AUDIO STEGANOGRAPHY TECHNIQUE USING CIRCULAR BIT REPLACEMENT

Sushma Bahuguna
Banarsidas Chandiwala Institute of Information Technology, Affiliated to GGSIP University, Delhi, India

ABSTRACT

Audio steganography is one of the important methods to transit hidden information by modifying an audio signal in an imperceptible manner. In audio steganography, determining the best possible position for embedding the secret message with minimum alteration of the cover audio remains a challenging issue. In this technique we hide secret text or audio information in a host message such that no one except the intended receiver is aware of its existence and prevents unauthorised access. Various techniques have been used for embedding information in digital audio. Least significant bit (LSB) technique is most commonly used technique for secure data transfer. This paper presents replacement of bits of samples to hide a sequence of bits of secret text. The bits of samples are selected in a circular manner from LSB to MSB or vice versa. The results reveal satisfactory performance of the system and may be used for secure movement of data.

Keywords: Audio Steganography, LSB, MSB, SteganoAudio.

Cite this Article: Sushma Bahuguna, Audio Steganography Technique Using Circular Bit Replacement, International Journal of Computer Engineering and Technology, 10(4), 2019, pp. 17-24.

http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=10&IType=4

1. INTRODUCTION

The information security is one of the major challenges in data communication. Data communication over internet is very insecure due to attacks made on data transfer and information sharing. The two kinds of attacks i.e. intentional and unintentional may affect stegan-cover [1]. Intentional attacks try to extract hidden information while unintentional attacks try to modify or destroy the stegan-cover. Transformation of digital data over the internet has forced researchers to enhance security system. Steganography is science of concealing confidential data in a cover file like image, audio or text so that no one other than sender and intended receiver is able to notice that secret data is hidden inside [2].

Audio steganography science uses the audio-file as a cover file. This methodology is not simple as Human Auditory System which senses the variation of audio file over a range of
power greater than one billion to one and range of frequencies greater than one thousand to one. However, it has holes and a large dynamic range can contribute to data hiding [3]. Audio file being larger is size, high level of redundancy and high data transmission rate make it more suitable as host file [4]. Many steganography techniques have been proposed using different digital files. Earliest and simplest method used to hide secret information in audio samples is Least Significant Bit. Due to low robustness and easy to recover, researchers have proposed algorithms to enhance the LSB techniques to overcome these demerits [5]. [6] suggested Parity and XOR methods for hiding secret data in host file. [7] proposed method based on diffusing the secret method over host audio in which selection position of secret bit from 0th to 7th LSB depends on the decimal value of 3 MSB’s. Hiding data in duel bits in the 4th and 1st LSB and modifying other bits has been suggested by [8] for more secure communication. [9] proposed 3rd and 4th bits for embedding the secret text and intelligent algorithms for altering 2nd and 5th bits for perceptual resemblance between cover file and stego file. [10] used advanced encryption standard to enhance the security of stego-file. [11] and [12] proposed genetic algorithms to overcome the substitution problem of LSB substitution. [13] and [14] have used multi-level steganography system for more secure data transmission. [15] used nth bit replacement technique for secure data transmission. In this paper a modified technique of bit replacement is proposed, in which the bit to be replaced will not be a fixed bit position of the samples but will be incremented or decremented in circular manner.

2. ELEMENTS REQUIRED FOR AUDIO STEGANOGRAPHY

Steganography means masking a wedge of information inside another [16]. Following elements are required in order to hide information within an audio file.

- The cover audio (Ca)
- The secret message (Sm)
- The Stegano function (Fs) and its inverse (Fs-1)
- A Stego-key (K) or password that could be used to cover and show the information to and from stego-audio (Sa)

2.1. The block diagram in figure 1 depicts the stegano-operations

![Figure 1 Audio Steganography Process](http://www.iaeme.com/IJCET/index.asp)

Now-a-days people prefer a system that hides the existence of message secret. The technique, Steganography highlights the model of security through oblivion. The standard LSB technique is very easy to implement where the Least Significant bit of samples of cover media is replaced with target bit [6]. The method can preserve imperceptibility but has a drawback of low robustness and capacity. The robustness of the LSB Substitution technique may increase by embedding data at higher LSB layer or through embedding at random positions of the cover audio, which also introduces a double layer security. Figure 2 (a) and 2(b) is the flow chart of the proposed method of audio steganography.
Audio Steganography Technique Using Circular Bit Replacement

Figure 2(a) Flow Chart of generating secret message from StegoAudio.

