VOL. 12, NO. 7, APRIL 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CAPACITY AND SECURITY ENHANCEMENT IN AUDIO BASED STEGANOGRAPHY USING RANDOM LOCATION TECHNIQUE

Muhammad Anwaar[1], Wareesa Sharif[2], Zartashia Shameen[3] and Khalid Bashir Bajwa[1]
[1]Department of Telecommunication Engineering, University of Engineering and Technology, Taxila, Pakistan
[2]Faculty of Computer Science and Information Technology, UniversitiTun Hussein Onn, Malaysia (UTHM)
[3]Department of Electrical Engineering, Air University, Islamabad, Pakistan
E-Mail: Muhammad.anwaar48@gmail.com

ABSTRACT

Audio steganography has attracted a great attention owing to secure communication for commercial and military purposes due to larger size of their files. Among these, audio based steganography has more potential to conceal information because audio files are larger in size as compare to other media. For audio steganography, mostly Least Significant Bit (LSB) techniques are used to hide the secrete data. LSB techniques hide data in limited capacity. Also, detection of data in lower bits is much easier, thus these techniques has less security. In this paper, audio based steganography technique is suggested. The proposed technique conceals data at the random location of audio signal by using chaotic based technique. The proposed technique enables us to hide the data in lower as well as higher significant bits of the audio data; that increases its capacity. It also enhances the security of the secrete data by placing at random location of the audio data. It believes that the given technique can be useful for secure communication of large amount of secrete data.

Keywords: steganography, audio steganography, secure communication, least significant bit (LSB) techniques, chaotic based technique.

INTRODUCTION

Steganography is the art and science of writing secretinformation in such a way that no one from the sender or the receiver finds the existence of the hidden data except the authentic recipient (Katzenbeisser and Petitcolas, 2000). The word steganography is the Greek originated word which means "concealed writing" and is the combination of two words as: steganos meaning "covered or protected" and graphei meaning "writing" (Al-Shatnawi, 2012). Steganography differs from cryptography in a sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret (Wang and Wang, 2004).

Steganography techniques can be implemented on various types of media like audio (Gopalan, 2003), video (Dasgupta, Mandal and Dutta, 2012), Image (Bailey and Curran, 2006) and text (Shirali-Shahreza and Shirali-Shahreza, 2006). Audio based steganography has more potential to conceal information because audio files are larger than images and small change in amplitude can store huge amount of information precisely (Singh, 2016). However, audio based steganography exploits the masking effect property of the Human Auditory System (HAS). HAS is more sensitive than Human Visual System (HVS) and it can identify the slight change in voice. Yet, HAS still tolerates common alterations in small differential range. For example, loud sounds tend to mask out quiet sounds. Additionally, there are some common environmental distortions, pointed that they would be ignored by listeners in most cases making it effective for hiding the data (Djebbar *et al*., 2012).

The basic methodology for sending and receiving hidden data using audio file as a cover is shown below in Figure1. Initially, both audio files and secrete data is converted into digital audio and digital data. After that, the digital data embeds in a digital audio file using a key to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message (Djebbar *et al*., 2012). This whole operation is known as steganography.

After that, stego file is sent to the receiver by the network, where the receiver recovers the hidden information from the stego file. The recovery of information from the stego audio is known as steganalysis. Steganalysis can be accomplished with the authentic key. Key plays an important role in secure communication if steganography is noticed.

There are many techniques available for audio based steganography. Among these, Least Significant Bit (LSB) is the most common technique used for audio steganography (Asad, Gilani and Khalid, 2011; Cvejic and Seppanen, 2002; Yadav, Mishra and Sharma, 2013). In this technique data is concealed in LSB bits of audio data. The host data before steganography and the stego data have the same characteristics. In LSB technique, only one of the least bit is changed; thus in steganalysis secret message can easily be detected. Furthermore, huge amount of secret message can't be embedded and robustness is also weak. Secret message can't be covered in each sample of data so there should be some technique or algorithm to hide secret message in random locations so transparency should be achieved and intruder had no way to sense the stego message.

