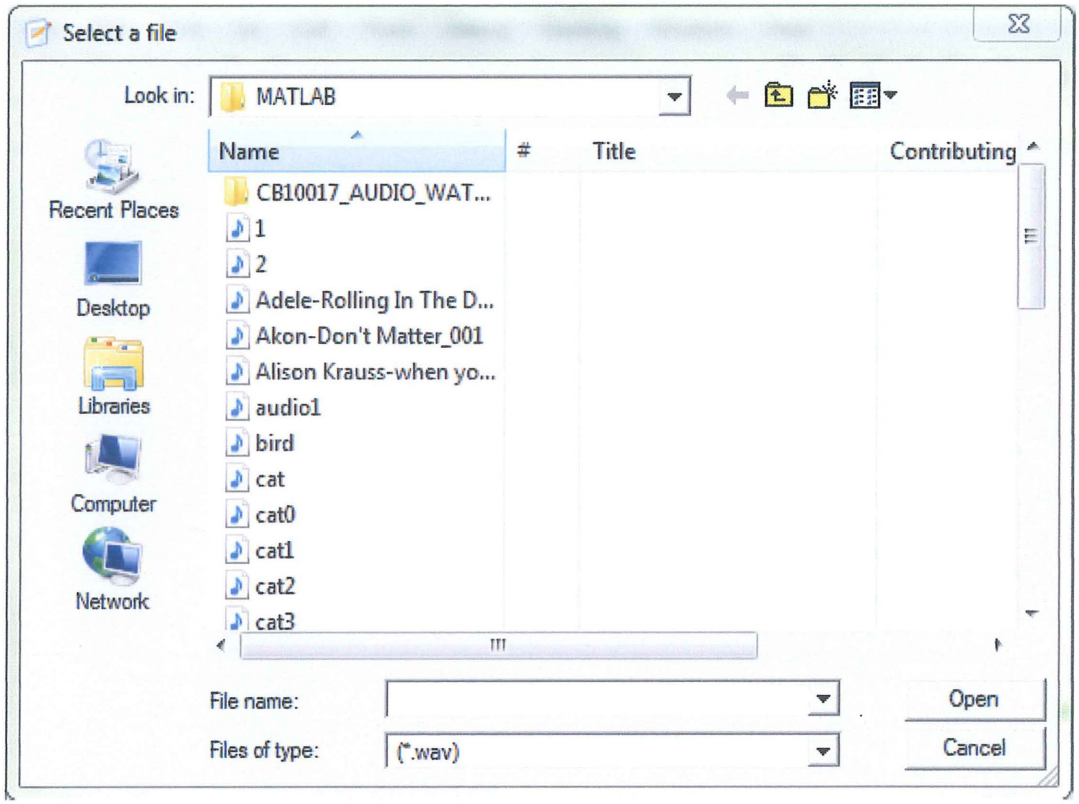


Figure 34: Choose the file and click open to retrieve the secret messages.

```
Command Window
  Hidden Message

  secmsg =

  hello i am ho man yen. nice to meet you.
```

Figure 35: The secret messages will show in the command window.

4.4 CONCLUSION

In this chapter, the process of audio steganography by using LSB method to embed and retrieve secret messages is proposed. The experimental result show that the quality of audio will affect by the secret messages while embedded into audio WAV file.

The SNR of the embedded audio WAV file show that the effect on quality in audio steganography will affect by the secret messages size of embedded, audio WAV file size and also the LSB for embed secret messages. The survey result also match the result of SNR. It can be conclude that, the lower the SNR, the noisy the audio sound and the higher the SNR, the better the audio sound.

The proposed LSB method has a 100% success rate for embedded and retrieved secret messages for audio WAV file. The result show that the LSB method perform well to embed secret messages into an audio WAV file.

CHAPTER 5

CONCLUSION AND DISCUSSION

5.1 INTRODUCTION

This chapter consists of section 5.2 that lists the contributions and limitations of the thesis. Section 5.3 describes the future work based on the outcome of this thesis. Lastly, section 5.4 summarizes the chapter.

5.2 CONTRIBUTIONS AND LIMITATIONS

The contributions of the thesis are as listed below:

In conclusion, LSB method can be used to embed and retrieve secret message and no one will suspect the existence of the hidden message except the sender and recipient.

