MP3 AUDIO STEGANOGRAPHY TECHNIQUE USING EXTENDED LEAST SIGNIFICANT BIT

MOHAMMED SALEM MOHAMMED ATOUM

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

MAY 2014

To soul of my late father

To my beloved mother

To my beloved sisters and brothers

To my beloved wife and sons

ACKNOWLEDGEMENTS

I would like to thank my principal supervisor Assoc. Prof. Dr. Subariah Ibrahim for her guidance during my research and study. Her perpetual energy and enthusiasm in research had motivated all his advisees, including me. In addition, she was always accessible and willing to help her students with their research. As a result, research life became smooth and rewarding for me. I would also like to thank my co-supervisor, Prof. Dr. Ghazali Sulong, for his support and encouragement. His contribution by far has dominantly influenced my focus and motivation toward it. I especially want to thank Prof. Dr. Azizah Abdul Manaf, and Prof.Dr. Jasni Mohamad as my thesis committee members. They read my thesis rigorously and helped me to correct it.

I also would like to thank all staff in Universiti Teknologi Malaysia (UTM) and all staff in Irbid Nation University (INU) in Jordan for funding my research and study.

I would like to thank my mother for offering their full support, encouragement and love throughout my life. Finally, I want to express my deepest feelings to my wife, family and friends for their constant supports, encouragement and understanding during the period of my studies.

ABSTRACT

Audio Steganography is the process of concealing secret messages into audio file. The goal for using audio steganography is to avoid drawing suspicion to the transmission of the secret message. Prior research studies have indicated that the main properties in steganography technique are imperceptibility, robustness and capacity. MP3 file is a popular audio media, which provides different compression rate and performing steganography in MP3 format after compression is the most desirable one. To date, there is not much research work that embeds messages after compression. An audio steganographic technique that utilizes Standard Least Significant Bits (SLSB) of the audio stream to embed secret message has gained popularity over the years. Unfortunately the technique suffers from imperceptibility, security and capacity. This research offers an extended Least Significant Bit (XLSB) technique in order to circumvent the weakness. The secret message is scrambled before embedding. Scrambling technique is introduced in two steps; partitioning the secret message (speech) into blocks followed by block permutation, in order to confuse the contents of the secret message. To enhance difficulty for attackers to retrieve the secret message, the message is not embedded in every byte of the audio file. Instead the first position of embedding bit is chosen randomly and the rest of the bits are embedded only in even value of bytes of the audio file. For extracting the secret message, the permutation code book is used to reorder the message blocks into its original form. Md5sum and SHA-256 are used to verify whether the secret message is altered or not during transmission. Experimental results measured by peak signal to noise ratio, bit error rate, Pearson Correlation and chi-square show that the XLSB performs better than SLSB. Moreover, XLSB can embed a maximum of 750KB into MP3 file with 30db average result. This research contributes to the information security community by providing more secure steganography technique which provides message confidentiality and integrity.

ABSTRAK

Steganografi audio adalah proses penyembunyian mesej rahsia ke dalam fail audio. Matlamat menggunakan steganografi audio adalah untuk mengelakkan daripada kecurigaan penghantaran mesej rahsia. Kajian penyelidikan sebelum ini, menunjukkan bahawa ciri-ciri utama dalam teknik steganografi adalah ketidakkelihatan, keteguhan dan muatan. Fail MP3 ialah fail audio yang popular, yang menyediakan kadar pemampatan yang berbeza dan melaksanakan steganografi dalam format MP3 selepas pemampatan adalah yang paling wajar. Sehingga kini, tidak banyak kerja penyelidikan yang membenam mesej selepas pemampatan. Teknik steganografi audio yang menggunakan bit terkurang bererti yang piawai (SLSB) untuk strim audio untuk membenamkan mesej rahsia mendapat sambutan sejak beberapa tahun. Malangnya teknik ini, mengalami masalah ketidakkelihatan, keselamatan dan muatan. Kajian ini menawarkan teknik lanjutan bit terkurang bererti (XLSB) untuk mengatasi kelemahan ini. Mesej rahsia dicampuraduk sebelum pembenaman. Teknik pencampuradukan diperkenalkan dalam dua langkah; pembahagian mesej rahsia (ucapan) ke blok-blok, diikuti dengan pilih atur blok untuk mengelirukan kandungan mesej rahsia. Untuk menambah kesukaran penyerang untuk mendapat semula mesej rahsia, mesej ini tidak dibenamkan dalam setiap bait fail audio. Kedudukan pertama bit yang dibenamkan dipilih secara rawak dan bit-bit seterusnya dibenam hanya dalam bait yang bernilai genap. Untuk mendapat kembali mesej rahsia, buku kod pilih atur digunakan untuk menyusun semula ke dalam bentuk asalnya. Md5sum dan SHA-256 digunakan untuk mengesahkan sama ada mesej rahsia itu diubah atau tidak semasa penghantaran. Keputusan eksperimen diukur dengan nisbah isyarat-hingar piksel, kadar ralat bit, korelasi Pearson dan khi kuasa dua menunjukkan bahawa XLSB prestasi lebih baik daripada SLSB. Selain itu, XLSB boleh membenam sehingga 750KB ke dalam fail MP3 dengan hasil purata 30dB. Kajian ini menyumbang kepada komuniti keselamatan maklumat dengan menyediakan teknik steganografi lebih selamat dengan menyediakan kerahsiaan dan integriti mesej.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

bps	-	Bit Per Sample
PN	-	Pseudorandom Number
CD	-	Compact Disc
CWT	-	Continuous Wavelet Transform
db	-	Decibel
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DVD	-	Digital Video Disc
DWT	-	Discrete Wavelet Transform
EOF	-	End-of-File
GA	-	Genetic Algorithm
HAS	-	Human Auditory System
HVS	-	Human Visual System
Hz	-	Hertz
Kbits	-	Kilo bits
Kbps	-	Kilo Bit Per Sample
KHz	-	Kilohertz
LSB	-	Least Significant Bit
MDEC	-	Minimizing the Distortion in the Equivalence Class
MPEG	-	Moving Picture Experts Group
MSE	-	Mean-Square-Error
PSNR		Peak Signal-to-Noise Ratio
RIFF	-	Resource Interchange File Format
SNR	-	Signal-to-noise ratio
STFT	-	Short-Time Fourier Transform
WAVE	-	Waveform Audio File Format

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

Information is shared globally through the Internet, in digital form (Fricker and Rand, 2002). There are issues and challenges regarding the security of information in transit from senders to receivers. The major issue is the protection of digital data against any form of intrusion, penetration, and theft. The major challenge is developing a solution to protect information and ensure their security during transmission (Feruza and Kim, 2007). Three components of information security are confidentially, integrity, and availability (Feruza and Kim, 2007). Confidentiality ensures that information is kept secret from any unauthorized access. This could be done through information hiding techniques, namely cryptography and steganography (Lenti, 2000).

