Audio Steganography Algorithm Using Java

Maitri Patel

Assistant Professor
Department of Computer Engineering,
Sabar Institute of Technology for Girls, Tajpur, Sabarkantha, India.
maitri_148@yahoo.co.in

Abstract: Now a day, we are widely using internet for exchanging any kind of data. So, while transmitting our data, protection of our data is very important from unauthorized access. Steganography has literally meaning of "Covered Writing". Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. Steganography techniques can be applied to images, a video file or an audio file. In this paper, we introduce new method of Steganography using audio file for transmitting our confidential messages through internet. The algorithm converts the input audio file and the text file which contains our confidential message into binary numbers which can't be understandable by any user. After this, it hides the message into the input audio file with my own encryption technique and converts it into output audio file which contains our confidential message. The main advantage of this type of technique is the length of input and output file will be same.

Keywords – Steganography, embedding, Stego medium, Key Streams, Cryptography

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient. The goal of Steganography is "to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. These formats are popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message.A pure steganography system's success relies solely on the secrecy of the algorithm.

Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. It is done in mainly two parts.

Hiding

Hiding a message in Wave samples is very similar to hiding it in the pixels of a bitmap. Again, we use a key stream to skip a number of carrier units (samples/pixels), grab one carrier unit, put one bit of the message into the lowest bit of the carrier unit, and write the changed unit to the destination stream. When the entire message has been hidden like that, we copy the rest of the carrier stream.

Extracting

Again, we use the key stream to locate the right samples, just as we did while hiding the message. Then we read the last bit of the sample and shift it into the current byte of the message. When the byte is complete, we write it into the message stream and continue with the next one.

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. Steganography can be implemented using Audio files like MP3, Wave.Human ears are not able to easily find the difference between the original sound and the resultant sound. You might miss the files that can hide lots of bytes without becoming larger, and can be generated in a few seconds, so that you don't have to store the original files on your disk. It is time to add Wave Audio to the list.

Need for Steganography

The following figure provides a simple example of a problem that benefit from the use of steganography:

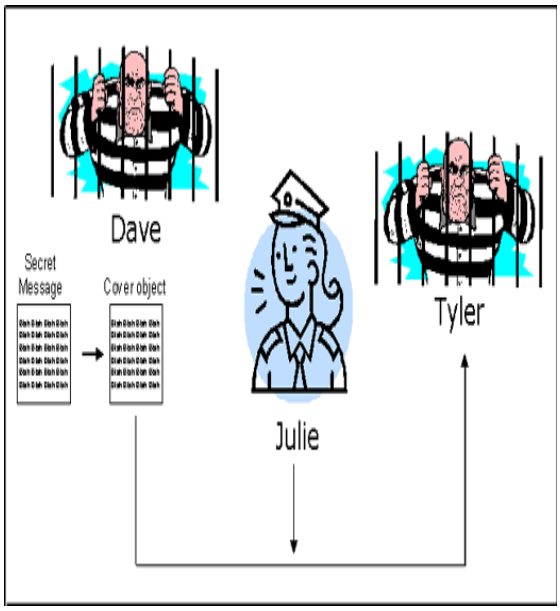

Fig 1 benefit from the use of steganography

Tyler and Dave are in prison. They are trying to communicate an escape plan, but unfortunately have one major problem: Warden Julie has access to ALL correspondence that passes between the two prisoners. Relying solely on encryption is out of the question since it would arouse Julie's suspicion and result in Dave and Tyler eating only bread and water for six weeks. They also would not be allowed to watch cable television during that time period. So, to avoid being caught, the two prisoners must devise a way to pass messages that appear harmless to Julie; the two prisoners might set up a code language beforehand. Then perhaps Dave may write a message to Tyler that says "Hey, I hear those new mint flavored Oreo's are delicious!" Tyler would know to interpret that to mean "Lets, hide in the trash dumpster and escape when the garbage truck comes on its weekly pick-up." That might work, but there is always the possibility that Julie intercepts the message, figures out the code, and changes the message before sending it on to Tyler. Tyler would have no idea, and Julie would be able to trick him and Dave so that they are caught in the attempted escape.

In order to give people like Dave and Tyler more flexibility in their steganography system and prevent Julie from catching on so quickly, multiple protocols of steganography exist, each with their own set of strengths and weaknesses. The three main protocols are pure steganography, secret key steganography, and public key steganography.

II. THE PROPOSED TECHNIQUE

For encrypting any image first we get the image which we want to encrypt and the key value. Key value is something like password. Security of key value is more important rather than our algorithm. Than we are taking the pixel values of that image. Here, we perform only arithmetic operation to pixel values of image with our key value. We have to repeat the process until end of pixel values of plain image. After that we create image using that pixel values than we can get encrypted image. This encrypted image is known as cipher image. For decrypting image we perform same operations but into reverse manner. After decryption of image at the receiver side we can get our original plain image.