In chapter 4, the testing result of SNR is show. The quality of the audio sound is imperceptible when the secret message is embedded from LSB 1 to LSB 3. There can be embed a huge size of secret message if the secret message is embedded in LSB 1 to LSB 3.

The survey result for the listening test are related to the SNR results. If the SNR is higher, there are many people found that the audio sound is imperceptible. If the SNR is lower, there are many people found that the audio sound is annoying.

The purposed LSB method has a 100% success rate for embedding and retrieving for audio steganography. Exact retrieved was achieved where the secret message will recover from the embedded audio.

The limitation are as below:

The limitation is that the audio quality will be affect if the secret message is embedded in LSB 4 and above.

Besides, if the message size is almost as big as the audio size, the audio quality will be affect too.

5.3 FUTURE WORK

Future work should be done to do much more test of LSB method and improve the LSB method. Since currently the audio quality resources are limited, more tests may make the result much clearer and more accurate.

Besides, LSB method can be proposed to develop into an application, so that people can hide the secret message into audio file. Based on the survey result, the application can develop for user to hide the secret message up to LSB 3.

Furthermore, a more advance application can be develop. The application can used to hide image and audio into audio file. It is not only for hiding text message into audio file.

5.4 SUMMARY

This chapter presented the research summary as well as the contributions and limitations of the research. The outcome from this research has opened up some possibilities for future work. Based on the results and evaluations, the objectives of this research outlines in chapter 1 had been achieved.

REFERENCES

AA, A., X, S. & H, Y., 2010. Information Technology Journal. *Robust adaptive image watermarking using visual models in DWT and DCT domain,* 9(3), pp. 460- 466.

Anderson, R. J. & Petitcolas, F. A., May 1998. IEEE Journal of Selected Areas in Communications. *On The Limits of Steganography,* 16(4), pp. 474- 481.

A, N. & K, G. A., 2011. International Conference on VLSI, Communications and Instrumentation. *Textual Information Encryption and Decryption in Multimedia Audio using VLSI technology,* pp. 5- 9.

Djebbar, F., Ayad, B., Meraim, K. A. & Hamam, H., 2012. EURASIP Journal on Audio, Speech, and Music Processing. *Comparative study of digital audio steganography techniques.*

Jasril, Marzuki, I. & Rahmat, F., December 2013. International Journal on Smart Sensing and Intelligent System. *Capacity Enhancement of Messages Concealment in Image and Audio Steganography,* 6(5).

Kiah, M. et al., 18 August 2011. International Journal of the Physical Sciences. *A review of audio based steganography and digital watermarking,* Volume 6(16), pp. 3837- 3850.

Kriti, S. & Kumar, S. P., December 2010. International Journal of Computer Applications. *A Variant of LSB Steganography for Hiding Images in Audio,* 11(6), pp. 12- 16.

Malik, H. & Kang, S. S., August 2013. International Journal of Advanced Research in Computer Science and Software Engineering. *Designing and Evaluation of Performance of a Spread Spectrum Technique for Audio Steganography* , 3(8).

Malviya, S., Saxena, M. & Khare, A., July 2012. International Journal of Emerging Technology and Advanced Engineering. *Audio Steganography by Different Methods,* 2(7).

Medani A, G. A. Z. O. Z. A., 2011. Scientific Research and Essays. *Review of mobile short message service security issues and techniques towards the solution,* 6(6), pp. 1147- 1165.

Nehru, G. & Dhar, P., January 2012. IJCSI International Journal of Computer Science Issues. *A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach,* 9(1), p. 2.

Sujay, N. & Gaurav, P., December 2010. Signal & Image Processing: An International Journal (SIPIJ). *Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions,* 1(2), pp. 60- 73.