Cryptography involves the act of encryption and decryption of a digital data. The major weaknesses of such techniques are that even though the message has been encrypted, it still exists. Steganography dwells on concealing any digital data in a in an innocuous digital carrier, the word steganography is derived from an old Greek word which means covered writing (Katzenbeisser and Petitcolas, 2000).

Steganography has been used of concealing secret messages during ancient times (Rahim, Bhattacharjee and Aziz, 2014). It was used by Histiaeus, the tyrant of Miletus who, in 499 BC, tattooed the scalps of his slaves with a hidden message with a command for his men to attack the Persian (Ricardo, 1999; Huayin and Li, 2008; Emelia, Sugathan and Ho, 2008; Yu *et al.,* 2010). The message became hidden when the slaves' hair grew back. According to researchers, steganography can be described as a study of the means of hiding secondary information within primary information without affecting the size of information nor the cause of any form of distortion which could be perceived (Francia and Gomez, 2006; Liu, Qiao and Sung, 2009a; Liu, Qiao and Sung, 2009b; Ganeshkumar and Koggalage, 2009; Petrovic and Yang, 2009; Lee *et al.*, 2009; Jangra, and Singh, 2014).

The primary information, known as the carrier or host, was embedded within the secondary information, which is typically hidden and could be in the form of a file or message. The media with the embedded information is called stego signal, file, bit stream or sequence (Matthews, 2003; Basu and Bhoumik, 2010; Khairullah, 2009; Alla, Parsad and Siva, 2009; Changder, Debnath and Ghosh, 2009; Qi, Ye and Liu, 2009; Farouk, 2014). Steganography is one of the two techniques used for covert communication. However, watermarking is the second technique that can embed watermark into host cover to keep copyright for the hosts. Steganography typically establishes point-to-point data security (Mandala, Kotagiri and Kapala, 2013). The strength of steganographic technique in keeping the data in the carrier medium against attacks or alteration is weak during transmission, storage or format conversion is weak (Katzenbeisser and Petitcolas, 2000).

The process of embedding information in host media in steganography technique and watermarking are usually done transparently (Manimegalai *et al.*, 2014; Koziel, 2014). The difference between steganography and watermarking is that while steganography is a technique which hides the information, visible watermarking actually allows the third person to see the message (Cvejic and Sebbanen, 2004; Neeta, Snehal and Jacobs, 2006). Thus, in terms of watermarking

visible and invisible, the process needs to ensure robustness so that any intentional attacks would not compromise, remove, or cause destruction of the information in any way in the marked media while at the same time preserving the quality of the signal (Scagliola, Berez and Guccione, 2009; Bhattacharyya and Sanyal, 2012). The invisible watermarking technique is the most suitable technique in cases where knowledge of the hidden information could cause possible manipulations (Yusnita and Othman, 2007; Naji *et al.*, 2009).

1.1 Problem Background

In steganography technique different media types such as image, audio, video and text can be used to embed as secret message into cover (Gomez-Coronel *et al.*, 2014). The techniques of steganography were originally developed and used for images. Researchers in the field then began to study how the techniques could be used on audio media. Hence, the introduction and development of the known algorithms for the audio steganography was developed. The steganography technique is still mostly used for images and there are not many methods for audio steganography and steganalysis. Audio steganography provides considerably better security (Cvejic, 2004). Using steganography in audio files is more difficult than in other types of media because the human auditory system (HAS) is more sensitive than other media systems such as the human visual system (HVS) (Cvejic and Seppanen, 2004).

There are three fundamental properties which serve as restrictions for steganography designers (Westfeld *et al.*, 2013). They are imperceptibility, robustness, and capacity. However, other properties should also be taken into consideration when dealing with different types of applications (Andres, 2002; Al-

Othmani, Manaf and Zeki, 2012). Computational time and delay are the two factors that could be certain in real time applications of steganography such as output screens of the instrument, which could determine the efficiency of the technique. Delay is another important variable in the same application. Other example of real time application is related to broadcast monitoring which involves real time processing and therefore cannot be tolerated (Andres, 2002; Venkatraman, Abraham and Babrzycki, 2004).

Imperceptibility refers to how the host or original signal and the completely embedded stego signal could be perceived without clearly seeing the difference between the original signal and the stego audio signal. The evaluation of imperceptibility in audio steganography could be managed by evaluating the audible distortion which is results in signal change. Some methods for measuring imperceptibility include performing listening tests and Peak Signal-to-Noise Ratio (PSNR) etc. The embedded information has a fidelity constraint which ensures that the perceptual distortion does not exceed the estimated threshold and is based on the HAS (Andres, 2002; Cvejic, 2004; Zamani *et al.*, 2009a).

Robustness is measured by the capability of the embedded information to withstand security attacks that is intentional or otherwise. An intentional attack is usually in the form of degradation, resizing or filtering of the media while manipulation of the media is considered a type of unintentional attack. Some applications require predefined level of robustness, which is why such applications involve a set of signal processing modifications such as watermarking techniques in fingerprint, copyright and authentication. Other applications, which have no prerequisite for any amount of robustness, are often called fragile audio watermarking techniques (Andres, 2002; Cvejic, 2004; Zamani *et al.*, 2009b; Park, 2013).

Capacity indicates the amount of information which could be successfully hidden by an information hiding technique. The capacity of a particular technique should also ensure that the embedded information does not cause obvious perceivable distortions. The measurements of the payload, capacity or bit rate are in bits per second (bps) (Andres, 2002; Cvejic and Seppanen, 2007; Zamani *et al.*, 2009c; Kamble *et al.*, 2013).

The three fundamental properties imperceptibility, robustness and capacity form a magic triangle. Magic triangle helps to visualize the requirements of audio steganography. Figure 1.1 shows the magic triangle of steganography properties. The corners of the triangle represent imperceptibility, robustness and capacity. The capacity and the robustness cannot be equally high in steganography. Therefore, in order to achieve a highly robust steganography algorithm, the embedding of the capacity should be low and vice versa. Furthermore, high capacity usually results in a fragile algorithm because high embedded results get a low imperceptibility results. Moreover, that increases the probability of attacker to detect the secret message and retrieve it (Cvejic, 2004).