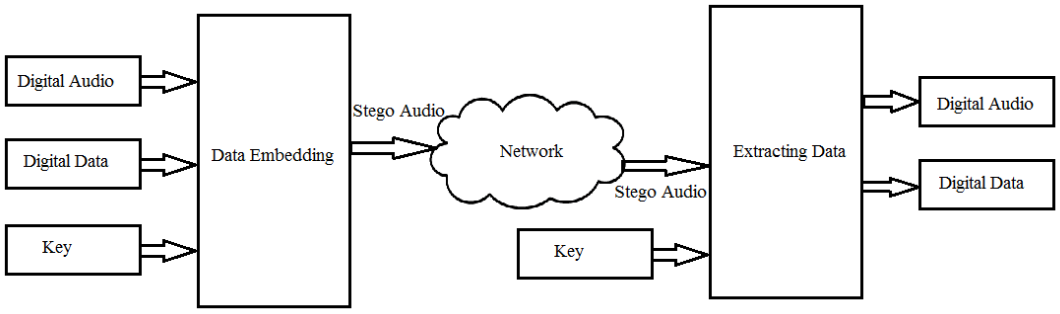

Figure-1. Basic model for sending and receiving hidden data by using steganography.

Also, some research has been performed to hide the data in higher bits. For example, Gopalan. (2003) used both higher and lower bits of the audio cover file for steganography. The covert message is represented in a compressed form with possibly encryption and encoding for added security. One bit in each of the samples of a given cover utterance is altered in accordance with the data bits and a key. However, in this research steganography is achieved by adding a noise in the audio file. Due to this noise a lot of intentional attackscan occur on the stego audio file to retrieve the data.

There are still many gaps in higher bit audiobased steganography. In this paper audio based steganography is presented for higher technique. For the given technique, audio is used as a cover file and text is used as a secrete message. This technique emphasis to enhance the capability and transparency of the audio based steganography.

DATA SET

Text used in our technique was the "steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient suspects the existence of the secret data in a form of security through obscurity".

This text is our secret information that was encoded in the audio file. The audio file obtained from the online dataset available at "http: // www. pacdv. com / sounds / voices-1. html". To validate this technique, we used "hello-4.wav" as a cover file. The characteristics of the cover file are given Table-1, below.

We used only one channel of the "hello-4.wav" file. The audio file contains some unwanted information at the start and at the end of the file. This information has been truncated to reduce the size of the audio file.

Table-1. The characteristics of the audio file used in our technique.

Type	Characteristics
File name	Hello-4
Audio type	.wav
Sampling rate	44100
Total number of samples	17658
Total number of channels	2

METHODOLOGY

The proposed methodology for steganography is shown below in Figure-2. In a given methodology, text is the secret information that is encoded in the audio file. Initially, a standard Huffman compression technique (Huffman, 1952) is applied on the incoming text and is altered into the bits. Similarly, the cover audio file is transformed into the bytes.

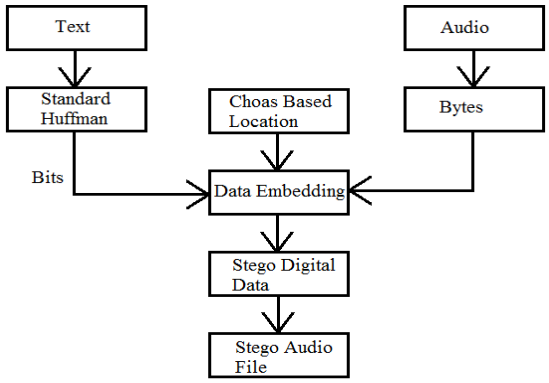

Figure-2. Encoding process of cover and secret data.

Afterward, a chaos based random location technique is applied for embedding the text bits into digital audio data. Chaos means a great disorder or confusion. Basically, chaos is a technique that is used for randomness and to create the disordered locations. This process will give us a stego digital data. In this technique, text was concealed in the different bifurcation random points.