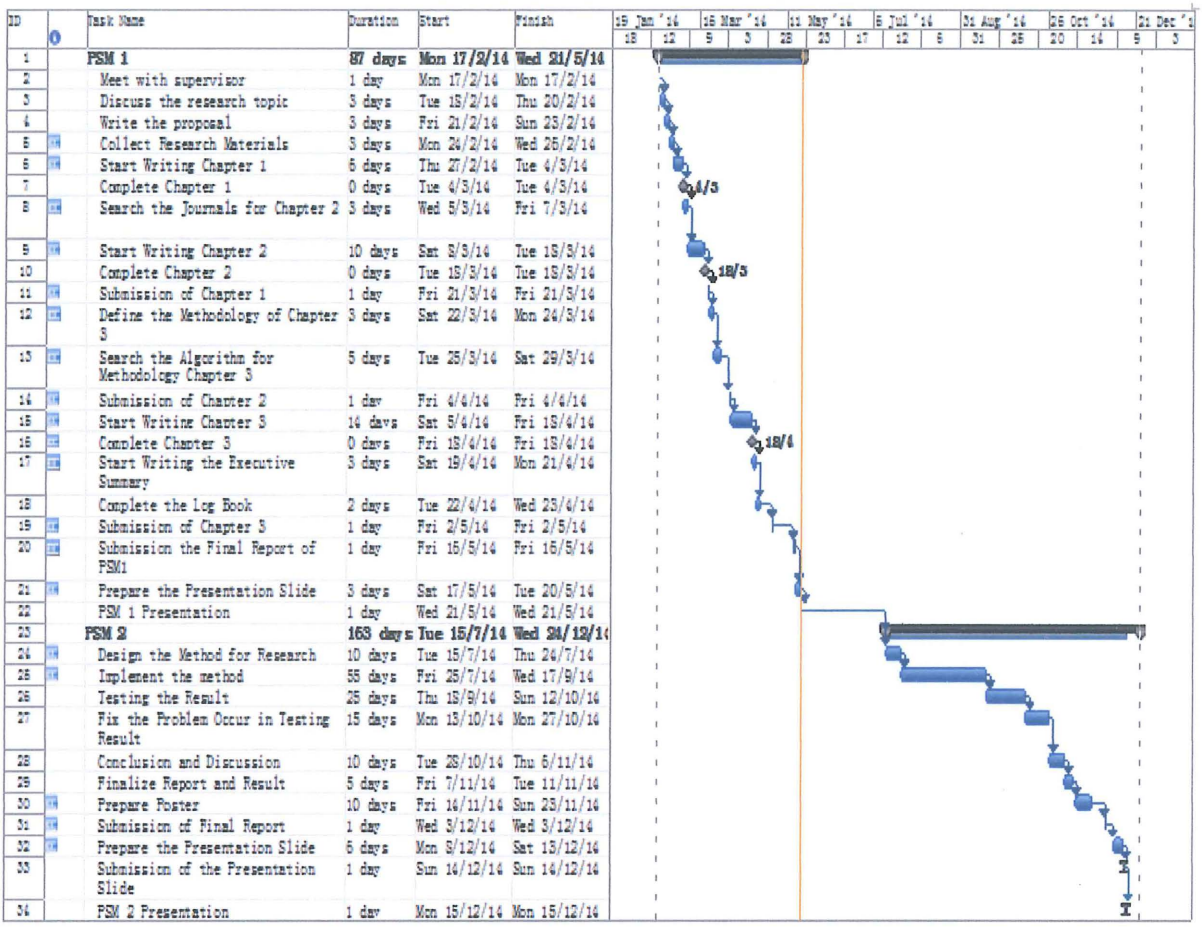
Venkateswaran, R. & V.Sundaram, 2011. (IJACSA) International Journal of Advanced Computer Science and Application. *Implementation of ISS - IHAS (Information Security System - Information Hiding in Audio Signal) model with reference to proposed e-cipher Method,* 2(6).

Y, L. & WH, A., 2008. International Conference on Acoustics, Speech, and Signal Processing. *Perceptual evaluation of audio watermarking using objective quality measures,* pp. 1745- 1748.

Y, Z., ZM, L. & DN, Z., 2010. Information Techonology Journal. *A blind image watermarking scheme using fast hadamard transform,* Volume 9, pp. 1369- 1375.