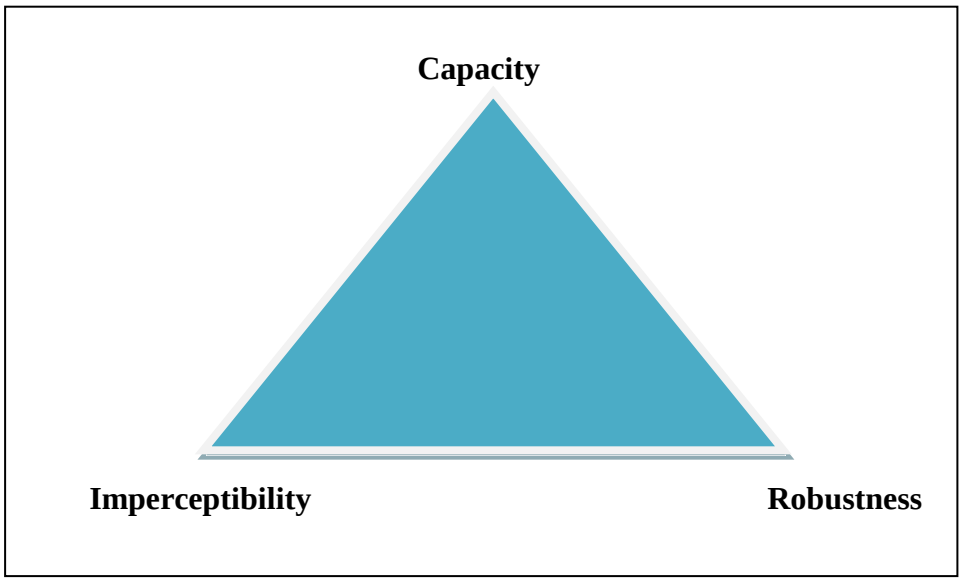

Figure 1.1 The Magic triangle for steganography properties

Referring to the basic model of steganography two processes embedding and extracting are aims to embed and extract respectively the secret message from cover.

The embedding process is concerned to generate stego object after embedding the secret message into cover. The extraction process is concerned with extracting secret message from stego object. However, using keys for embedding could increase the security for the basic model (Amin *et al*., 2003; Khairullah, 2009; Qi, Ye and Liu, 2009).

The designer of steganography followed general steps to generate a stego object. Firstly convert both the secret message and cover into bit stream, and secondly use any embedding algorithm to embed the bit stream of the secret message into cover. If the secret message is embedded directly into cover, it will be much easily for attacker to retrieve the secret message when they detect it. In order to avoid the secret message can be scrambled before embedding. Encryption and encoding are the two current techniques which using in message scrambling. Steganographic designers are used that methods to increase the confusion content of the secret message. The drawbacks of the encryption process are complexity of the procedure as well as decrease the capability of the secret message (Asad, Gilani, and Khalid, 2011). On the other hand, the drawbacks of encoding process are increased computational complexity in addition to the potential loss of some of the message contents. The designers of steganography usually embed secret messages in covers without taking message preparation into consideration (Byandenburg, 1999; Deng, 2010).

Audio file is one of the media types can be used as a cover in steganography technique. One of the problems in audio steganography is when the payload needs to be high; however, high payload will result in intolerable noise and reduced robustness. In short, one of the principal problems in steganography is embedding a huge amount of data while at the same time maintaining the robustness and quality of audio files (Chan and Cheng, 2004; Cvejic, 2004; Quan and Zhang, 2006; Deng *et al*., 2010; Chan, 2011; Devi, 2013).

In audio steganography, many types of files can be used as a cover for steganography, such as Waveform Audio File Format (WAVE, or more commonly known as WAV due to its filename extension) or MPEG-1 or MPEG-2 Audio Layer III (MP3). Likewise, secret messages that can be embedded as secured types, such as text or speech. MP3 is the most popular compression format for digital audio. In steganography which uses MP3 as a cover, the secret message could be embedded during and after compression (Chan, 2011; Deng *et al*., 2010).

Nowadays, there are many audio hiding methods, which commonly include least significant bit (LSB), phase coding, spread spectrum, and echo hiding (Bender *et al*., 1996; Gruhl, Lu and Bender, 1996; Kirovski, Malvar and Yacobi, 2002; Gupta and Sharma, 2013). However; these methods are designed for the uncompressed audio format. If such algorithms were applicable in compressed audio format, it would create two significant problems. First, it would require that the decoding/coded procedure to achieve data hiding. This would greatly increase the computational complexity. Second, it is possible to miss the mystery information in the decoding/coded procedure (Deng *et al*., 2010). The information-hiding algorithms that work directly in the compressed domain could prevent these problems. Therefore, it is extremely desirable to produce an audio information hiding algorithm that works in the compressed domain.

The development of steganography software called the MP3Stego is specific for the MP3 audio media (Petitcolas, Anderson and Kuhn, 1999). The software embeds secret messages based on the parity of error length after audio quantizing and coding. Nevertheless, it cannot match the real-time requirement and its capacity is too low. In modifying the scale factor of MPEG, audio bit stream embeds the secret message. However, the results for testing the robustness were not discussed in this scheme (Qiao, Sung and Liu, 2009).

Neubauer (2000) embedded digital steganography in the compressed domain of Advanced Audio Coding (AAC) audio. In this scheme, secret messages could be extracted with ancillary data calculated using the psychoacoustic model. Therefore, it would significantly increase computational complexity. Another researcher employed wet paper codes and hid data directly in the MPEG audio bit stream by modifying the MPEG audio quantization process (Quan and Zhang, 2006). The drawback is that the scheme could change the size of the audio file.

Embedding during compression generally hides information by modifying the Discrete Cosine Transform (DCT) quantization coefficients, Discrete Wavelet Transform (DWT) quantization coefficients, and is complex and requires the original .wav audio file. Having to hold the original audio file makes the hiding process tedious. However**,** there is error accumulation and low capacity with this strategy (Chan, 2011; Deng *et al*., 2010). The efficiency of embedding after compression is increased without requiring encoding and decoding process during embedding and extraction (Chan, 2011; Deng *et al*., 2010).

In recent years, several methods for embedding secret messages after MP3 compression have been proposed. Most of them can be easily modified for the purpose of steganography. However, the researchers used different position for embedding secret messages, such as unused bit or padding stuffing or between frames or before all frames or audio data. Nevertheless, the different sizes and types of secret message were used, such as text or image. The researchers applied methods with different sizes of MP3 files (non-standard data set), such as 3MB or 5MB or 6 MB or 12MB. In the experimental result, researchers found that the hiding capacity and security were very low and most of them use cryptography techniques to increase security. Most methods do not embed secret messages in the audio to ensure the quality of sound (Maciak, Ponniah and Sharma, 2005, Zaturenskiy,2009; Chan 2011; Atoum *et al*., 2011a; Atoum *et al*., 2011b; Bhattacharyya , Kundu and Sanyal, 2011, Bhattacharyya *et al*., 2011; Zaturenskiy,2013).

An important point in using LSB in audio steganography is the simplicity to apply this technique and its higher capacity compared to other techniques in audio steganography. But it is still has two drawbacks. Firstly, it is not efficient in that the human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file. Secondly, the technique is not robust (Cvejic, 2004; Quan and Zhang, 2006; Zamani *et al*., 2009b; Deng *et al*., 2010; Bhowal *et al.*, 2010; Chan, 2011; Chandrakar, Choudhary and Badgaiyan, 2013). The simple way to embed secret message into cover is by embedding sequentially. However, this technique allows and enables the attacker to retrieve the secret message easily.

