INFORMATION HIDING BASED ON AUDIO STEGANOGRAPHY

USING LEAST SIGNIFICANT BIT (LSB)

NURUL SAHIRA BINTI MOHD YASIN

BACHELOR OF COMPUTER SCIENCE
(COMPUTER NETWORK SECURITY)
UNIVERSITI SULTAN ZAINAL ABIDIN
2018
DECLARATION

I hereby declare that this report is based on my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Sultan Zainal Abidin or other institutions.

________________________________
Nurul Sahira Binti Mohd Yasin

Faculty of Informatics and Technology UNISZA

Date : .............................................
CONFIRMATION

This is to confirm that:

The research conducted and the writing of this report was under my supervisor.

________________________________
Name : ..................................................

________________________________
Date : .............................................
DEDICATION

In the Name of Allah Most Gracious and Most Merciful, I am grateful because He has given me strength to complete my report for final year project entitled “Information Hiding Based on Audio Steganography Using Least Significant Bit (LSB)”.

I would like to express my sincere thanks and appreciation to my supervisor, Prof. Madya Dr Fatma Susilawati Binti Mohamad for her guidance and understanding in imparting her knowledge and constructive comment during the course of this project.

Special thanks also go to all of my beloved family and friends for giving me moral support and encouragements. Last but not least, I would like to thank any person that contributes to my project and guide me throughout the preparation of the project.
ABSTRACT

Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. A few problems arise especially in securing data and information when the information had been lost or stolen from unauthorized user. Traditionally, we give information manually using paper; it is possible that the information could be stolen by unauthorized user. The main objective of this study is to hide secret information in audio so that other persons will not notice the presence of the information. The proposed method of this study is by using Least Significant Bit (LSB) algorithm to design an audio steganography. In the proposed method each audio sample is converted into bits and then the text data is embedded. The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand.

Keywords: Steganography, Audio Steganography, LSB algorithm.
ABSTRAK

Steganography adalah idea untuk menyembunyikan data atau maklumat peribadi atau maklumat sensitif dalam sesuatu yang kelihatan diluar kebiasaan. Beberapa masalah timbul terutamanya dalam menjaga data dan maklumat apabila maklumat itu telah hilang atau dicuri oleh pihak yang tidak berwajib. Secara tradisinya, memberikan maklumat secara manual menggunakan kertas; berkemungkinan bahawa maklumat itu boleh dicuri oleh pihak yang tidak berwajib. Objektif utama kajian ini adalah untuk menyembunyikan maklumat rahsia dalam audio supaya orang lain tidak akan mengetahui kehadiran maklumat tersebut. Kaedah kajian ini adalah dengan menggunakan algoritma Least Significant Bit (LSB) untuk merangka steganografi audio. Dalam kaedah yang dicadangkan setiap sampel audio ditukar menjadi bit dan kemudian data teks dibenamkan. Hasil yang diharapkan dari kajian ini akan menghasilkan audio steganografi yang dapat menyembunyikan data atau informasi secara efisien dari pihak yang tidak berwajib dan juga untuk memastikan keselamatan informasi berada di pihak yang betul.

Kata kunci: Steganografi, Steganografi Audio, algoritma LSB.
# CONTENTS

| DECLARATION | i |
| CONFIRMATION | ii |
| DEDICATION | iii |
| ABSTRACT | iv |
| ABSTRAK | v |
| CONTENTS | vi |
| LIST OF TABLES | viii |
| LIST OF FIGURES | ix |

## CHAPTER I

### INTRODUCTION

1.1 Introduction 1

1.2 Problem statement 2

1.3 Objectives 2

1.4 Scopes 3

1.5 Limitation Of Work 4

1.6 Summary 4

## CHAPTER II

### LITERATURE REVIEW

2.1 Introduction 5

2.2 Existing Method 6-8

2.2.1 Audio Steganography Using RSA and Genetic Based Method to Enhance Security 6
2.2.2 A View on LSB Based Audio Steganography 6
2.2.3 Encrypted Information Hiding using Audio Steganography and Cryptography 7
2.2.4 Multi-Level Stenographic Algorithm for Audio Steganography using LSB and Party Encoding 7
2.2.5 Genetic Algorithm Based Model in Text Steganography 8