APPENDICES

GANTT CHART



ID	Task Name	Duration	Start	Finish
1	**PSM 1**	**87 days**	**Mon 17/2/14**	**Wed 21/5/14**
2	Meet with supervisor	1 day	Mon 17/2/14	Mon 17/2/14
3	Discuss the research topic	3 days	Tue 18/2/14	Thu 20/2/14
4	Write the proposal	3 days	Fri 21/2/14	Sun 23/2/14
5	Collect Research Materials	3 days	Mon 24/2/14	Wed 26/2/14
6	Start Writing Chapter 1	6 days	Thu 27/2/14	Tue 4/3/14
7	Complete Chapter 1	0 days	Tue 4/3/14	Tue 4/3/14
8	Search the Journals for Chapter 2	3 days	Wed 5/3/14	Fri 7/3/14
9	Start Writing Chapter 2	10 days	Sat 8/3/14	Tue 18/3/14
10	Complete Chapter 2	0 days	Tue 18/3/14	Tue 18/3/14
11	Submission of Chapter 1	1 day	Fri 21/3/14	Fri 21/3/14
12	Define the Methodology of Chapter 3	3 days	Sat 22/3/14	Mon 24/3/14
13	Search the Algorithm for Methodology Chapter 3	5 days	Tue 25/3/14	Sat 29/3/14
14	Submission of Chapter 2	1 day	Fri 4/4/14	Fri 4/4/14
15	Start Writing Chapter 3	14 days	Sat 5/4/14	Fri 18/4/14
16	Complete Chapter 3	0 days	Fri 18/4/14	Fri 18/4/14
17	Start Writing the Executive Summary	3 days	Sat 19/4/14	Mon 21/4/14
18	Complete the Log Book	2 days	Tue 22/4/14	Wed 23/4/14
19	Submission of Chapter 3	1 day	Fri 2/5/14	Fri 2/5/14
20	Submission the Final Report of PSM1	1 day	Fri 16/5/14	Fri 16/5/14
21	Prepare the Presentation Slide	3 days	Sat 17/5/14	Tue 20/5/14
22	PSM 1 Presentation	1 day	Wed 21/5/14	Wed 21/5/14
23	**PSM 2**	**163 days**	**Tue 15/7/14**	**Wed 24/12/14**
24	Design the Method for Research	10 days	Tue 15/7/14	Thu 24/7/14
25	Implement the method	55 days	Fri 25/7/14	Wed 17/9/14
26	Testing the Result	25 days	Thu 18/9/14	Sun 12/10/14
27	Fix the Problem Occur in Testing Result	15 days	Mon 13/10/14	Mon 27/10/14
28	Conclusion and Discussion	10 days	Tue 28/10/14	Thu 6/11/14
29	Finalize Report and Result	5 days	Fri 7/11/14	Tue 11/11/14
30	Prepare Poster	10 days	Fri 14/11/14	Sun 23/11/14
31	Submission of Final Report	1 day	Wed 3/12/14	Wed 3/12/14
32	Prepare the Presentation Slide	6 days	Mon 8/12/14	Sat 13/12/14
33	Submission of the Presentation Slide	1 day	Sun 14/12/14	Sun 14/12/14
34	PSM 2 Presentation	1 day	Mon 15/12/14	Mon 15/12/14

Survey Question for Effects on Quality in Audio Steganography

This survey questions is for the use of the Undergraduate Project. The purpose of having this survey is to collect the audio quality test result from all social group.

Please **Tick** (√) on the correct option.

Gender ☐ Male
☐ Female

Social Group ☐ Senior Citizen
☐ Adult
☐ Teenager
☐ Children

Please answer the question **1 to 8** below by listen to the songs given. **Circle** the relevant grade.

Subjective Difference Grade:
5: Imperceptible
4: Perceptible but not annoying
3: Slightly annoying
2: Annoying
1: Very annoying

Please listen to the **original song (original.wav),** then answer the **question 1- 4.**

Song Name	**Grade**				
1. Song 1	5	4	3	2	1
2. Song 2	5	4	3	2	1
3. Song 3	5	4	3	2	1
4. Song 4	5	4	3	2	1

Please listen to the **original song (audio.wav),** then answer the **question 5- 8.**

5. Song 5	5	4	3	2	1
6. Song 6	5	4	3	2	1
7. Song 7	5	4	3	2	1
8. Song 8	5	4	3	2	1