AUDIO STEGANOGRAPHY-MODIFIED LSB USING REDUCED DISTORTION

Pooja Sharma

M.tech(C.S.E) Research Scholar, Galgotias College of Engineering & Technology
Greater Noida, (India)

ABSTRACT

In this study, we will have a survey on audio steganography recent researches. In present day to day life, effective data hiding methods are needed due to attack made on data communication. This paper presents the technique for the above requirement. In this proposed method, secret message in form of audio file is embedded within another carrier audio file (.wav) .In the transmitter end the output will be similar to the carrier with secret message embedded inside. The hacker will be blinded by the transmitted signal. At the receiver end the original message can be retrieved without any loss. The entire proposed system is simulated and their corresponding waveforms prove the effectiveness of this method.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.The paper follows the least distortion method applied in improving the LSB and data is hided in the bits whose frequency ranges are least audible. 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 Steganography, LSB Method, Cryptography, Data Hiding, FrequencyRange, Logical Operators***

I. INTRODUCTION

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. A secret information is encoded in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data .It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carriermedium, then the method has failed. The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.

Basically, the model for steganography is shown in Fig below. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

This paper proposes a technique of audio steganographic that gives a unique stage to hide the secret information in audio file. Least Significant Bit (LSB) data modification technique is the most easy and popular technique used for audio steganography. This proposed technique has been tested successfully on a .wav using MATLAB.

The information hiding process consists of following two steps:

1) Identification of redundant bits in a cover-file. Redundant bits are those bits that can he modified without corrupting the quality or destroying the integrity of the cover-file.

2) To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

Audio Steganography is the technique of hiding information inside an audio signal. 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. As data is embedded in the signal, it gets modified. This modification should be made imperceptible to the human ear. Image can also be taken as a medium but audio

steganography is more challenging because of the characteristics of Human Auditory System (HAS) like large power, dynamic range of hearing and large range of audible frequency. All paragraphs must be indented. All paragraphs must be justified, i.e. both leftjustified and right-justified.

II. LITERATURE SURVEY

2.1 Hiding is done Using Pattern

Wav files make use of either 8 or 16 bits to store sound information. 8 bit files allow values of sound in the range between 0 and 255 and the 16 bit files will have values from 0 to 65535. By changing the values of bytes slightly, we can store our secret data.

If for example, we have 8 byte sample of wav audio:

200 234 157 141 128 178 62 39

These values would be represented in binary as:

11001000 11101010 10011101 10001101

10000000 10110010 0111110 00100111

Suppose we want to hide the binary file 11101010 (234) inside this sequence. We replace the least significant bit in each byte of wav sample(the least significant bit because it will cause the least amount of change in the value) by bits of the binary form that makes up 234. The sequence of binary after modifying wav by stuffing 234 is shown below:

11001001 11101011 10011101 10001100

10000001 10110010 0111111 00100110

The new binary values deviates from the values of original audio only a little.. These discrepancies are negligible since human auditory system cannot differentiate between the two at such small levels.

This system has replaced the LSB of every byte whatever its value may be. There won't be much variation from original audio file if the byte value whose LSB being replaced is large. But if the value is very less say 1 or 2, the change in LSB causes change in the value of the byte by around 100% . This large deviation may make one think of LSB being used and one may try to crack it. This could be overcome by modifying least significant bit

only when its value is large or by using some pattern to stuff bits in various positions of the byte in all channels of WAV file which is our proposed system.

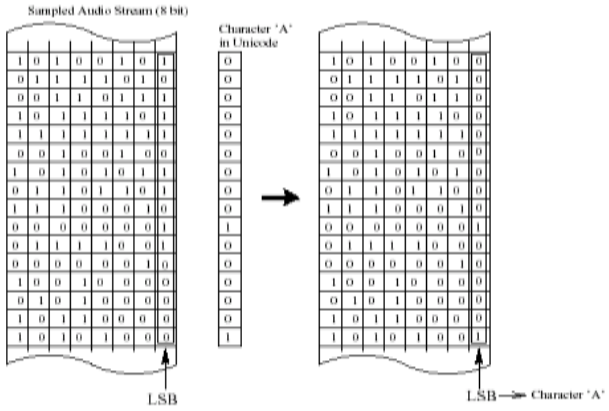

Fig.1

Wav file consists of number of channels. In the modified LSB algorithm proposed here, instead of stuffing bit of the message only in the least significant bit in the consecutive bytes of wav file, a pattern is used to stuff bits. The same pattern can be made use to decode the file to get back the hidden message. Since it is quite easy to encode and decode if we make use of the same pattern to stuff message bits in different positions of byte in all channels, we stuff the bits in same pattern in all the channels. For example if we use the pattern 3142, then the 1st bit of message is stored at 3rd bit position , 2nd bit of message is stuffed in 1st position, 3rd bit in 4th position, 4th bit in 2nd position, 5th bit in 3rd position and so on.