ARPN Journal of Engineering and Applied Sciences

The bifurcation behavior of this technique is shown in Figure-3. In Figure-3 along x-axis "X" is the random variable and along y-axis orbit points are located to find the bifurcation points. At X<3 the bifurcation diagram showed a smooth behavior and as value of r (random variable) reached at x=3, logistic map information. Locations of the secret bits were synchronized between the transmitter and the receiver. Finally, the stego digital data has been converted into a stego audio file.

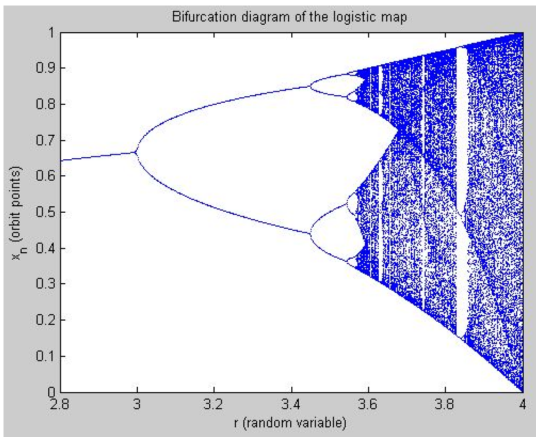

Figure-3. Bifurcation random points.

To recover the secrete text data, the steganalysis methodology is shown below in Figure-4.

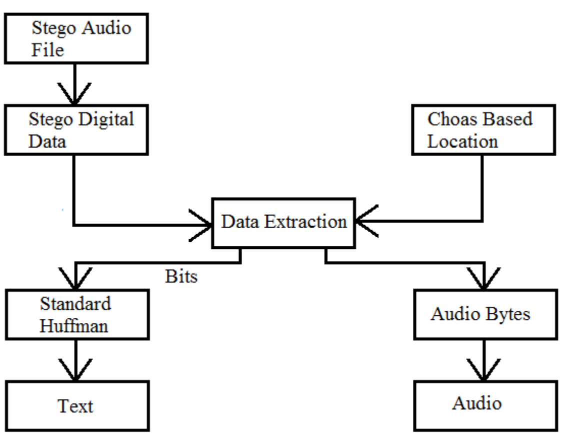

Figure-4. Decoding process of cover audio file and secret data.

In data recovery process, initially stego audio file has been converted into a digital data. Afterwards, chaos based random location technique is used to extract audio and text data. Data extraction process gives us a digital data audio and text data. To recover the secrete message, Huff transform has been applied on the extracted digital text data.

SIMULATION RESULTS

The given technique has been implemented in Matlab 2015a version. The output of the Huffman compression technique (Huffman, 1952) for our secret text is given in Table-2 below.

Table-2. Output of the Huffman compression technique for our secret text.

Secret text	Output
steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient suspects the existence of the secret data in a form of security through obscurity.	1111001111100010101111110001 1001100011110001011110101 0 0100011010101001111101010 1 0111101001001111010100101 1 1110011110010100101111000 0 1110010101110101101100110 1 1111100001101011110101011 0 0110000010100001111001001 1 1111010011110001000101010 1 0010100110111001110011111 1 0000101010111011111110111 1 0101011100010111111101010 1 0100111100001010111011111 1 0110110010010100101101010 0 0010101100110101011110100 1 0010111111001010110001100 1 0101011001110000111101010 0 1011110100101111100111100 1 0101000011100110011011101 0 1011110100100111101010111 0 1011111100001110011111110 0 0101001011110000111001010 1 0011110001111001111110000 1 1100111101110010101110001 1 1101101100111101010011011 1 1110001111001010111011111 1 1110111010011110110111110 1 1101010101111010010011110 1 0100111100101001111101111 1 0011111100001101011110101 0 1100110000010101111010010 0 1111010101110101111011011 1 1000111111110010100111001 0 1111110010110101001011010 1 0100001100111100101110101 0 1100110000010101110101111 0 1101111111110010011111100 0 1101010111101001011100110 0 1111111000110010010101100 1 0110011101011011111111100 1 0011111100011

For this technique, capability and the transparency of the stegoisconsidered. Capability is the amount of secret data that is to be embedded in the cover message. On the other hand transparency is how efficiently information can be embedded and robustness indicates the resistance to attack.

