www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-7, Issue-2, Apr 2019
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Analysis of Various Techniques for Audio Steganography in Data Security

Manisha Verma[1], Hardeep Singh Saini[2*]

[1]Research Scholar, Indo Global College of Engineering, Abhipur, Mohali, Punjab, India
[2*]Professor, Indo Global College of Engineering, Abhipur, Mohali, Punjab, India

[*]*Corresponding Author: hardeep_saini17@yahoo.co.in, Tel.: +91-9988016668*

Received: 27/Mar/2019, Accepted: 22/Apr/2019, Published: 30/Apr/2019

***Abstract*—**In today's digital world one is concerned with the secrecy of data and focused on copyright-dependent individuals and organizations, specifically in the domain of the entertainment industry. The variations in the human voice lead to the difficulties to generate the watermark to the audio signals in order to preserve them from unauthenticated access. The major objective of the steganography process is to enhance the security of the transmitted data. The unauthorized user can not access or misuse the steganographic file. Audio steganography is also applicable to the non-technical fields in order to keep the privacy and security of the data. This paper presents a review of recent research on audio steganography. The major focus of the study is to address various types of audio steganographic techniques along with their pros and cons. There is a need to find technique so that the data hiding is done more securely and it is not possible for the third parties to detect the data in bits.

***Keywords*—** Audio Steganography, Bit, LSB, Security, Watermarking

I. INTRODUCTION

Data hiding, in order to secure the data from malicious activities, is the part of the information security. "Steganography" is a concept to hide the data in a cover file with the objective to preserve the confidential data from the third party. The steganography can be defined as an art or science as well that secure the data by hiding confidential data to a cover file. The hidden data can only be visible to the sender and the receiver of the message. The hidden information is encrypted by using encryption mechanisms no-one can even find that there is hidden information behind the cover file [1], [2], [3]. Along with the data encryption techniques, data compression techniques can also be applied to the data. The data compression techniques are used to compress the data so that a large amount of data can also be encrypted and embedded upon the cover file. The application of data compression techniques along with the data encryption techniques ensures the highest security level of the information. Due to fewer storage requirements, one could not even know that the data is present there [4], [5].

The sound files carrying the information are represented in the form of .wav, .au, and even .mp3 files. In the process of audio steganography system, the properties of the human auditory system are utilized. The evaluation of audio system is done on the basis of the critical band analysis that exists in the inner part of the ear. In critical band frequency to location, transformation happens beside the basilar membrane. The received sound power spectra represented on limited frequency bands called critical bands [6]. The generalized model for audio steganography comprised of a message, a password and a carrier file [7]. The carrier file can be defined as the cover file also. The cover file is used to hide the data that is confidential to the user and the receiver of the data. The message is the information that is going to embed behind the cover file. It can be text, audio, video or image, etc. The password is described as a stego-key that is utilized for embedding and extracting the data from the cover file. It is mandatory that the sender and the receiver of the data must be aware of the stego-key so that data can be accessed by both of them. The cover file that is obtained after embedding the message on it with the help of stego-key is known as a steganographic file [5]. The block diagram of basic audio stenography is shown in Fig.1.

This paper gives a review of various audio steganographic techniques. The audio steganographic methods and applications are given in section 2 and in its sub-sections. In section 3, simplest data compression technique i.e. Run-length encoding (RLE) is presented. Section 4 is dedicated to the Literature review. Section 5 is added for further discussion on problem formulation. Finally, the conclusion is presented at the end of this paper.

