New Secure Scheme in Audio Steganography (SSAS)

1Mohammed Salem Atoum, 2Subariah Ibrahim, 3Ghazali Sulong and 4Ali Ahmed

1,2,3,4Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia Skudai, Johor bahru, Malaysia 83100

Abstract: To hide information or embed secret message in a multimedia, steganography or cryptography gives best solutions. Cryptography refers to change information into unreadable format by unauthorized persons. Steganography is the science of embedding and extracting information in/from the media. The steganography method was developed for image media. But in recent years, the researchers develop steganography methods for audio and video media. All steganography types through embedding algorithm use real information of the secret message, thus the probability of disclosure of information after detecting a secret message will be increased. In this paper, a new scheme for audio steganography is proposed to increase the security by addressing secret message before embedding, and using a mathematical model for embedding, and also using map for extracting secret message. All these techniques increase the security of Stego object, and also reduce the probability to attack the secret message or exchange it. In addition, information security results with experimental examples are discussed and finally conclusion and remarks are presented.

Key words: Steganography, Cryptography, Security, MP3.

INTRODUCTION

Information security is the first important issue that must be considered when using the Internet. There are two basic ways in which information can be secured; cryptography and steganography (Lentij, 2000). Cryptography refers to changing information by using well defined rules to a form that is hard to be distinguished or read to ensure that no one can identify the information except people who know the rules. This type of method is known as cryptography. Cryptography is a Greek word also known as secret writing (Petitcolas, Anderson and Kuhn, 1999).

Steganography refers to hiding information or object in a secret place that cannot be accessed by anyone except people who are familiar with the secret sender. Steganography is a Greek word that is also known as covered writing (Petitcolas, Anderson and Kuhn, 1999). In the digital world, although steganography and cryptography operate in different ways, they have the same goal of securing information from unwanted parties (Dunbar, 2002). The two methods are often lumped together, even though they are very unalike.

Cryptography operates by changing the contents of a file or message in a way that data can only be accessed by the right people. In this method, the intended recipient is given a decryption key to enable him accessing the data. It is difficult to figure out the means of encryption, and decryption keys used to secure the information. However the method has a drawback of not being able to hide the message transfer process (Katzenbeisser and Peticotas, 2000).

Steganography, on the other hand, operates by hiding the message transfer process in such a way that the observer is not able to see and observe the exchange of messages. This method secures the overall communication process because it hides the message exchange process. However, some steganography methods combine traditional cryptography with steganography, which enables the encryption of the secret message prior to the embedding process. According to the combination of traditional cryptography and steganography method, the security of overall communication process is increased, as it becomes more difficult for an attacker to detect embedded cipher text (Katzenbeisser and Peticotas, 2000).

Many researches that have been done on information hiding adopt steganography and watermarking methods. Steganography refers to methods that are used to transmit the embedded message without the observer being able to notice the embedded message in the cover message.

In steganography method transparency is a critical issue but not robustness. Watermarking ensures security of data by embedding a “watermark” for authentication purpose, which is an important step for copyright protection and tamper proofing. The embedded watermark is usually perceivable and cannot easily be removed from the Stego message. Watermarks are extended information and are considered as attributes of the cover image but moreover, they are usually required to be semi-fragile or robust (Seppanen and Cvejic, 2002).

This paper introduces various concepts of steganography type and comparison between the three steganography types. The proposed method will be explained, discussed and analyzed.
**Steganography:**

Steganography or (Covert Communication) is an ancient art that has been reborn in recent years. It plays an increasingly important role in today's connected society, as the demand for covert communications and digital copyright protections continues to rise (Nedeljko, 2004). Steganography basically aims at hiding communication between two parties from the attackers (Baron, Bresler and Mihcak, 2003). Steganography operates by embedding a secret message, which might be a copyright mark, or a covert communication, or a serial number in a cover message such as a video film or an audio recording, or computer code, in such a way that it cannot be accessed by any wrong person during data exchange. A cover message containing a secret message is known as a Stego Object (Katzenbeisser and Peticotas, 2000). After data exchange, it is advisable for both parties (sender and receiver) to destroy the cover messages in order to avoid accidental reuse.

The steganography method was developed for image media. But in recent years, the researchers are developing steganography method for audio and video media. The basic model of a steganography system is shown in the Figure1 (Cacciaguerra and Ferretti, 2000).

![Fig. 1: Basic model of steganography](image)

Each steganography method consists of embedding algorithm and extracting algorithm. The embedding algorithm is used to hide secret messages inside a cover messages, and the embedding process is protected by a key word so that only those who possess the secret key word can access the hidden message. The extracting algorithm is applied to a possibly modified carrier and returns the hidden secret message.

**Types Of Steganography:**

The three types of steganography include the pure steganography, secret key steganography and public key steganography. The three types are described in the sections below.

**Pure Steganography:**

Pure steganography does not require a prior exchange of some secret information (like a stego-key). Its embedding process can be described by mapping $E: C \times M \rightarrow C$. The extraction process which involves the extraction of a secret message from a cover message is defined by mapping $D: C \rightarrow M$, where $C$ is a set of possible covers and $M$ is a set of possible messages and $|C| \geq |M|$.

