International Engineering Journal For Research & Development
Vol.4
Issue 1

E-ISSN NO:-2349-0721

Impact factor : 3.35

ENHANCED SECURITY FOR AUDIO SIGNALS USING STEGANOGRAPHY

Dr. S.L. Satarkar , Mr. T. R. Sangole

Head, Department of Computer Science & Engineering

College of Engineering & Technology, Akola (MH)

shri1satarkar@rediffmail.com

ABSTRACT

Steganography is a useful tool that allows covert transmission of information over an overt communications channel. Combining covert channel exploitation with the encryption methods of substitution ciphers and/or one time pad cryptography, steganography enables the user to transmit information masked inside of a file in plain view. The hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher.

In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size.

In the proposed system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. It uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

The basic idea behind this paper is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined.

KEYWORDS

Audio Signals, Message Hiding, Stegenography,

1. INTRODUCTION

Steganography is the practice of hiding information “in plain sight”. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer – the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the

content of the secret message unreadable while not preventing non-intended observers from learning about its existence. Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding.

There are numerous methods used to hide information inside of Picture, Audio and Video files.

2. OVERVIEW

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). The origin of steganography is biological and physiological. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia". A short overview in this field can be divided into three parts and they are Past, Present and Future.

2.1 PAST

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists.

Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information.

2.2 PRESENT

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. In modern approach, depending on the nature of cover object, steganography can be divided into five types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

So, in the modern age so many steganographic techniques have been designed which works with the above concerned objects. More often in today's security advancement, we sometimes come across certain cases in which a combination of Cryptography and Steganography are used to achieve data privacy over secrecy. Various software tools are also available in this regard.

2.3 FUTURE

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual

Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

3. DETAILS AND TECHNIQUES

Information can be hidden inside a multimedia object using many suitable techniques. As a cover object, we can select image, audio or video file. Depending on the type of the cover object, definite and appropriate technique is followed in order to obtain security. In this section, we will discuss different techniques or methods which are often used in image, audio and video steganography.

3.1 TEXT STEGANOGRAPHY

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways.

Many techniques involve the modification of the layout of a text, rules like using every n-th character or the altering of the amount of white space after lines or between words. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key.

3.2 IMAGE STEGANOGRAPHY

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in “noisy” areas that draw less attention—those areas where there is a great

deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

Each of these techniques can be applied, with varying degrees of success.

3.3 AUDIO STEGANOGRAPHY

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files.

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The list of methods that are commonly used for audio steganography are listed and below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

3.3.1 LSB CODING

Using the least-significant bit is possible, as modifications will usually not create audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks.

3.3.2 PARITY CODING

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

3.3.3 PHASE CODING

Phase coding addresses the disadvantages of the noise inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

3.3.4 SPREAD SPECTRUM

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

3.3.5 ECHO HIDING

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

3.4 VIDEO STEGANOGRAPHY

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

3.5 PROTOCOL STEGANOGRAPHY

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI

network model there exist covert channels where steganography can be used.

4. EXISTING SYSTEM

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. It supports water marking method to encode .It complexity arises when more message to be encoded. The message length is restricted to 500 characters. It doesn't shows the variations occurred after encoding the message. The LSB algorithm in the existing system is not efficient because it hides the message in consecutive bytes received from audio files.

The disadvantages of existing system is

- Selection of audio formats is restricted to one.
- Non-Provision of encryption key
- Length of the message is limited to 500.
- Absence of frequency chart to show the variations.
- Lack in good user interface.
- Consume much time to encode and decode.
- Non-Provision of sending the file to the destination.
- User needs to understand better to know the operations.

These are the disadvantages in the existing system which can be overcome by the proposed system.