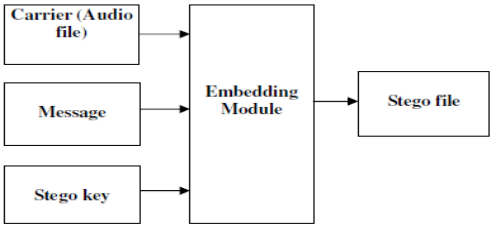

Figure 1. The basic audio stenography model

II. AUDIO STEGANOGRAPHIC METHODS AND APPLICATIONS

A. Audio Steganographic Methods

The watermarking of audio signals is a challenge because we have to concentrate on some parameters very effectively such as the quality of signal should not reduce embedding messages in the form of a watermark on it. The power range for sound should be greater than 109:1 & the range of frequencies for it should be greater than 103:1, signal to noise ratio should be greater than 20 dB. The sensitivity of the human audio system to the AWGN noise, i.e. additive white Gaussian noise should be as low as 70 dB below ambient level so that noise level should be low and the quality of audio signal remains good in strength. There is a large variety of techniques available that can be used for hiding the information behind an audio cover file without affecting its signal quality. These techniques enable the sender to hide the data so efficiently that the alterations performed on the audio file are indiscernible and it is not detectable by the third party [6], [8]. The categorization of audio steganographic techniques can be done on the basis of different domains such as time-based domain, frequency-based domain, transformation-based domain, etc. These domains have further sub-categories like transform domain which is further divided to the wavelet and frequency domain and its major relative techniques are defined as follows:

(a) LSB Coding

It is the most ancient method of hiding audio information which is called least significant bit (LSB) algorithm. In this technique the user can convert the image into audio and audio into the image by replacing the least significant bits in the cover file in order to embed a sequence of bytes [3]. This is performed to upsurge safety by reshuffling the information message before hiding it to the audio document. This is done to secure the data from the attacker. In case the attacker comes to know about the hidden data, then he will not be capable to crack the originality of data as it is in the coded format. This happens because of the shuffling of the message that is performed by the dynamic generation of the random sequence. The random sequence generation relies upon the criteria of file selection for hiding the data. That is normally a successful procedure in situations where the LSB substitution doesn't cause quality degradation as there is a high channel bit rate. In terms of computing, the LSB can be defined as the bit position in a binary integer with respect to the available unit value which evaluates whether the number is odd or even. Therefore, its complexity is lower and consumes less time and less delay for data hiding and extracting. The ideal data transmission rate is 1 kbps per 1 kHz in LSB coding. Two least significant bits of a sample are replaced with two message bits [9]. This technique is also called as the right-most bit, due to the convention of positional notation of writing a less significant digit further to the right. This technique is easy to detect so; it is preferred to use it with the XORing method which increases the security of data.

(b)Parity coding

Parity coding is a robust audio steganographic technique [10]. It doesn't break the signal into single samples; instead of it, in this method, a signal is broken into different samples and every bit of the secret message from a parity bit is embedded [10]. Suppose, if somebody wants to decode the signal and parity bit of a selected region does not match the secret bit to be encoded, then the inversion of the LSB of one of the samples will be done and there will be one more choice of encoding the secret bits information, it will not be encoded easily in another way. The main disadvantage is that they are not strong and suppose if the information is re-sampled some of the data may be lost.

(c)Phase coding

This is also an efficient technique of watermarking. First, we convert the message into blocks and then embed in to phase, further, the user replaces the phase of an initial audio signal with a reference phase containing hidden data. The relative phase among various segments is adjusted and arranged by using the remaining phase [8]. This coding mechanism is considered as an effective and prominent once with respect to the signal to noise ratio (SNR). This technique suffers from slight phase dispersion in the scenario when a huge variation takes place in the phase and frequency components. Though, as long as the variations of the phase are smaller, indistinct coding can be attained [10]. The major drawback of this mechanism is that it suffers from the issue of ineffective payload.

(d) Spread spectrum

Spread spectrum steganography provides secure communications to send the information in the frequency spectrum of audio systems. The methodology of the speed spectrum has been used in this technique which means that hidden data or secret data is spread over the wide frequency bandwidth. The main idea behind using this technique is that the SNR ratio in every frequency is very small, which means that noise in the signal is too high due to which it is unable for anyone to detect the presence of data. If some of the data parts are removed from several bands, but still enough information is present on other bands in order to recover the data. Thus, it is an advantage as without destroying the cover, complete data cannot recover. Consequently, it is a robust technique mostly used in military communication.

(e) Echo hiding

In the echo hiding technique, an echo is introduced in a sound file by changing the amplitude and putting the delay in the signal and at last, it is extracted to recover the original data. Here, if the echo is generated in the original signals,

then one bit of information could be hidden. This can be done by sending the two signals, one after the other with some delay, so that overlapping up to some extent will nullify the effect of two and this will express that delay during which transmitter will store the hidden message. Thus, the original signal or the input signal is firstly divided into the blocks before initializing the data encoding process. At the time of data encoding subdivides blocks are joined together in order to create the final single block [8]. The main advantage of the echo hiding technique is that it provides a high data transmission rate and maintains a strong strength of the signal so that it is robust in nature.