The audio signal is as shown in Figure-5. The audio file is in a stereo format.

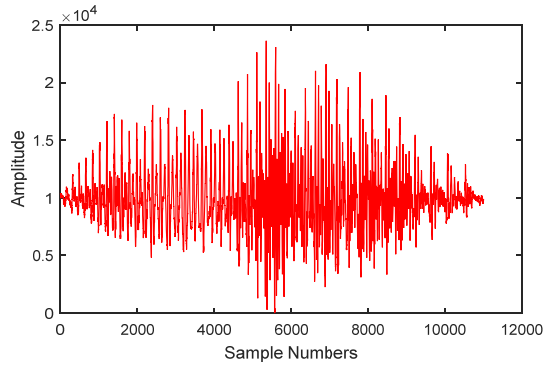

Figure-5. Host signal plot in Matlab.

Figure-6 below shows the stego signal which is the combination of host and secret bits.

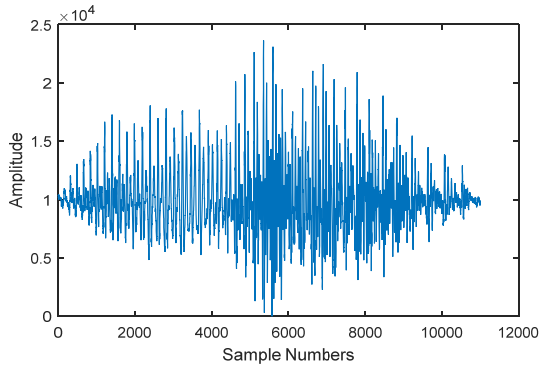

Figure-6. Stego signal plot in Matlab.

From the above figures, we can see that there is no such difference between the original audio file and the stego signal. It's very hard to detect the visual difference between these two signals.

Figure-7 below depicts the resemblance of host and the stego message. These blue and red lines are identical which shows the accurate implementation of our proposed technique. Figure-7(a) shows the small portion of the stego signal in close view. While Figure-7(b) represent the resemblance of full audio files.

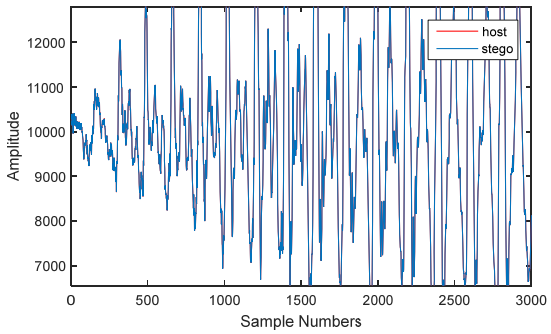

Figure-7(a). Close view of the audio and stego signal resemblance.

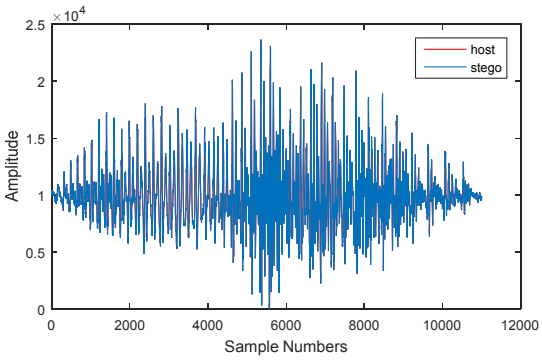

Figure-7(b). Audio and stego signal resemblance.

Both, Figures 7(a) and 7(b) indicate that audio and stego signals are almost same. The resemblance of both signals indicates that our technique provides a significant transparency. Hiding the data in higher bits of audio signal makes it difficult to trace. Similarly, this technique also increases the capacity of hiding the secrete data in by placing it in both higher and lower bits cover file.