Previous research studies has shown that on average, the maximum LSB depth that can be utilized for audio steganographic technique without causing noticeable perceptual distortion is the fourth LSB layer when 16 bits per sample audio sequences were used, audio quality and evaluation showed that; the method succeeded in increasing the depth of the embedding layer to seventh LSB layer (Kekre, *et al*., 2010).

All methods of audio steganography produce embedding digital information, such as secret message text or code. From other points of view, there is a scientific interest to design methods and algorithms that would allow the embedding of human speech signal. Unlike texts that represents impersonal information, speech and voice signals look like human fingerprints. Speech and voice are personal identification information. Furthermore, numerous researches have shown that speech signals contain linguistic, expressive, organic (Pickett *et al*., 1999) and biological information (Skopin *et al*., 2010). This is the reason why, in some cases, secure transmission of messages embedded in speech signal is an extremely important problem.

Skopin *et al*., **(**2010) have developed algorithms to embed speech in MP3 by using spectrum-spreading algorithm and shift spectrum algorithm. The researchers found that the spectrum-spreading algorithm caused sufficiently significant audio quality degradation compared to shift spectrum algorithm. Increasing voice signal attenuation increases audio quality to an acceptable quality level. Nonetheless, both proposed algorithms of audio steganography do not change the voice properties and voice tone. Nevertheless, storing a stenographical data in MP3, which is in a form of lossy data compression, is to reduce objective differences in quality grade by 0.5 when the data is stored with the maximum bit rate of 320 Kbps. Less MPEG bit rate causes significant degradation of voice quality starting from data speed of 192 Kbps and some noise will also be heard.

The important to the security of information, is integrity, which is the situation where inputs and outputs converge to the same point. This means that the message send should be ensure that it are kept intact while in the transmission medium. The process that will validate if the message is altered or not during the transmission is called message integrity.

A few methods have been developed in image steganography that provide message integrity. Generating codes from coefficient in DCT domain is the techniques can apply to achieve message integrity in an image cover (Potdar, Han and Chang, 2005). These techniques not concern for the security, which ensure that since the content of the message, is neither altered nor modified or destroyed (Park *et al.*, 2006). In image steganography, this technique is not suitable, because there is probability that an attacker can detect the present of message from stego object and will easily change the validation code and eventually create a new validation code matching with the new embedded message, which tries to embed after modification. However, this could drag the suspicion of the presence of message embedded. The tendency with which the message could be extracted by the random bits is minimal, thus this could be vulnerable to the steganographic technique (Morekl, 2012).

1.2 Problem Statement

Prior research studies have shown that the main challenge in digital audio steganography is that human ear is very sensitive and can often detect even the slightest bit of noise introduced into an audio track. Crucial to that is the robustness and high capacity trade-off with which audio signal can endure in steganographic systems. In general audio steganography techniques always tend to meet two basic requirements; perceptual transparency, that is imperceptibility of stego file after embedding secret message and the ability for the stego file to withstand any form of intentional or un-intentional degradation (robustness). Many researchers attempt to meet this requirement when developing audio steganographic technique. Unfortunately, as of the time of writing this research, to the best of our knowledge, these two challenges still remain the major problems of audio steganography

Nowadays, there are many audio hiding methods which commonly include least significant bit (LSB), phase coding, spread spectrum, and echo hiding. But these methods are designed for the uncompressed audio format. However, if such algorithms are applicable in compressed audio format, it would create two significant problems. First, it needs the decoding/coding procedure to achieve the data hiding. It would increase the computational complexity greatly. Second, it is possible to lose the secret information in the decoding/coding procedure. Moreover the software named MP3Stego is developed to embed secret message during compression but unfortunately it cannot meet the real-time requirement and its capacity is too low.

The main problems of using MP3 audio format after compression are low security and capacity. Most current methods embed the secret message in the header of frames rather than in the body of the audio track streams. Moreover, embedding secret message into the header frames can be easily detected since the position of header frames can be determined.

Audio steganographic technique that utilizes LSB of audio stream to embed secret message gain a lot of popularity over the years in meeting the perceptual transparency requirement. Unfortunately the technique suffers from security and capacity of audio steganographic requirements. This is because embedding in normal LSB embedding technique, the inserted bits changes the statistical properties of one part of the audio stream and give a pattern with which could be easily predicted by an attacker, leading to a security problem, since it can tracked (Cvejic, 2004; Quan and Zhang, 2006; Zamani *et al*., 2009b; Deng *et al*., 2010; Bhowal *et al*., 2010; Geetha and Muthu, 2010). Furthermore, LSB embedding does not provide a step for encrypting data, and if secret message is sequentially or randomly embedded and attackers know this pattern of embedding the message, they can obtain the message. Although, validation code is the current methods that implements message integrity in LSB steganography, unfortunately this method suffers from security problems because the validation code is stored in the stego object. Thus, there is a possibility to extract the validation code and change the content of the secret message. LSB technique also adds noise into the cover data, the ratio of audio stream to the stego file is not always balance, and this directly affects one of the requirements of audio steganographic system capacity. As a result an eXtended Least Significant Bits (XLSB) technique is proposed in this research to circumvent the weakness stated above.

1.3 Research Questions

Based on the review of related works and preliminary study, three key research questions are posed to represent the main areas to be examined in this research. Limiting research questions to three or four allows a narrow focus, and does not lead to overly constraining the research (Groenewald, 2004).

The main research question is: How to design and develop a secure scheme to embed speech in an MP3 file which provides high hiding capacity without affecting the imperceptibility of MP3?

Several other questions relating to this are:

i. How to enhance the security of secret message in steganographic technique
ii. What capacity MP3 audio signal as a cover file can endure in extended least significant bit steganographic systems
iii. What could be the strength of embedding technique against intentional or unintentional degradation of embedded file in MP3 audio extended least significant bit steganographic systems
iv. What message integrity method will be suitable for MP3 extended least significant bit audio steganography?

1.4 Research Aims

The main aim of this research is to provide a new MP3 steganography technique based on LSB approach in order to address the issues of robustness, imperceptibility, capacity and integrity.

1.5 Research Objectives

This study dwells on providing extended least significant bit (XLSB) MP3 audio steganographic technique that will circumvent the drawbacks studied in the LSB techniques. The specific objectives are:

i. To enhance security of secret message before embedding through scrambling the secret message
ii. To design algorithm for MP3 audio extended least significant bit steganographic systems capable of solving capacity problems observed in LSB technique
iii. To design message integrity method suitable for MP3 for the proposed extended least significant bit audio steganographic algorithm

1.6 Research Scope

This research focuses on extending LSB technique on MP3 audio files. The unit of analysis is capacity, robustness, and security of the proposed technique.The following are the highlights:

i. Embedding speech into MP3 audio format after compression
ii. Using spatial domain
iii. Extending LSB algorithm
iv. This research does not focus on real time application.