Figure 2(b) Flow Chart for Generating SteganoAudio using Circular Bit Replacement Algorithm.
3. SYSTEM IMPLEMENTATION

Sound waves are analyzed on the basis of pitch, duration, loudness, timbre, sonic texture and spatial location. Duration of sound is a total time of onset and offset signals created by nerve responses to sound. When a new sound is noticed, a sound onset message is sent to the auditory cortex. When the repeating pattern is missed, a sound offset message is sent. Sound waves create low- and high-pressure areas called compressions and refractions. The highest points are called peaks and lowest points are called troughs. The peaks & troughs and areas of compression & refractions and combination of these samples may be used for audio steganography. This paper proposes the bit modification of the onset message of the sound. The offset part of message is not manipulated or modified. We have not used LSB or any fixed higher bit for audio steganography. It is based on dynamic selection of bit by user and replacing the bits of samples in circular order as stated in Figure 3.1 and 3.2.

![Circular Bit Replacement Technique](image)

**Figure 3** Proposed Circular Bit Replacement Technique 3.1 & 3.2

Pseudo-code of Circular bit replacement:

1. Read Cover audio
2. Input secret text (stego text)
3. Accept the initial bit index position from the user ranging from 1-7.
4. Fetch the first onset sample of cover audio.
5. If bit_index < 1 or bit_index >7 set bit_index to 1
6. Replace the bit index position of the current onset sample of cover audio with the current secret text bit.
7. Fetch the next onset sample of the cover audio.
8. If end of cover audio is reached then exit
9. Increment the bit_index by 1. Go to step 5
4. EXPERIMENTAL RESULTS
In audio steganography, determining the optimum location for embedding the secret message precisely with minimum distortion of the host medium still remains a challenging issue. In this paper we have selected samples from area of compressions and refractions of the onset signal as shown in Figure 4. The bit index of first sample to be replaced is dynamically selected and the index of next bit is calculated by incrementing the index bit. The experiment shows that the secret message is embedded with minimum distortion of the cover audio generating the stego-audio. Table 1 shows that only 38% of total bit length of the samples were replaced in the cover audio and rest of the bits were the same as of the cover audio, which lead to a minimum change in stegano audio.

Table 1 Secret text embedded in cover audio. 27 audio samples changed out of 70 samples in stegano audio.

| Sample Matched i.e. Sample bits not replaced | Sample Replaced i.e. Sample bits replaced |
|---------------------------------------------|-------------------------------------------|
| 43                                          | 27                                        |
| 139 140 143 145 146 147 148 150 151 153 155 156 158 159 161 162 166 167 168 169 171 173 174 175 176 183 184 187 189 190 191 193 195 197 198 200 201 202 203 204 205 206 207 | 138 141 142 144 149 152 154 157 160 163 164 165 170 172 177 178 179 180 181 182 185 186 188 192 194 196 199 |

On the input audio onset sample, bit modification is performed and a new audio is generated which is the SteganoAudio containing the hidden message. Figure 4 shows the original audio and stegano audio. We then compute MSE, PSNR and total number of bit of the secret message that modify the host audio.

**Figure 4:** Stego-audio and Original-audio samples
The PSNR is most commonly used as a measure of quality of reconstruction of lossy signals. A higher PSNR would indicate that the reconstruction is of higher quality. When two audios are equal, the MSE is zero and the PSNR is undefined. There is an inverse relationship between PSNR and MSE. So a lower MSE will lead to a higher PSNR value that indicates the signal has least effect of the modification. When PSNR is 40dB and greater, the difference of original audio and Stegano Audio is indistinguishable by human ear. MSE mean square error is the mean of the square of the difference between original and Stegano Audio. PSNR and MSE are defined in the following equations.

\[ MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - K(i,j))^2 \]

The PSNR (in dB) is defined as

\[ PSNR = 20 \cdot \log_{10}(MAX_i) - 10 \cdot \log_{10}(MSE) \]

Where

- MSE: Mean Square Error
- PSNR: Peak Signal to Noise Ratio
- MAX: Maximum sample value (In this case 7 bits per sample – 127)