5. PROPOSED SYSTEM

It is a method of hiding the message in the audio file of any formats. It provides an easy way of implementation of mechanisms when compared with audio steganography. Apart from the encoding and decoding in Audio steganography, It contain extra layers of encryption and decryption. The four layers are:

- Encoding
- Decoding
- Encryption
- Decryption

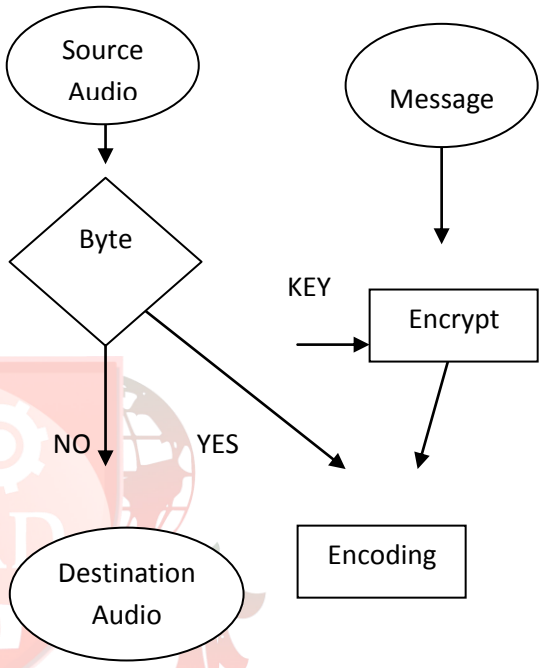

Figure: Encoding

- **Encoding** is a process of hiding the message in the audio.
- **Decoding** is a process of retrieving the message from the audio.

Modified LSB(Least Significant Bit) Algorithm is used to encode the message into audio. It performs bit level manipulation to encode the message. The following steps are

1. Receives the audio file in the form of bytes and converted in to bit pattern.
2. Each character in the message is converted in bit pattern.
3. Replaces the LSB bit from audio with LSB bit from character in the message.

Powerful encryption algorithm is used to encrypt the message before encoding for further security purpose. The following steps is used to

1. Adding all ASCII values of characters in
2. Converting the sum into bit pattern
3. Performing logical operation to the bit
4. Adding to the encoded character.

For more security enhancement the encoding is done only when the byte which is received from the audio is 254 or 255.This selection of particular bytes for encoding will reduce the lack in quality of audio after encoding. It can be proved by seeing the frequency chart indicating the deviations happened after encode. Thought it shows bit level deviations in the chart as a whole the change in the audio cannot be determined.

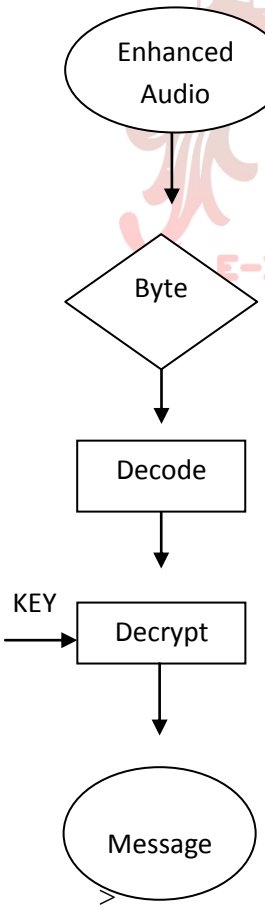

Figure: Decoding

5.1 BASIC IDEA

The basic idea behind this is to provide a good, efficient method for hiding the data from hackers and sent to the destination in safe manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message.

The main two features of this system are

1. Size of file is not changed after encoding.
2. Since it is bit level manipulation the sound variations cannot be determined by any current

The proposed system over comes all the restrictions made on the existing systems. It provides good looking environment to user .It also provide the user to give secret key for encryption. The length of message is more than the existing system, and provides frequency chart to see the variations after encoding. The quality of the audio doesn't change variably. It cannot detect the lack in quality of sound. The encryption key can be any combination of characters, symbols, and numbers. The key which is used for encoding is also used for decoding .This is a secret key where the both user have to agree upon a single common key.

5.2 ADVANTAGES OF PROPOSED SYSTEM

- Different Audio formats are supported the system.
- Provision of encryption key and performs simple encryption algorithm.
- The encryption key is modified by a strong algorithm to get a new key, which is used to encrypt the message.
- So even if the key is known for an intruder, he cannot break the code with that key.