1.7 Organization of the Report

This thesis consists of five major parts, excluding the introductory chapter which presented a background of the problem as well as outlined the purpose and objectives of the research. The importance and expected contributions of the research are also highlighted and emphasized. While the second part describes the research setting as well as previously published work in the field of audio steganography, the third part describes the scope of research. Finally, the last part presents the phases for research frameworks.

Chapter 2, the *Literature Review*, begins with an overview of information security and a comparison of steganography, watermarking, and cryptography. The existing literature on the main topic of research is steganography; the types, fundamental properties, and different various media and transmission environment are discussed. After presenting the description of the audio domain for steganography, the chapter presents the MP3 file structure. The second part explains the method of audio steganography and steganalysis to highlight current methods and introduce the advantages and disadvantage of each method in order to find the solutions for audio steganography. The steganalysis are also discussed the methods of attacks in order to discover the hidden message in convert message is presented. Message Integrity including hashing technique as well as scrambling methods are presented. Finally the chapter concluded with the summary of the applicability of the mentioned methods for audio steganography.

Chapter 3, *Research Methodology*, describes the overall methodology adopted in this research in order to achieve the objectives set.. The phases of the research framework are discussed in generate.. The data set are presented and explained. The step by step recording of the secret message and also the details of the cover message are presented here. The metrics for measuring performance (PSNR,

BER, Correlation and Chi-square) are presented. Finally the chapter concluded with a summary.

Chapter 4, *Design of the Proposed Scheme*: This chapter discusses the philosophy for the design of the proposed scheme and the two phases which were added to the basic model of steganography. The first phase is scrambling message, which includes two processes, namely message partition and message permutation are presented and discussed. The second phase is message integrity which includes two steps to generate secret information that will be sending to the end user in order to achieve message integrity. In addition, the propose XLSB *Embedding and Extraction Algorithms are* describes in details. The steps to enhance the LSB algorithm to make it more secure by choosing the first byte from first 10000 bytes to embed the secret message randomly, and using the bytes that start with zero value to complete the embedding of the secret message are presented. This chapter ends with a summary.

Chapter 5, *Results and discussion*; this chapter presents and analyses the experimental data used for the study. Three parameters imperceptibility, capacity, and robustness were obtained for both the standard LSB and the XLSB. Moreover, using standard benchmark, the XLSB with current method that are using MP3 file as a cover are compared and presented in this chapter. Finally, the chapter summary is presented.

The last chapter presents the *Conclusion and Future Work*, it discusses and concludes the overall work and highlights the findings and contributions made by this study and provides recommendations for the future research.

REFERENCES

Adhiya, K. P., and Patil, S. A. (2012). Hiding Text in Audio Using LSB Based Steganography. *In Information and Knowledge Management* (Vol. 2, No. 3, 8-14).

Ahmad, A.M. (2012), *a 2-Tier Data Hiding Technique using an Improved Exploring Modification Direction Method and Huffman Coding*. Master Thesis, Universiti Teknologi Malaysia.

Alla, K., Prasad, R., and Siva R. (2009). An Evolution of Hindi Text. *Journal of Computer Science*, 09(5), 113-117.

Al-Laham, M., and El Emary, I. M. (2007). Comparative Study Between Various Algorithms of Data Compression Techniques. *IJCSNS*, 7(4), 281.

Al-Najjar, Atef J., Aleem K. Alvi, Syed U. Idrees, and Abdul-Rahman M. Al-Manea. (2007). Hiding Encrypted Speech Using Steganography. *In 7th WSEAS International Conference on Multimedia*, Internet and Video Technologies (MIV'07), Beijing, China.

Al-Othmani, A. Z., Abdul Manaf, A., and Zeki, A. M. (2012). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation. *IJCSI-International Journal of Computer Science*, 9(1), 30-37.

Alsalami M. A. and Al-Akaidi, M. M. (2003). Digital Audio Watermarking: Survey. *17th European Simulation Multiconferece*. Uk, 1-14.

Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003). Information Hiding Using Steganography. *In Telecommunication Technology, NCTT 2003 Proceedings*. 4th National Conference on IEEE .21-25.

Andres G. (2002). *Measuring and Evaluating Digital Watermarks in Audio files*. Washington, Dc.

Arnold, M. (2002). *Subjective and Objective Quality Evaluation of Watermarked Audio Tracks*. International Conferences. Wedelmusic.

Asad, M., Gilani, J., & Khalid, A. (2011). An Enhanced Least Significant Bit Modification Technique For Audio Steganography. *In Computer Networks and Information Technology (ICCNIT)*, 2011 International Conference on IEEE . 143-147.

Atoum, M. S., Rababah, O. A. A.-, and Al-attili, A. I. (2011). New Technique for Hiding Data in Audio File. *International Journal of Computer Science and Network Security*, 11(4), 173-177.

Atoum, M. S., Suleiman, M., Rababaa, A., Ibrahim, S., and Ahmed, A. (2011). A Steganography Method Based on Hiding secretes data in MPEG / Audio Layer III. *International Journal of Computer Science and Network Security*, 11(5), 184-188.

Aura, T. (1998). Practical Invisibility in Digital Communication, Information Hiding: Second International Workshop, *Proceeding of lecture Note in Computer Science Springer*, Vol. 1525, .269-278.

Bender W., Gruhl D., Morimoto N.,and Lu A. (1996). Techniques for Data Hiding, *IBM System Journal*, Vol. 35, No. 3and4,

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

Bhattacharyya, S., Kundu, A. and Sanyal, G. (2011). a Novel Audio Steganography Technique by M16MA. International Journal of computer application, 30(8), 26-34.

Bhattacharyya, S., Kundu, A., Chakraborty, K., and Sanyal, G. (2011). Audio Steganography Using Mod 4 Method. *Journal of Computing*, 3(8), 30-38.

Bhowal, K., Pal, a J., Tomar, G. S., and Sarkar, P. P. (2010). Audio Steganography Using GA. *International Conference on Computational Intelligence and Communication Networks*, 449-453.

Brachtl, Bruno O., Don Coppersmith, Myrna M. Hyden, Stephen M. Matyas Jr, Carl HW Meyer, Jonathan Oseas, Shaiy Pilpel, and Michael Schilling. (1990). Data Authentication Using Modification Detection Codes Based on A Public One Way Encryption Function. *U.S. Patent* 4,908,861.

Brandenburg K., (1999), MP3 and AAC Explained, *Proceeding Of AES 17 Th. International Conference On High Quality Audio Coding*.

Brandenburg, K., and Popp, H. (2000). MPEG Layer-3. *EBU Technical Review*, 1-15.