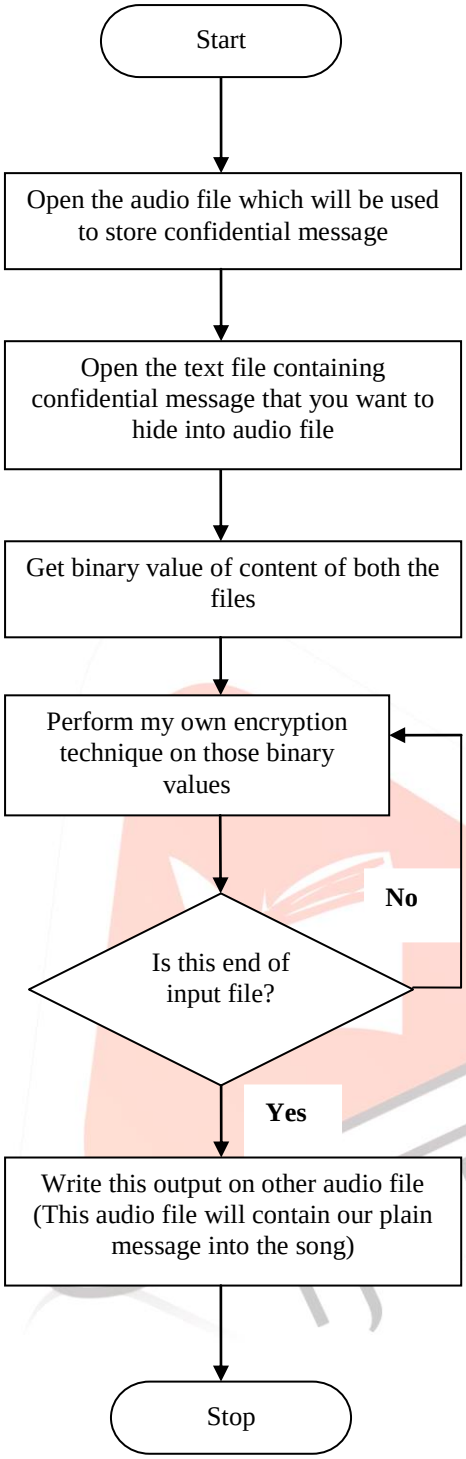

Fig 2 The structure for the implemented technique

Methods of code

1. **Available ()** - Returns the number of bytes of input currently available for reading.
2. **Read ()** - Returns the integer representation of the next available byte of input. -1 is returned when the end of the file is encountered.
3. **toBinaryString()** - Returns the string that contains the binary equivalent of given argument.
4. **toCharArray()** - Returns array of characters for the entire string given as an argument.
5. **charAt()** - Returns the character at the specified location from a given string.

III. THE EXPERIMENT ANALYSIS

Select one input audio file named "AIRTEL.mp3" of size 255 KB and one text file containing confidential message of size 1 KB. I will hide the confidential message into our audio file and convert it into output audio file named "India.mp3" with "SAME LENGTH" i.e. 255 KB. I'll Show the binary values of input audio file, text file containing confidential message and output audio file.

Following is the outcome of my experimental analysis with same audio file and different confidential message:

Confidential Message: Hi,How r u???? Size of input audio file:260885 Size of text file containing confidential message:20	**Confidential Message:** Password is tango charlie. Size of input audio file:260885 Size of text file containing confidential message:32	
Binary values of audio and text file containing confidential message:	Binary values of audio and text file containing confidential message:	00000001
1001000	1010000	00000001
1101001	1100001	00000001
101100	1110011	00000001
1001000	1110011	00000000
1101111	1110111	00000000
1110111	1101111	00000001
100000	1110010	00000001
1110010	1100100	01011001
100000	100000	01101001
1110101	1101001	01101111
111111	1110011	01100110
111111	100000	00000000
111111	1110100	00000001
111111	1100001	00000001
1101	1101110	00001111
1010	1100111	00000001
1101	1101111	00000001
1010	100000	00000100
1101	1100011	01010011
1010	1101000	00000001
11111111111111111111111111111111	1100001	00000011
Binary values of output audio file:	1110010	11111011
11111111	1101100	00010101
11111010	1101001	00000000
01010000	1100101	00000011
11000101	101110	00000101
00000000	1101	00000111
00000000	1010	00001001
00000000	1101	00001101
00000001	1010	00001111
00000001	1101	00010001
00000000	1010	00010100
00000001	11111111111111111111111111111111	00010110
00000000	Binary values of output audio file:	00011001
00000000	11111111	00011010
00000001	11111010	00011101
00000001	01010001	00100001
00000000	11000100	00100010
00000001	00000000	00100100
00000001	00000000	00100111
00000000	00000000	00101010
00000000	00000001	00101100
	00000001	00110001
	00000000	00110010
	00000000	00110100
	00000000	00110110
	00000000	00111010
		00111100

IV. CONCLUSION

Steganography will continue to increase in popularity over cryptography. As it gets more and more advanced as it will get the Steganalysis tools for detecting it. In future we will see more encrypted data being hidden using Steganography as the combination of the two provides an even hard target to crack (but not necessarily a harder concoction to assemble). The Main advantage of the Audio Steganography is the files that can hide lots of bytes without becoming larger, and can be generated in a few seconds, so that you don't have to store the original files on your disk. Steganography may also be used to hide sensitive information and transfer it from one place to another. People should be focusing on the important aspects of Steganography, such as what it is really used for, instead of believing propaganda put out by the media like Steganography is a potential threat that is probably used to hide illegal material such as child pornography or it will be used by Terrorists.

REFERENCES

[1] http://www.snotmonkey.com/work/school/405/overview.html
[2] http://en.wikipedia.org/wiki/Key_(cryptography)
[3] http://www.webopedia.com/TERM/S/steganography.html
[4] http://en.wikipedia.org/wiki/Steganography
[5] Teach Yourself JAVA: by Joseph O'neil and Herb Schildt
[6] The Complete Reference, Fifth Edition: by Herbert Schildt
[7] http://www.techopedia.com/definition/4131/steganography