- Presence of frequency chart to show the variations that helps the user to determine.
- Consumption of time to encode and decode is reduced.
- Provision of sending the file to the destination is given so that after encoding the user can send the file by giving destination IP address.

5.3 ENCODING

The audio file contains set of bytes. For example is take an audio file which play for 10 seconds. It has more than 60,000 bytes. Each byte is received and checked if the received byte is 254 or 255. If it is byte 255 or 254, encoding is done.

So for one character to encode we need eight 254 or 255 bytes. One character is hidden in consecutive eight 254 or 255 bytes. In order to mark the end of message, the LSB bit of next eight consecutive 254 or 255 bytes which comes after all the messages have encoded are replaced by 1.Before encoding, message is encrypted using public key.

5.4 DECODING

The encoded file is decoded to get the message. The message is decoded first and then decrypted by the public key. The eight consecutive 254 or 255 bytes are taken and decrypted with the public key. This decrypted byte have value less than 128.So if the value is 255 after decrypted then it is said to be end of message.

5.5 ENCRYPTION

The user allowed entering the public key/shared key in any combination of numbers, symbols and characters. The key contains set of characters. All characters are converted to ASCII value and add all the ASCII value to get single number. And that single number is converted to bit pattern and by simple logical operation (XOR) you can get a single number less than 128.It is a new private key .It is added to the characters one by one in the message, before encoding.

5.6 DECRYPTION

The LSB bits of consecutive eight 254 or 255 bytes are taken and subtracted with the key to get the original character.

6. APPLICATION

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate intelligence by sending out trade secrets without anyone at the company being any the wiser.

Steganography can also be used in the noncommercial sector to hide information that someone wants to keep private. Spies have used it since the time of the Greeks to pass messages undetected. Terrorists can also use steganography to keep their communications secret and to coordinate attacks.

As you can hide information without the cover source changing, steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files

because of a watermark, steganographic methods can be used to hide this.

7. DISCUSSION

Steganography is used to have a level of privacy while doing data communication with others. We have already discussed several methods related with that. But only the concealment of data may not give the best result always. So, some extra level of security along with the privacy has to be incorporated. Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of the computer era. Although the techniques are still not used very often, the possibilities are endless.

Again the concept of Dual Steganography i.e., first application of steganography in between the embedding object and the cover object and then again apply the same method with the help of other object, can be developed to obtain a new definition of security. Concept of object self encryption technique before the application of steganography to hide that inside a cover can also be developed to achieve a level of security.

8. CONCLUSION

Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. In the near future, the most important use of steganographic techniques will probably be lying in the field of audio signals. Content providers are eager to protect their data against illegal access and provide a way of tracking the owners of these materials.

This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust.

9. FUTURE ENHANCEMENTS

Although it is well modulated system, it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message.

The quality of the sound in the encoded audio file can be increased. There are number of ways that this project could be extended. Its performance can be upgraded to higher levels in practical conditions. There are also other weighting algorithms like spread spectrum, echo data hiding etc., and those can be implemented. Instead of having common secret key to encode and decode, a public–private key pairs will be introduced.

10. REFERENCES

[1]. [Anderson and Petit colas 2001] Anderson, R., Petitcolas, F.: On the limits of the steganography, IEEE Journal Selected Areas in Communications, 16, 4, 474-481.

[2]. Audio Engineering Society E-Library - Steganographic Approach to Copyright Protection of Audio; Preprint Number: 7067 Convention: 122 (May 2007)

[3]. Eugene T. Lin, Edward J. Delp. A Review of Data Hiding

[4]. F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no. 7,1999, pp. 1062–1078.

[5]. Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on Publication Date: 5-7 April 2004

[6]. Increasing robustness of LSB audio steganography using a novel embedding method.Cvejic, N. Seppanen, T. MediaTeam Oulu Group, Oulu Univ., Finland.

[7]. Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[8]. Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography (2003).

[9]. Robert Krenn. Steganography and steganalysis paper no. : 11.

[10]. Saraju P. Mohant. Digital Watermarking: A Tutorial Review