Figure-8 below shows the spectral variance of the host and the stego signal.

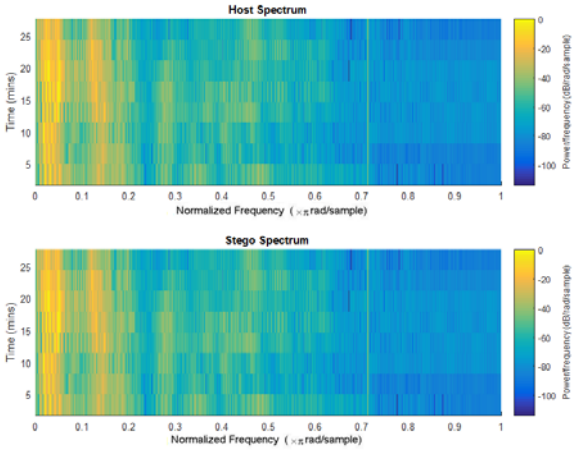

Figure-8. Host and stego signals spectrum.

The proposed technique achieved the same spectral behavior for the both signals. This is due to the sound level selection of masked frequencies. Generally in steganography, the set of masked frequencies are selected on the basis of sound pressure level. In this technique, two masked frequencies are selected below the hearing threshold; thus it provided the same spectral behavior and reduces the influence of the adding bits.

CONCLUSIONS

From this research it can be concluded that the given technique is cable of successfully hiding the more data in the random bits of audio signal to the previous techniques. This technique can hide the data in the lower and as well as per significant of the audio data. Thus, it

increases the capacity and transparency of the stego signal. Hiding of data in higher bit makes it difficult to trace the secrete data without key. It believes that this technique will enhance the security of the transmitted data. In future, cryptographic methods can be added with the proposed audio based steganography technique to enhance it for further security.

ACKNOWLEDGEMENT

We express gratitude to and acknowledge the PacDV free sound effects, for publically making available the dataset at http://www.pacdv.com/ sounds/voices-1.html.

REFERENCES

Al-Shatnawi A. M. 2012. A new method in image steganography with improved image quality. Applied Mathematical Sciences. 6(79): 3907-3915.

Asad M., Gilani J. and Khalid A. 2011. An enhanced least significant bit modification technique for audio steganography. 1st International Conference on Computer Networks and Information Technology (ICCNIT). pp. 143-147.

Bailey K. and Curran K. 2006. An evaluation of image based steganography methods. Multimedia Tools and Applications. 30(1): 55-88.

Cvejic N. and Seppanen T. 2002. Increasing the capacity of LSB-based audio steganography. 2002 IEEE Workshop on Multimedia Signal Processing. pp. 336-338.

Dasgupta K., Mandal J. and Dutta P. 2012. Hash based least significant bit technique for video steganography (HLSB). International Journal of Security, Privacy and Trust Management (IJSPTM). 1(2): 1-11.

Djebbar F., Ayad B., Meraim K. A. and Hamam H. 2012. Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing. 2012(1): 1-16.

Gopalan K. 2003. Audio steganography using bit modification. In IEEE International Conference on Multimedia and Expo, 2003 (ICME'03). pp. 629-632.

Huffman D. A. 1952. A method for the construction of minimum-redundancy codes. Proceedings of the IRE. 40(9): 1098-1101.

Katzenbeisser S. and Petitcolas F. 2000. Information hiding techniques for steganography and digital watermarking: Artech house.

Shirali-Shahreza M. H. and Shirali-Shahreza M. 2006. A new approach to Persian/Arabic text steganography. 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06).

Singh P. 2016. A Comparative Study of Audio Steganography Techniques. International Research Journal of Engineering and Technology (IRJET). 3(4).

Wang H. and Wang S. 2004. Cyber warfare: steganography vs. steganalysis. Communications of the ACM. 47(10): 76-82.

Yadav P., Mishra N. and Sharma S. 2013. A secure video steganography with encryption based on LSB technique. 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).