Cacciaguerra, S., and Ferretti, S. (2003). *Data Hiding: Steganography And Copyright Marking*. Department of Computer Science, University of Bologna Mura A.

Chan, C.K. and Cheng, L.M. (2004). Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition*, 37(3), 469–474.

Chan, P. (2011). Secret Sharing in Audio Steganography. *Industrial Research*.

Chandrakar, P., Choudhary, M., and Badgaiyan, C. (2013). Enhancement in Security of LSB Based Audio Steganography using Multiple Files. *International Journal of Computer Applications*, 73.

Changder, S., Debnath, N. C., and Ghosh, D. (2009). A New Approach to Hindi text Steganography by Shifting Matra. *International Conference on Advances in Recent Technologies in Communication and Computing*. 199-202.

Connell, J. B. (1973). A Huffman-Shannon-Fano Code. *Proceedings of the IEEE*, 61(7), 1046-1047.

Coron, J. S., Dodis, Y., Malinaud, C., and Puniya, P. (2005). Merkle-Damgård Revisited: How to Construct a Hash Function. *In Advances in Cryptology–CRYPTO 2005* Springer Berlin Heidelberg ,430-448.

Cox I. J., and Shamoon T. (1997). Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transaction On Image Processing*, 6, 1673 -1687.

Curran, K. and Devitt, J. M. (2008). Image Analysis for Online Dynamic Steganography Detection. *Computer and Information Science*, 1(3), 32-42.

Cvejic, N and Seppanen, T. (2002). Increasing the Capacity of LSB Based Audio Steganography. *IEEE Transactions on Computers*, .336–338.

Cvejic, N and Seppanen, T. (2007). *Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks*, Published In The United States Of America and The United Kingdom, Information Science Reference (An Imprint Of Igi Global).

Cvejic, N. (2004). *Algorithms for Audio Watermarking and Steganography*. PhD. Thesis. Oulun yliopisto.

Cvejic, N., and Seppanen, T. (2004). Reduced Distortion Bit-Modification For LSB Audio Steganography. *International Conference on Signal Processing*. (3), 2318-2321.

Delforouzi, A., and Pooyan, M. (2008). Adaptive Digital Audio Steganography Based on Integer Wavelet Transform. *Circuits, Systems & Signal Processing*, 27(2), 247-259.

Deng, K., Zhang, R., Tian, Y., Yu, X., Niu, X., and Yang, Y. (2010). Steganalysis of the MP3 Steganographic Algorithm Based On Huffman Coding. *In Intelligent Computing and Integrated Systems (ICISS), International Conference on* IEEE, 79-82.

Devi, K. J. (2013). *A Secure Image Steganography Using LSB Technique and Random Pseudo Random Encoding Technique*. (Doctoral dissertation).

Dowdy S. and Wearden S. (1983). *Statistics for Research*. Wiley. ISBN 0471086029, 230.

Dunbar B. (2002). *A Detailed Look at Steganographic Techniques and Their Use in an Open-Systems Environment*, Sans Institute.

Emelia A., Sugathan, S. K., and Ho, A. (2008). Receiver Operating Characteristic (Roc) Graph to Determine the Most Suitable Pairs Analysis Threshold Value. *Advances In Electrical and Electronics Engineering*. 224-230.

Farouk, M. H. (2014). Steganography and Security of Speech Signal. In Application of Wavelets in Speech Processing, *Springer International Publishing*, 45-47.

Fei, C., Kundur, D. and Kwong, R.H. (2006). Analysis and Design of Secure Watermark-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security*, 1(1):43- 55.

Feruza, Y. and Kim, T. (2007) IT Security Review: Privacy, Protection, Access Control, Assurance and System Security, *International Journal of Multimedia and Ubiquitous Engineering*, 2(2), 17-32.

Forouzan, B. A. (2011). *Cryptography and Network Security* (SIE). Tata McGraw-Hill Education.

Francia, G. A., and Gomez, T. S. (2006). Steganography Obliterator: An Attack on the Least Significant Bits. *Information Security Curriculum Development Conference*. 85-91.

Fricker .R, and Rrand M.S. (2002). Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature. *Field Methods*, 14(4),1–23.

Fridrich, J. (1998). Methods for detecting changes in digital images. *Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems*.

Fridrich, J. and Du, R. (1999). Secure Steganographic Methods for Palette Images. *Lecture Notes in Computer Science*, 1768:47-60.

Fridrich, J. and Goljan, M. (1999). Protection of Digital Images Using Self-Embedding. *Proceedings of the Symposium on Content Security and Data Hiding in Digital Media*.

Fridrich, J. Goljan, M. and Soukal, D. (2003). Higher-Order Statistical Steganalysis of Palette Images. *Proc. SPIE, Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents V,* Santa Clara, California, 178-190.

Fridrich, J., Goljan, M. and Du, R. (2001). Steganalysis Based on JPEG Compatibility. *Special Issue on Theoretical and Practical Issues in Digital Watermarking and Data Hiding, SPIE Multimedia Systems and Applications*, 275-280.

Ganeshkumar, V., and Koggalage, R. L. W. (2009). Secured Communication using Steganography Framework with Sample RTF Implementation. *4th International Conference on Industrial and Information Systems* 2009. 15-21

Geetha, K., and Muthu, P. V. (2010). Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy. *International Journal on Computer Science and Engineering*, 2(04), 1308-1313.

Gomez-Coronel, S. L., and Escalante-Ramırez, B., Acevedo-Mosqueda, M. A., & Acevedo, M. E. (2014). Steganography in Audio Files by Hermite Transform.Appl. *Math*, 8(3), 959-966.

Gopalan, K., and Shi, Q. (2010). Audio Steganography Using Bit Modification-A Trade-off on Perceptibility and Data Robustness for Large Payload Audio Embedding. *In Computer Communications and Networks (ICCCN)*, 2010 Proceedings of 19th International Conference on IEEE .1-6.

Groenewald, T. (2004). *A Phenomenological Research Design Illustrated.*

Gupta, N., and Sharma, N. (2013). Hiding Image in Audio using DWT and LSB, .*International Journal of Computer Applications*.

Hacker, S. (2000). *MP3: The Definitive Guide* (p. x388). Sebastopol, CA: O'Reilly.

Huayin Si and Chang-Tsun Li. (2008). Maintaining Information Security in E-Government through Steganography. Department of Computer Science, University of Warwick, UK.

Jangra, T., and Singh, D. (2014). Message Guided Random Audio Steganography Using Modified LSB Technique. *International Journal of Computers & Technology*, 12(5), 3464-3469.

Jaro M. A. (1995). Probabilistic Linkage of Large Public Health Data File. *Statistics in Medicine* 14 (5-7)., 491–498,.

Jaro. M. A. (1989). Advances in Record Linking Methodology as Applied to the 1985 Census of Tampa Florida. *Journal of the American Statistical Society*. 84:414–420.