In pure steganography, the only people who can access the algorithms used during the embedding and extraction processes are the sender and receiver not the public (Katzenbeisser and Peticotas, 2000). However, the method has a drawback of being less secured since the sender and receiver rely only on the assumption that no other parties are aware of this secret message. Figure 2 below shows the pure steganography type.
Secret Key Steganography:
Secret key steganography requires exchange of a secret key (Stego-Key) prior to communication. Secret key steganography embeds the secret message inside a cover message by using a secret key (Stego-Key). In this method, the secret message can be read by parties who know the secret key.

Unlike pure steganography where a perceived invisible communication channel is present, Secret key steganography exchanges a Stego-Key, which makes it more susceptible to interception. The advantage with the secret key steganography is that even if it is intercept, only parties who know the secret key can extract the secret message (Katzenbeisser and Peticotas, 2000). Figure 3 below shows the secret key steganography type.

Public Key Steganography:
Public key steganography is based on the concepts of public key cryptography. Public key steganography uses a public key and a private key to secure the communication between the parties.

Public key steganography operates in such a way that the sender uses the public key during the encoding process and uses only the private key, which has a direct mathematical relationship with the public key to decipher the secret message. Some of the advantages of public key steganography include its robustness in such a way that it utilizes much more robust and researched technology in public key cryptography. It also has multiple levels of security, which makes it difficult for others to access the secret message. They first have to make so many guesses in order to crack the algorithm used in the public key system before they could intercept the secret message (Katzenbeisser and Peticotas, 2000). Figure 4 below shows the public key steganography type.
Referring to the types of steganography, it can be observed that all types use the real information in the secret message to embed it by using any embedding algorithms, so if the attacker catch the Stego-object it becomes easily to read the secret message, and can be easily to change or remove the secret message. Thus, to solve this problem, some of researchers use cryptography technique to encrypt data before embedded. But this way can increase the complexity of steganography technique, and also reduce the size of secret message that will be embedded, because the encryption algorithms increase the size of message more than twice (Atoum et al., 2011a, Atoum et al., 2011b, Atoum et al., 2012).

Hence, should be to find an outlet to address the secret message without using encryption algorithms, and to reduce the probability of an attacker to read the real information of secret message. In our proposed method, new secure model for steganography will be designed by using a mathematical formulation to increase security before embedding secret message.

**Proposed Method:**

In this section, we will explain and discuss a new secure scheme for audio steganography. The proposed method contains two phase: Stego Math Selections phase and Embedding, Extracting phase. The proposed method will be conducted according to the workflow process as illustrated in Figure 5.

**Stego Math Selections (SMS):**

In this phase, the input is Cover (C) and the Message (M). SMS is the process to select math formulation to apply it in secret message to increase security. The outputs of this process are: Stego-Embed (SE) used in the embedding process, P_Map (P) used in the extracting process.
This process includes three sub-processes; message and cover preparation, message partitioning and message permutation.

**Message And Cover Preparation:**
This subsection addresses the preparation of both message and cover. For message preparation, the first step is recording speech by using application sound record in Microsoft windows, then save the speech in a file. The second step is noise removal, which is used to remove the background noise that exists in the speech signal. The power spectral subtraction method is used for noise removal in order to adjust the subtraction factor. The adjustment is done according to the signal to noise ratio (SNR). It calculates the number of initial silence that exists in the signal based on the shift percentage value, and then it calculates the noise length. Noise counter will return the number of previous noise frames presented in the signal, and after that it detects the noise only on periods and will attenuate the signals. At last, the noises are removed and as a result a noise free signal is reconstructed.

The last step is to convert speech into byte stream, and then, all the bytes are converted into a decimal value to be stored in an array. It is worth mentioning that the secret message in speech can use many types such as wav, wma, MP3, etc. However, the widely spread type is MP3 because it gives the smallest file size by using specific settings for encoding.

Regarding cover preparation, the MP3 file is converted into byte stream, and then into decimal values that are stored in an array.

**Message Partitioning:**
In this subsection, the message have been prepared and converted into byte stream will be partitioned into blocks by using Equation 1. This Equation shows the number of the message partitions based upon the size of the cover and of the message. Therefore, the result will be always variable.

\[ S = \frac{\text{SIZE}(C)}{\text{SIZE}(M)} \]  

Where \( S \) is the number of partitions, \( C \) is the cover and \( M \) is the message.