In this scheme we stuff the entire byte in 1 channel, next byte in next channel and so on using the same pattern. Instead of stuffing bits in consecutive sequential bytes as in conventional LSB, we stuff entire byte in one channel, next byte in next channel and so on. This gives the shield against possible attack by trying to read the wav file sequentially.

For example if we want to stuff the message “abcdef” in a wav file consisting of 3 channels using the pattern 3142, character ‘a’ will be stuffed in 1st channel, ‘b’ in 2nd channel, ‘c’ in 3rd channel, ‘d’ in 1st channel and so on. While storing a character in a channel, pattern 3142 is used to stuff bits. ASCII value of ‘a’ is 97 i.e 01100001. It requires 8 bytes of channel 1 to stuff ‘a’, 1st bit 1 is stored in 1st byte of channel 1 at position 3, 2nd bit 0 is stored in 2nd byte of channel 1 at position 1 and so on according to the pattern chosen. This gives additional security and robustness for encoding scheme.

2.2 Hiding is done Using Key

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Here a key is taken at the transmitter with that a pseudo sequence is generated and this sequence is performed a logical operation with the secret message. Then the embedding process is carried out with the carrier audio file and is transmitted at the transmitter side as

In the receiver side with the audio stego file the LSB are recovered first and with the known key generated at the transmitter the decryption process is carried out and the secret message is recovered from the stego file

The steps are as follows:

1. Get the carrier audio signal and calculate the length it is noted as A1.
2. Get the secret audio or text file and calculate the length, it is noted as A2.

3. As per the assumption check whether the L1 is eight times greater than A2.

3.1 If it is greater than proceed with the proposed algorithm.

3.2 Else display the message as secret message is too large and initializes the process from starting.

4. Get the secret key and with that a pseudorandom sequence is generated and is performed logical operation with the secret message and is then embedded using LSB method in the carrier audio file.

5. The stego file is created and is transmitted from the transmitter side.

The reverse operation is performed at the receiver side for retrieving the secret message embedded in the transmitted stego audio file.

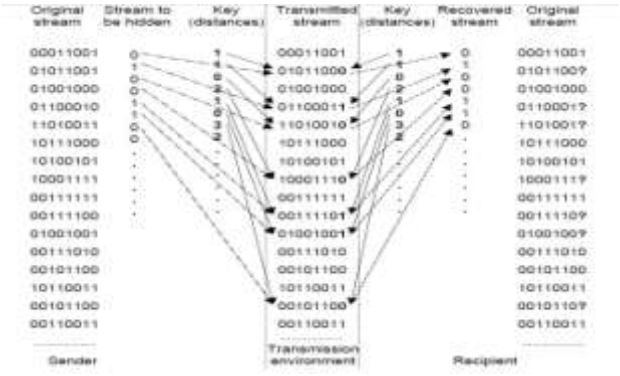

Fig.2

III.PROPOSED WORK

Enhanced Audio Steganography is a method of hiding the message in the audio file of any formats. EAS provides an easy way of implementation of mechanisms when compared with audio steganography.

To improve the outcome and quality of received audio file with the image and data hidden in it is done in such a way that it would lead to less distortion n more robustness.

This can be done by applying the LSB technique separately in audible and non-audible voices. The data hidden in less audible and non-audible voice will lead the audio file to be less or not at all distorted. The misuser or intruder would find no difference in cover file and original audio file.

Apart from the encoding and decoding in Audio steganography, EAS contain extra layers of encryption and decryption.

The four layers in EAS are:

- Encoding
- Decoding
- Encryption
- Decryption

Encoding is a process of hiding the message in the audio.

Decoding is a process of retrieving the message from the audio.

Accepted audible range of frequency is 20 to 20000 Hz.

Range of frequency individual hear is greatly influenced by environmental factor.

Frequency below 20Hz → generally felt rather than heard.

Frequency above 20000Hz → sensed by young people.

1)Audible frequency is between 32.70 Hz to 16744 Hz.

2) Non-Audible Frequency →Frequency below 32.70 Hz → lowest organ note , Lowest note for tuba , Large pipe organs etc.

- Frequency below 32.70 Hz are not audible.
- 32.70 Hz→ Lowest C on a standard 88-key piano.
- Frequency above 16744 Hz are also not audible.
- 16744 Hz → the tone that a typical CRT TV emits while running.

Fig. 3 Image Hidden Screen Shot

Fig.4 Image retrieved Screen shot

Fig.5 Final Retrieved Image

3.1 Algorithm for Stagnography Using Logical Operator

3.1.1 For Encodind Process

1. First hide the identity.
2. Hide the size of image.
3. Apply logical operator in LSB Coding.

3.1.2 For Decoding Process

1. Matchtheidentity hidden in encoding process.
2. Fetch the size of the image.
3. Apply logical operator in LSB coding to retrieve the image.
4. Make the frame with the help of image size recovered and set all value of image at proper pixel position.