Table Of Comparison 9-10
Discussion and Proposed Work 11
Summary 11

CHAPTER III METHODOLOGY

3.1 Introduction 12
3.2 Evolutionary/Iteration Model 12
3.2.1 Planning Phase 13
3.2.2 Analysis Phase 13
3.2.3 Design Phase 14-17
3.2.4 Implement Phase 18-19
3.3 Summary 19

REFERENCES 20


## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>First table in chapter 2</td>
<td>9-10</td>
</tr>
<tr>
<td>3.1</td>
<td>First table in chapter 3</td>
<td>18</td>
</tr>
<tr>
<td>3.2</td>
<td>Second table in chapter 3</td>
<td>19</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>First figure in chapter 3</td>
<td>13</td>
</tr>
<tr>
<td>3.2</td>
<td>Second figure in chapter 3</td>
<td>14</td>
</tr>
<tr>
<td>3.3</td>
<td>Third figure in chapter 3</td>
<td>15</td>
</tr>
<tr>
<td>3.4</td>
<td>Fourth figure in chapter 3</td>
<td>17</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

1.1 BACKGROUND

Information security is one of the most challenging problems in today's technological world. This paper is to come up with a technique hiding the presence of secret message which is called steganography. It is also called as “covered writing” because it uses a “cover” of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous looking cover media objects, such as images using the human's visual, aural redundancy or media objects' statistical redundancy. Steganography is a powerful tool which increases security in data transferring and archiving. In the steganographic scenario, the secret data is first concealed within another object which is called “cover object”, to form “stego object” and then this new object can be transmitted or saved. Embedding secret messages into digital sound is known as Audio Steganography. In this project, the stego-audio will be saved in format audio.wav only.
1.2 PROBLEMS STATEMENT

Today, security of data is of foremost importance in today’s world. Security has become one of the most important factors in communication and information technology. Nowadays, a few problems arise especially in securing data and information when the information had been lost or stolen from unauthorized user. The problem is giving information manually will have a high tendency to be stolen. In traditional way, information is passing manually using papers and the possibility of being stolen by unauthorized user is high.

1.3 OBJECTIVES

Generally, the aim of this project is to develop a system that can hide secret information in audio so that other person will not notice the presence of the information. The objectives of implementing audio steganography using LSB are:

1.3.1 To design audio steganography model using LSB algorithm for data hiding
1.3.2 To prevent data from being stolen by an unauthorized user
1.3.3 To develop an audio steganography system for data security
1.4  SCOPE

This project focuses on hiding data or information efficiently from unauthorized user using Least Significant Bit (LSB). The scope includes two main users. First, is the sender and secondly is the receiver. It is directly send from the sender to the receiver.

The general role of user access in the application:

1.4.1 Choose an audio

1.4.2 Write the message that will be sent to receiver

1.4.3 Select encode process

1.4.4 Enter the public key pair

1.4.5 Send to the receiver

1.4.6 Select decode process

1.4.7 Enter private key pair
1.5 LIMITATION OF WORK

In order to implement this project, a few limitations have been detected.

1.5.1 The format of hidden message must be in text

1.5.2 The stego-audio will be saved in audio.wav format only

1.6 SUMMARY

The purpose of this project is to overcome the problem that occurs in the environment. Besides, the function of the project and the limitation of the project were also identified.
CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

Today Security of data is of foremost importance in today’s world. Security has become one of the most important factors in communication and information technology. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography. The word steganography comes from the Greek Steganos, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. Secret information is encoded in a manner that the very existence of the information is concealed.

Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is not only prevented others from knowing the hidden information, but it also prevented others from thinking that the information even existed. The objective of this project is to hide information in audio steganography using LSB algorithm. This chapter presents a survey of the existing techniques, advantages and disadvantages of the research work.
2.2 EXISTING METHODS

2.2.1 Audio Steganography using Rivest-Shamir-Adleman (RSA) algorithm and Genetic based Substitution method to Enhance Security

Gaurav Singh, Kuldeep Tiwari, Shubhangi Singh present an approach for resolving the problem related to the substitution technique of audio steganography. In first level of security we use RSA algorithm to encrypt message, in the next level, encrypted message is to be encoded in to audio data for this we used genetic algorithm based substitution method. The basic idea behind this paper is to enhance the security and robustness.