Figure 5.1 shows the waveform of cover audio and the SteganoAudio, embedding the message at the 1st bit of the sample in the first onset sample. The figure shows that the percent replacement of bits is 46.93% and the values of MSE and PSNR conveys that the modified samples have a negligible impact on the audio quality. Figure 5.2 shows SteganoAudio and the extracted message form the stegano audio. The three most important parameters for audio steganography are imperceptibility (indicated as PSNR), payload (bit rate or capacity) and robustness. Any technique which tries to improve the payload or robustness should preserve imperceptibility. The noise which is introduced due to bit modification would limit payload [7]. The secret message of suitable size i.e. less than the length of the onset samples of the cover hosts audio is selected [8]. As shown in table 2 a sample message text of bit length 1225 is selected to be embedded in the cover audio. The results reveal that on an average the samples modified are around 50% of the total onset samples of cover audio i.e. if bit-length is of 1225 the effect will only be on (1225/2) bits of the host audio samples to produce SteganoAudio. The lower the replacement, the better will be the quality of SteganoAudio.

\[ \text{Figure 5.1 Embedding secret message in cover audio} \]
Audio Steganography Technique Using Circular Bit Replacement

5. CONCLUSION
The method begins with the solution to the low robustness issue in standard LSB technique by using the higher bit layer for embedding data in the cover audio. This technique becomes more robust by considering bit-planes randomly in circular manner for embedding target data and secrecy and imperceptibility is also maintained. The performance of the system remains the same for any of the start index bit selected and system may be used for secure movement of data.

REFERENCES
[1] Al-Othmani, A.Z., A.A. Manaf and A.M. Zeki, 2012. A survey on steganography techniques in real time audio signals and evaluation. Int. J. Comput. Sci., 9(1).
[2] Antony, J., C. Sobin and A. Sherly, 2012. Audio steganography in wavelet domain-a survey. Int. J. Comput. Appl., 52: 33-37.
[3] Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35(3,4): 313-336.
[4] Nosrati, M., R. Karimi and M. Hariri, 2012. Audio steganography: A survey on recent approaches. World Appl. Programm., 2(3): 202-205.
Ahmed Hussain Ali, Zohd Rosmadi Mokhtar and Loay Edwar George, 2016. A Review on Audio Steganography Techniques, Research Journal of Applied Sciences, Engineering and Technology 12(2): 154-162.

Kekre, H., A. Athawale, S. Rao and U. Athawale, 2010. Information hiding in audio signals. Int. J. Comput. Appl., 7(9): 14-19.

Pathak, P., A.K. Chattopadhyay and A. Nag, 2014. A new audio steganography scheme based on location selection with enhanced security. Proceeding of the 1st International Conference on Automation, Control, Energy and Systems (ACES, 2014).

Rahim, L.B.A., S. Bhattacharjee and I.B. Aziz, 2014. An audio steganography technique to maximize data hiding capacity along with least modification of host. Proceeding of the 1st International Conference on Advanced Data and Information Engineering (DaEng-2013).

Tanwar, R., B. Sharma and S. Malhotra, 2014. A robust substitution technique to implement audio steganography. Proceeding of the International Conference on Optimization, Reliability, and Information Technology (ICROIT, 2014), pp: 290-293.

Khan, M.S., M.V. Bhaskar and M.S. Nagaraju, 2011. An optimized method for concealing data using audio steganography. Int. J. Comput. Appl., 33(4): 25-30, (0975-8887).

Bhowal, K., D. Bhattacharyya, A.J. Pal and T.H. Kim, 2013. A GA based audio steganography with enhanced security. Telecommun. Syst., 52(4): 2197-2204.

Santhi, V. and L. Govindaraju, 2014. Stego-audio Using Genetic Algorithm Approach. Res. J. Appl. Sci. Eng. Technol., 7(22): 4806-4812.

Bandyopadhyay, S.K. and B.G. Banik, 2012. Multilevel steganographic algorithm for audio steganography using LSB modification and parity encoding technique. Int. J. Emerg. Trends Technol. Comput. Sci. (IJECTCS), 1(2).

Kaur, K. and D. Verma, 2014. Multi-level steganographic algorithm for audio steganography using LSB, parity coding and phase coding technique. Int. J. Adv. Res. Comput. Sci. Software Eng., 4(1).

Bahuguna, Sushma, 2018, Evaluation of Nth Bit replacement in Audio Steganography,International Journal of Computer Engineering & Technology (IJCET) Volume 9, Issue 4, July-August 2018,pp. 159-165.

Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom and Salwani Mohd Davd, 2011, A Survey on Image Steganography Algorithms and Evaluation, Digital Information Processing and Communications, ICDIPC 2011, pp. 406.