3.2 Logical Operator During Encoding

1. Take the last wave sample LSB (648) where last size bit is stored
   Set as bit1
2. Take the next wave sample LSB (649)
   Set as bit2
3. Fetch the all bit sample of image from column vector starting from first to last
   Set as bit3 (FROM 1: LENTH)

4. Now apply the XOR Operationto bit1 and bit2 and obtain the bit4.
5. Now apply the XOR Operationto bit3 and bit4to obtain new bit named bit5
6. At last we will hide bit5 to wave sample (650)
7. This will be happened until all the bits are imbedded.

3.3 Logical Operator During Decoding

1. Take the last wave sample LSB (648) where last size bit is stored
   Set as bit1
2. Take the next wave sample LSB (649)
   Set as bit2
3. Fetch bit sample from next wave sample LSB (650) where the image data is saved
   Set as bit3
4. Now apply the XOR Operation to bit1 and bit2 and obtain the bit4
5. Now apply the XOR Operationto bit3 and bit4to obtain new bit named bit5
6. We will hide bit5 to wave sample (648) TO LENGTH
7. Fetch the LSB OF wave sample starting (648) all this LSB bit is the image data
8. All data is kept in the frame of the image using the size of image obtained.

IV. EVALUATION OF AUDIO STEGANOGRAPHY

4.1 Advantages

Audio based Steganography has the potential to conceal more information

- Audio files are generally larger than image
- Our hearing can be easily fooled
- Slight changes in amplitude can store vast amounts of information

The flexibility of audio Steganography is makes it very potentially powerful :

- The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications.
- For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented. On the other hand, a large corporation wishing to protect its intellectual property from "digital pirates" may consider a more sophisticated method such as phase coding, SS, or echo hiding.

Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptography technologies.

- Users no longer have to rely on one method alone. Not only can information be encrypted, it can be hidden altogether.

Many sources and types makes statistical analysis more difficult :

- Greater amounts of information can be embedded without audible degradation

4.2 Security

- Many attacks that are malicious against image Steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be implemented against audio Steganography schemes. Consequently, embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio.
- As emphasis placed on the areas of copyright protection, privacy protection, and surveillance increases, Steganography will continue to grow in importance as a protection mechanism.
- Audio Steganography in particular addresses key issues brought about by the MP3 format, P2P software, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

4.3 Disadvantages

- Embedding additional information into audio sequences is a more tedious task than that of images, due to dynamic supremacy of the HAS over human visual system.
- Robustness: Copyright marks hidden in audio samples using substitution could be easily manipulated or destroyed if a miscreant comes to know that information is hidden this way.
- Commercialized audio Steganography have disadvantages that the existence of hidden messages can be easily recognized visually and only certain sized data can be hidden.
- Compressing an audio file with lossy compression will result in loss of the hidden message as it will change the whole structure of a file. Also, several lossy compression schemes use the limits of the human ear to their advantage by removing all frequencies that cannot be heard. This will also remove any frequencies that are used by a Steganography system which hides information in that part of the spectrum.

V.FUTURE SCOPE

In today's world ,we often listen a popular term HACKING. Hacking is nothing but an unauthorised 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 steganalyser cracks the cover object to get the hidden data. So whatever be the technique will be developed in future,degree of security related to 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 below mentioned technique. Work on this techniques is in progress. The better and improved version of steganography can be done as follows:

To improve the outcome and quality of received audio file with the image and data hidden in it is done in such a way that it would lead to less distortion n more robustness.

This can be done by applying the LSB technique separately in audible and non-audible voices. The data hidden in less audible and non-audible voice will lead the audio file to be less or not at all distorted. The misuser or intruder would find no difference in cover file and original audio file.

VI. AUDIO STEGANOGRAPHIC APPLICATIONS

Audio data hiding can be used anytime you want to hide data. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. In the

business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention. Audio data hiding can also be used in the non commercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. In the project ARTUS1 which aims to embed animation parameters into audio and video contents. Data hiding in video and audio, is of interest for the protection of copyrighted digital media, and to the government for information systems security and for covert communications. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

REFERENCES

[1] Fridrich, Jessica and others. "Steganalysis of LSB Encoding in Color Images." Proceedings of the IEEE

[2] http://en.wikipedia.org/wiki/Steganography

[3] International Conference on Multimedia [2] Sridevi R., Damodaram A., SVL.Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, 2009.

[4] Muhammad Asad, JunaidGilani, Adnan Khalid "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 2011 international conferenceon Computer Networks and Information Technology (ICCNIT), pages 143-147

[5] MasoudNosrati, RonakKarimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.

[6] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.

[7] NedeljkoCvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.