Johnson N.F., Duricn Z., and Jajodia S. (2001). *Information Hiding: Steganography and Watermarking Attack and Counter measurements*, Kluwer Academic Publishers, USA.

Kamble, M. P. R., Waghamode, M. P. S., Gaikwad, M. V. S., and Hogade, M. G. B. (2013). Steganography Techniques: A Review. *International Journal of Engineering*, 2(10).

Karen, R. (2001). *Steganography and Steganalysis*.

Katz, J., and Lindell, Y. (2008). *Introduction to Modern Cryptography*. CRC Press.

Katzenbeisser S., and Petitcolas F. (2000). Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Inc.

Kekre, H. B., Athawale, a, Rao, B. S., and Athawale, U. (2010). Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding. *3rd International Conference on Emerging Trends in Engineering and Technology*, 196-201.

Kessler, G. C. (1998). *An Overview of Cryptography*. Published by Auerbach

Kexin. Z. (2010). Audio Steganalysis Of Spread Spectrum Hiding Based On Statistical Moment, *Signal Processing*. 381-384.

Khairullah, M. (2009). A Novel Text Steganography System Using Font Color of the Invisible Characters in Microsoft Word Documents. *International Conference on Computer and Electrical Engineering*. Volume (1), 482-484.

Kim, H. O., Lee, B. K., and Lee, N. Y. (2001). *Wavelet-Based Audio Watermarking Techniques: Robustness And Fast Synchronization*. Division of Applied Mathematics, KAIST.

Kirovski D., Malvar H. and Yacobi Y. (2002). Multimedia Content Screening Using a Dual Watermarking and Fingerprinting System. *Acm Multimedia*. Juan Les Pins, France. 372–381.

Kivanc M. (2002). *Information Hiding Codes and their Applications to Images and Audio*, PhD. Thesis, University of Illinois at Urbana-Champaign.

Koso A., Turi A., and Obimbo C., (2005), Embedding Digital Signatures in MP3s, . *From Proceedings Internet and Multimedia Systems, and Applications*. 271-274. 274

Koziel, G. (2014). Simplified Steganographic Algorithm Based on Fourier Transform. *Advanced Science Letters*, 20(2), 505-509.

Kundu A., Chakraborty K. and Bhattacharyya S., (2011). Data Hiding in Images using Using Mod 16 Method, *in the Proceedings of National confence on Emeging thhgg Trends in Electronics & Communication Engineering*, SAMALKHA, utngjhgnPANIPAT, Haryana, India ETECE 2011.

Lee, Y.K., Bell, G., Huang, S.Y., Wang, R.Z. and Shyu, S.J. (2009). An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding. *Advances in Image and Video Technology*. Berlin / Heidelberg: Springer, 349-360.

Lenti J. (2000). Steganographic Methods, Department Of Control Engineering and Information Technology, Budapest University. *Periodica Poltechnica Ser. El. Eng*. Vol.44, No. 3–4, 249–258.

Lin, E. T., and Delp, E. J. (2001). A Review of Data Hiding in Digital Images. *In PICS* 274-278.

Lin, E.T., Podilchuk, C.I. and Delp, E.J. (2000). Detection of Image Alterations using Semi-Fragile Watermarks. *Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents*, 3971:152-63.

Liu, Q., Sung, A. H., and Qiao, M. (2009a). Novel Stream Mining for Audio Steganalysis. *ACM Multimedia Conference*. 95-104.

Liu, Q., Sung, A. H., and Qiao, M. (2009b). Spectrum steganalysis of WAV audio Streams. *In Machine Learning and Data Mining in Pattern Recognition* (pp. 582-593). Springer Berlin Heidelberg.

Maciak L. , Ponniah M. and Sharma R. (2005). *MP3 Steganography*.

Mandala, J., Kotagiri, S., & Kapala, K.(2013). Watermarking Scheme for Color Images. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS).*2(5),179-182.

Manimegalai, P., Gomathi, K. S., Ponniselvi, D., and Santha, M. (2014). The Image Steganography and Steganalysis Based On Peak-Shaped Technique for MP3

Audio and Video. *International Journal of Computer Science and Mobile Computing*,3(1), 300-308.

Matthews C. (2003). *Behind The Music: Principles of Audio Steganography*.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (2010). *Handbook of Applied Cryptography*. CRC press.

Mitra, S., and Manoharan, S. (2009). Experiments with and Enhancements to Echo Hiding. *In Systems and Networks Communications, 2009. ICSNC'09*. Fourth International Conference on IEEE. 119-124.

Morkel, T. (2012). *Image Steganography Applications for Secure Communication*, Doctoral dissertation, University of Pretoria.

Naji A.W., Zaidan A. A., Zaidan B.B., Shihab A., and Othman O.Khalifa. (2009). Novel Approach for Secure Cover File of Hidden Data in the Unused Area Within exe File Using Computation between Cryptography and Steganography. *International Journal of Computer Science and Network security*. Volum (9), 294-300.

Neeta, D., Snehal, K., and Jacobs, D. (2006). Implementation of LSB Steganography and Its Evaluation for Various Bits. *International Conference On Digital Information Management*. 173-178.

Neubauer C. H. J. (2000). *Audio Watermarking MPEG-2 AAC Bit stream*. 109th AES Convention, Audio Engineering Society Preprint 5176. Los Angeles.

Nilsson M. (1999*).* Id3 Tag Version 2.3.0.

Nilsson M. (2000) . *ID3 Tag Version 2.4.0 - Main Structure,*

Nilsson M. (2002), Audio Steg: Overview, *Internet Publication on Www.Snotmonkey.Com*
Http://Www.Snotmonkey.Com/Work/School/405/Overview.Html1577-1578.

Nilsson, M. (2001). The Private Life of MP3 Frames. *Available In Internet Www. Id3. Org/Mp3frame. Htm*.

Ozer H. (2003). Steganalysis of Audio Based On Audio Quality Metrics, *Proceedings Of Spie*, 55-66.

Paar, C. (2000). *Applied Cryptography and Data Security*. Lecture Notes), Ruhr-Universität Bochum.

Pan, D. (1995). A Tutorial on MPEG / Audio Compression. *IEEE Multimedia*, 60 - 74.

Park, J. O. (2013). A Secure Audio Steganography Algorithm Using Genetic Approaches. International Journal of Computer Science & Network Security,13(10).

Park, Y., Kang, H., Yamaguchi, K., and Kobayashi, K. (2006). Integrity Verification of Secret Information in Image Steganography. *In Symposium on Information Theory and its Applications*, Hakodate, Hokkaido, Japan,1-4.

Petitcolas F.A, Anderson R.J., and Kuhn M.G. (1999). Information Hiding – A Survey, *IEEE, Special Issue on Protection of Multimedia Content*: 1062-1078.

Petitcolas, F. A. (1998). *MP3STEGO*. Computer Laboratory, Cambridge.