2.2.2 A View on LSB Based Audio Steganography

Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay & Tai-hoon Kim propose a novel approach where a duel encryption methodology has been implemented. In the first level of encryption a pattern matching algorithm has been employed to encrypt the text message in terms of their positional value. In second level, the conventional LSB method has been used to embed the positional value in the cover file. Such a duel encryption method will ensure data security in an efficient manner.
2.2.3 Encrypted Information Hiding Using Audio Steganography and Audio Cryptography

*Nishith Sinha, Anirban Bhowmick & B. Kishore* proposed a novel approach for concealing data. The proposed algorithm is an amalgamation of text encryption, audio steganography and audio encryption. In the first step, the original text message is encrypted using modified Vigenère cipher algorithm. The cipher text gets embedded into the cover audio using LSB encoding, in the second step. Further, the audio file is then subjected to transposition making use of Blum Blum Shub pseudo random number generator.

2.2.4 Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique

*Prof Samir Kumar Bandyopadhyay and Barnali Gupta Banik* give an overview of two primitive techniques to get an idea of how steganography in audio file works. LSB modification and phase encoding technique are very primitive in steganography. An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion, Data Rate and Robustness. These characteristics are called the magic triangle for data hiding.
2.2.5 Genetic Algorithm Based Model in Text Steganography

Christine K. Mulunda, Peter W. Wagacha, Alfayo O. Adede worked with text as the cover medium with the aim of increasing robustness and capacity of hidden data. Elitism was used for the fitness function.
# 2.3 TABLE OF COMPARISON

<table>
<thead>
<tr>
<th>No</th>
<th>Title</th>
<th>Algorithm</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Audio Steganography using RSA algorithm and Genetic based Substitution method to Enhance Security <em>(Gaurav Singh, Kuldeep Tiwari, Shubhangi Sing)</em></td>
<td>RSA and Genetic Based Algorithm</td>
<td>The theory of technique is that simply replacing either a bit or a few bits in each sample will not be noticeable to the human eye or ear depending on the type of file</td>
<td>The main problem s of audio substitution steganography algorithm is considerably low robustness. There are two types of attacks to steganography and therefore there are two type of robustness. One type of attacks tries to reveal the hidden message and another type tries to destroy the hidden message. Substitution techniques are vulnerable against both types of attacks.</td>
<td>96.37</td>
</tr>
<tr>
<td>2</td>
<td>A View on LSB Based Audio Steganography <em>(Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay &amp; Tai-hoon Kim)</em></td>
<td>LSB Algorithm</td>
<td>Allows a large volume of data given in audio or text format to be encoded and data are found in the receiving end in loss-less format</td>
<td>It is easy for the invaders to identify and destroy the information</td>
<td>97</td>
</tr>
<tr>
<td>No</td>
<td>Title</td>
<td>Algorithm</td>
<td>Advantages</td>
<td>Disadvantages</td>
<td>Accuracy (%)</td>
</tr>
<tr>
<td>----</td>
<td>-------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3</td>
<td>Encrypted Information Hiding using Audio Steganography and Audio Cryptography <em>(Nishith Sinha, Anirban Bhowmick &amp; B. Kishore)</em></td>
<td>An amalgamation of text encryption, audio steganography and audio encryption</td>
<td>This combination of cryptography and steganography ensures that even if the audio file is intercepted by an unauthorized person, the person doesn’t discover the secret information.</td>
<td>The audio is encrypted only using transposition. The authors recommend more secure encryption algorithms to be utilized for text encryption so that data is not easily stolen by an unauthorized party.</td>
<td>95.97</td>
</tr>
<tr>
<td>4</td>
<td>Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique <em>(Prof. Samir Kumar Bandyopadhyay &amp; Barnali Gupta Banik)</em></td>
<td>Multi-Level Steganography Algorithm</td>
<td>This method is easy to implement but is very susceptible</td>
<td>This method can be used when only a small amount of data needs to be concealed</td>
<td>95.88</td>
</tr>
<tr>
<td>5</td>
<td>Genetic Algorithm Based Model in Text Steganography <em>(Christine K. Mulunda, Peter W. Wagacha, Alfayo O. Adede)</em></td>
<td>Genetic Algorithm</td>
<td>This approach works, achieving effective optimization, security, and robustness</td>
<td>Applicable for text files only</td>
<td>96.59</td>
</tr>
</tbody>
</table>
2.4 DISCUSSION AND PROPOSED WORK

The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand.