By using Equation 2, the message will be partitioned.

\[ M = M_1, M_2, M_3, \ldots \ldots, M_s \]  

**Message Permutation:**
In this subsection, the message have been partitioned will be encoded by reordering the blocks that will have been permutation by using Equation 3. A permutation, also called an "arrangement number" or "order," is a rearrangement of the blocks of an ordered list \( P \) into a one-to-one correspondence with \( P \) itself. The number of permutations on a set of \( n \) elements is given by \( n! \). This Equation shows the probabilities that can be produced from this reordering.

\[ P(n,k) = \frac{n!}{(n-k)!} \]  

Where \( n \) is the number of blocks, \( k \) is the number of chosen. And note that if maximum probability, when the chosen \( k=n \), to achieve high possibility for random chose, thus, the equation will be as follows: \( P_k = n! \)

**A. Embedding and Extraction process phase:**
This phase has two processes; embedding process and extracting process. In embedding process, the inputs are SE and C. The output Stego Object (SO) is used in extracting process. In extracting process the input is SO and P and the output is M. the steps for two processes are shown below:

**Embedding process steps:**
1. SE and C converted to bit stream.
2. Choosing randomly byte for C as even value to begin embedding from it.
3. Apply LSB technique to embed SE to C by trying embedding 1,2 and 4 bit from SE with 1,2 and 4 bit from C respectively.
4. After that, randomly jump is used to move for the next byte in C.
5. Repeating step 3 to complete embedding SE in C.

**Extracting process steps:**
1. Receiving SO from sender.  
2. Finding first byte embedded in it by using information sent by receiver.  
3. Extracting bit to collect secret message by repeating step 2.  
4. Apply P to re-order blocks for secret message.  
5. Listening to secret message.

**Discussion and Results:**

The benefits of partition and permutation secret message to blocks are to achieve security by three important things:  
1. Reordering the message blocks by using permutation formula to generate randomly blocks of message to encode secret message. This can increase the ambiguity to detect secret message by attackers, and decode secret message to know its content.  
2. To achieve integrity message by using a mathematical and logical equation (to apply it in message blocks to build secret information) will be used later to confirm and validate phase to proof the secret message if it is attacked or not.  
3. To Use different embedding techniques for each block that can increase the security to detect secret message and extraction.

Hence, this paper discusses and explains first benefit. To evaluate the result peak signal-to-noise ratio (PSNR) will be used. PSNR is the ratio between a signal's maximum power and the power of the signal's noise. Engineers commonly use the PSNR to measure the quality of reconstructed signals that have been compressed. Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale [12].

Table 1 shows the different size of MP3 file, which was used as a cover.

<table>
<thead>
<tr>
<th>Table 1: Data Set</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>File Size in Bytes</td>
<td></td>
</tr>
<tr>
<td>Test1</td>
<td>5,872,584</td>
<td></td>
</tr>
<tr>
<td>Test2</td>
<td>4,563,728</td>
<td></td>
</tr>
<tr>
<td>Test3</td>
<td>3,964,589</td>
<td></td>
</tr>
<tr>
<td>Test4</td>
<td>2,773,818</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 shows the PSNR results of our proposed method. We have embedded 40KB as speech in different MP3 file sizes. In experimental result, we chose different LSB bit embedded 1-bit, 2-bit and 4-bit for embedding secret speech and benchmark with LSB-Based.

<table>
<thead>
<tr>
<th>Table 2: Experimental results of proposed method.</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE NAME</td>
<td>METHODS</td>
<td>1LSB</td>
<td>2LSB</td>
</tr>
<tr>
<td>TEST1</td>
<td>LSB-PROPOSED</td>
<td>66.1083</td>
<td>62.4070</td>
</tr>
<tr>
<td></td>
<td>LSB-BASED</td>
<td>62.4450</td>
<td>58.0902</td>
</tr>
<tr>
<td>TEST2</td>
<td>LSB-PROPOSED</td>
<td>66.4275</td>
<td>62.0469</td>
</tr>
<tr>
<td></td>
<td>LSB-BASED</td>
<td>63.2982</td>
<td>59.2824</td>
</tr>
<tr>
<td>TEST3</td>
<td>LSB-PROPOSED</td>
<td>65.6908</td>
<td>61.3546</td>
</tr>
<tr>
<td></td>
<td>LSB-BASED</td>
<td>62.1402</td>
<td>57.9353</td>
</tr>
<tr>
<td>TEST4</td>
<td>LSB-PROPOSED</td>
<td>64.9981</td>
<td>60.6220</td>
</tr>
<tr>
<td></td>
<td>LSB-BASED</td>
<td>61.5761</td>
<td>57.4329</td>
</tr>
</tbody>
</table>

**Conclusions:**

Basically, the designers of steganography technique have used basic model for embedding and extracting secret messages. Some of them used key for embedding message in the host signal, and also used the same key to extract secret messages. This model used real information for secret message that is embedded in the cover media, and the result Stego Object contains cover and message. However, it increases the probability of attackers to destroy the secret message and to read it. So, the attack can modify or remove the secret message, because the attacker has discovered the secret message. Our Proposed model uses Mathematical equation to partition secret message into blocks, and applies permutation equation to re-order the blocks position, which will change and create new secret message addressing. So, if attackers catch the Stego object they can’t know the secret message contains. In addition, the proposed model applied a mathematical model for embedding, and also used map for extracting secret message. All these techniques increase the security of Stego object and also reduce the probability to attack the secret message or exchange it.
REFERENCES