Petrovic, R., and Yang, D. T. (2009). Audio Watermarking in Compressed Domain. *International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*. 395-401.

Pickett, J. M. (1999). The Acoustics of Speech Communication: Fundamentals, speech perception theory and technology. Boston*: Allyn and Bacon*.

Potdar, V.M., Han, S. and Chang, E. (2005). Fingerprinted Secret Sharing Steganography for Robustness Against Image Cropping Attacks. *Proceedings of the IEEE International Conference on Industrial Informatics*, 717-724.

Qi, Y., Ye, L., and Liu, C. (2009). Wavelet Domain Audio Steganalysis for Multiplicative Embedding Model. *International Conference on Wavelet Analysis and Pattern Recognition*. 429-432.

Qiao, M., Sung, A. H., and Liu, Q. (2009). Feature Mining and Intelligent Computing For MP3 Steganalysis. *International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing*. 627-630.

Quan, X., and Zhang, H. (2006). Data Hiding in MPEG Compressed Audio Using Wet Paper Codes. *18th International Conference on Pattern Recognition* (ICPR'06), 727-730.

Rahim, L. B. A., Bhattacharjee, S., and Aziz, I. B. (2014). An Audio Steganography Technique to Maximize Data Hiding Capacity along with Least Modification of Host. *In Proceedings of the First International Conference on Advanced Data and Information Engineering (DaEng-2013) Springer Singapore.* 277-289.

Raissi, R. (2002). *The Theory behind MP3*. MP3'Tech.

Rey, C. and Dugelay, J. (2002). A Survey of Watermarking Algorithms For Image Authentication. *EURASIP Journal on Applied Signal Processing*, 6:613-621.

Ricardo A. G. (1999). Digital Watermarking of Audio Signals Using A Psychoacoustic Auditory Model And Spread Spectrum Theory. *In Audio Engineering Society Convention 107. Audio Engineering Society.*

Rogaway, P., and Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Pre-Image Resistance, Second-Pre-Image Resistance, and Collision Resistance. *In Fast Software Encryption Springer Berlin Heidelberg*. 371-388.

Scagliola, M., Pérez, F., and Guccione, P. (2009). An Extended Analysis of Discrete Fourier Transform - Rational Dither Modulation For Non-White Hosts. *1st IEEE International Workshop On Information Forensics and Security*, 146-150.

Schneier, B. (1963). Secrets and Lies–Digital Security in a Networked World, *John Willey & Sons*.

Sellars D., (2003), *An Introduction to Steganography*, Department of Computer Science, University of Cape Town,

Shahreza, S. S., and Shalmani, M. T. M. (2007). Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate. *In Proceedings of the IEEE International Conference on Information and Emerging Technologies*,(ICIET „07) . 1729-1732.

Singh, P. K., Singh, H., and Saroha, K. (2009). A Survey on Steganography in Audio. *In National Conference on Computing for Nation Development*, Indiacom.

Skopin, D. E., El-Emary, I. M., Rasras, R. J., and Diab, R. S. (2010). Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal. *IEEE 978*-(1), 4244-5848.

Sridevi, R., Damodaram, A. and Narasimham, S. V. L. (2009). Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. *Journal of Theoretical & Applied Information Technology*, 5(6).

Supurovic. P, (1998). MPEG Audio Frame Header, *Available In Internet Www.Dv.Co.Yu/Mpgscript/Mpeghdr.Htm#Mpegtag*.

Venkatraman, S., Abraham, A. and Paprzycki, M. (2004). Significance of Steganography on Data Security. *Proceedings of the International Conference on Information Technology: Coding and Computing*, 2:347.

Wakiyama M., Hidaka Y., and Nozaki K., (2010), An Audio Steganography by a Low-Bit Coding Method With Wave Files, *Sixth International Conference On Intelligent Information Hiding and Multimedia Signal Processing*. 530-533.

Walton, S. (1995). Information Authentication for a Slippery New Age. *Dr. Dobbs Journal*, 20(4):18-26.

Westfeld, A., and Pfitzmann, A. (2000). Attacks on Steganographic Systems. *In Information Hiding Springer Berlin Heidelberg* . 61-76.

Westfeld, A., Wurzer, J., Fabian, C., and Piller, E. (2013). Pit Stop for an Audio Steganography Algorithm. *In Communications and Multimedia Security*. Springer Berlin Heidelberg. 123-134.

Whitiak D. (2003). *Art of Steganography*, Sans Institute, As Part of GIAC Practical Repository.

William, S., and Stallings, W. (2006). *Cryptography and Network Security*, 4/E. Pearson Education India.

Winkler W. E. (1999). The State Of Record Linkage and Current Research Problems. Statistics of Income Division, *Internal Revenue Service Publication R99/04*.

Wong, P. (1998). A Public Key Watermark for Image Verification and Authentication. *Proceedings of the International Conference on Image Processing*, 1:455-9.

Xiao, D., Liao, X., & Deng, S. (2005). One-way Hash function Construction Based on the Chaotic Map with Changeable-Parameter. *Chaos, Solitons & Fractals*, 24(1), 65-71.

Yusnita Y. and Othman O. K. (2007). Digital Watermarking for Digital Images using Wavelet Transform. *14th IEEE International Conference On Telecommunications*. Penang, Malaysia.

Zamani, M. (2010). *Genetic Based Substitution Techniques for Audio Steganography*. PhD. Thesis, Universiti Teknologi Malaysia.

Zamani, M., Manaf, A. A., Ahmad, R. B., Zeki, A. M., and Abdullah, S. (2009a). a Genetic-Algorithm-Based Approach for Audio Steganography. *Engineering and Technology*, 360-363.

Zamani, M., Manaf, A. A., and Ahmad, R. B. (2011). Knots of Substitution Techniques of Audio Steganography. *Computer Engineering*, 2, 370-374.

Zamani, M., Manaf, A., Ahmad, R. B., Jaryani, F., Taherdoost, H., and Zeki, A. M. (2009b). a Secure Audio Steganography Approach. *in Internet Technology and Secured Transactions, ICITST 2009.* International Conference for IEEE. 1-6.

Zamani, M., Taherdoost, H., Manaf, A. A., Ahmad, R. B., and Zeki, A. M. (2009c). Robust Audio Steganography via Genetic Algorithm. *Soft Computing*, 1-4.

Zaturenskiy, M. (2009). MP3 Steganography.

Zaturenskiy, M. (2013). MP3 files as a steganography medium. *In Proceedings of the 2nd Annual Conference on Research in Information Technology ACM* .

Zeki, A. M. and Manaf, A. A. (2009). A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit). *International Journal of Information Technology*, 5, 989-996.

Zeki, A.M. (2009), *Watermarking Techniques using Intermediate Significant Bit*. PhD. Thesis, Universiti Teknologi Malaysia.