2.5 SUMMARY

This chapter focuses on the pros and cons of the existing system. The research gap is identified and the problem definition and objectives are formulated. Moreover, the developing tool will be enhanced by the existing system. However, there is also the limitation of this project.
CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

This chapter discusses how to develop the system. The suitable methodology is chosen and will be followed until the end of the project. There are some steps that must be considered. The development of this project is carried out by applying the methodology of Evolutionary/Iteration Model. Evolutionary/Iteration Model is used on every phase of development process.

3.2 EVOLUTIONARY/ITERATION MODEL

Figure below shows the evolutionary/iteration development model that is chosen to develop the project. Evolutionary/Iteration model is an iterative life cycle model does not attempt to start with a full specification of requirement. Instead, development begins by specifying and implementing just part of software, which can then be reviewed in order to identify further requirements. This process is the repeated, producing a new version of the software for each cycle of the model. Besides, this model are building and improving the product step by step. Hence, we can track the defects at early stages. This avoids the downward flow of the defects.
3.2.1 Planning Phase

In this phase after determine the problems statement of this project, this phase will discover the solution to overcome those problems. The scope of the system includes two main users, the sender and the receiver. In this phase also, will determine the important functions needed to meet the objectives.

3.2.2 Analysis Phase

Literature review is done to study on other’s work which relates to audio steganography, LSB algorithm. By comparing the advantages and disadvantage of other works stated in literature review will help in produce the product in overcoming the problem stated in regarding to the audio steganography. To meet the requirement in producing this project, the scope had been analysed and observe.
3.2.3 Design Phase

In this phase, the audio steganography divided block diagram of the system, LSB algorithm, and the interfaces.

The figure 3.2 shows block diagram of audio steganography and general concept of the project.

Figure 3.2 Block Diagram of Audio Steganography

- The secret message to be transmitted is embedded inside a cover file
- A stego key is also used to provide security
- Using suitable algorithm secret message is embedded into the carrier object
- The resultant file is called stego file and this stego file is transmitted to the receiver side
- At the receiver side stego file is decoded using the stego key to extract the secret message
3.2.3.1 LSB Algorithm

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By 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.

Figure 3.3 shows the encryption and decryption process of the audio steganography.

Figure 3.3 Encrypted and Decrypted Message
Embedding process (Encryption)

1. Enter audio input
2. Separate the header and data because header in audio file is very sensitive and must not change that
3. Replace the LSB of the data with secret text
4. Finally get stego audio that have secret text

Extraction Process (Decryption)

1. Receiver receive the stego audio that contain audio and secret data
2. Separate header and the data
3. Store the LSB of the data because LSB contain secret text
4. The LSB will be in binary format, and convert into ASCII format to get the text back
3.2.3.2 Interface

![Figure 3.4 Interface of the system](image)

Figure 3.4 Interface of the system
3.2.4 Implementation Phase

After design phase, the implementation phase will implement the system. This project will use some tools or application in order to finish and proceed with the implementation phase. The tool that has been listed in this phase is Matlab.

3.2.4.1 Software and Hardware Requirements

This section will show the list of all software and hardware that involve in the development process.

**Hardware Requirement**

<table>
<thead>
<tr>
<th>HARDWARE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Intel corei5</td>
</tr>
<tr>
<td></td>
<td>RAM: 4GB</td>
</tr>
<tr>
<td></td>
<td>OS: WINDOWS 10</td>
</tr>
<tr>
<td></td>
<td>• Use to develop the application</td>
</tr>
<tr>
<td>Printer</td>
<td>• To print the report</td>
</tr>
<tr>
<td>Hard disk</td>
<td>• To back up the data project</td>
</tr>
</tbody>
</table>

*Table 3.1 Hardware Requirement*
Software Requirement

<table>
<thead>
<tr>
<th>SOFTWARE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MatLab</td>
<td>• To process all the code</td>
</tr>
<tr>
<td>Microsoft Office 2010</td>
<td>• To prepared the report</td>
</tr>
</tbody>
</table>

Table 3.2 Software Requirement

3.3 SUMMARY

This chapter discuss on the methodology selected to implement the audio steganography using LSB algorithm, Evolutionary/Iteration Model. That model involve a several phase such as planning phase, analysis phase, design phase, and implementation phase. The objectives, problem statement and scope will be determined at the first phase. In the analysis phase, the works on other research related will be studied. The design phase include LSB algorithm, the system framework and interface.
REFERENCES

1) IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814 www.IJCSI.org


3) Information and knowledge management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.3, 2012


DOI: 10.5815/ijcnis.2015.07.03