B. Audio Steganographic Applications

In today's world cheating, manipulating and copying of data is common and for these reasons we need to hide the data as it is helpful in providing confidential communication and secret data storing from unauthorized persons. Moreover we can safeguard our data from outside threats and alteration in addition to this access to control the system for the personal use in the media can be curbed. Audio steganography is also applicable to the non-technical fields in order to keep the privacy and security of the data. The example of such applications is that the terrorists are also using the audio steganography in order to encrypt their communication [11]. Information hiding by using the audio or video cover file is majorly done by the entertainment world to protect the copyright of the digital media files. It is also used by the government in order to copyright legal documents. Its other application fields are medical science and research domain.

III. RUN-LENGTH ENCODING

Run-length encoding (RLE) comprises of the runs of data which are sequences with similar data value occurring in several subsequent data elements, and it is one of the simplest data compression techniques. Data values are saved as a single digit instead of the original one. It is quite beneficial for data comprised of multiple such runs. Most of the formats of bitmap files such as .tiff, .bmp, .pcx and .rle are supported by this technique. The compression ratio is affected by the content of the data achieved by RLE. The operation of RLE decrements the physical size of a repeating string of characters referred to as run typically encoding into two bytes. The numbers of characters in the run called the run count are represented in the first byte. The encoded run generally comprised of 1-128 or 256 characters, the run count generally comprised of a character less than the characters of encoded run i.e. 127-255. Also, the second byte called the run value with a range of 0 to 255 is the value of the character in the run.

Advantages and disadvantages

This procedure is very simple to apply and not necessitates much CPU horse-power. RLE compression is only effective with files that cover a lot of repetitive data. These can be text files if they contain lots of spaces for indenting but line-art images that contain large white or black areas are far more suitable. Computer generated color images (e.g., architectural drawings) can also give fair compression ratios. RLE compression can be used in the TIFF and PDF files.

IV. LITERATURE REVIEW

The study presents the analysis over various techniques for audio steganography such as genetic algorithm and LSB mechanism [12]. In the process of steganography, the message is used to embed on the cover file and the hidden message is known as the host message or cover message. When the cover message is modified then the resultant message is known as stego-message. In simple words, it can be said that the combination of stego message and cover message results to the stego message. In the case of audio steganography, the message and cover file both are in audio formats. Due to the replication, the cover audio message before the process of steganography and the stego message after the process of steganography remains similar. Various kinds of audio steganography techniques are presented with their pros and cons in [13]. Information hiding is the basic step that is taken to secure the privacy of the data over the communication medium. Steganography is another form of data hiding. Among all of the steganography techniques, the LSB and phase encoding are prominent techniques [14].

A. Binny and M. Koilakuntla [15] presented an audio steganography technique by using the LSB technique. This technique hides the text data in an audio cover file. In this work, the audio signals were first converted to the bits and then the textual message was embedded. While embedding, the text is converted to the binary format. With the help of developed mechanisms, it has been seen that the data hiding capacity had been increased. After implementation, the performance evaluation was done in terms of SNR. K. Kaur and D. Verma [16] had proposed a multi-level steganography algorithm by implementing three of the most prominent techniques i.e. LSB, parity coding and phase coding. This technique had the advantage that it is difficult to decode the message by an unauthorized person. The study had also represented a review of the three-layered audio steganography approach for multi-level steganography. The study was found to be effective to attain higher security.

Another technique "Enhancement in the security of LSB based audio steganography using multiple files" was about the enhancement of the data security by utilizing the LSB method to hide the message into more than one audio file [17]. On the basis of the results, it was observed that the message hidden by this technique is less vulnerable to the third party. This level of security was attained due to the defined reasons:

First, more than one file was considered to hide a large amount of data and thus it leads to the enhancement in the data hiding capacity. The second reason is that initially the message was divided into subparts and then the divided parts were shuffled randomly on the basis of generated permutation. S. Divya and M. R. M. Reddy [18] had developed a substitution mechanism for audio based steganography with the objective to enhance the capacity of cover audio for embedding the additional data on it. The LSB data embedding technique was used up to 7 LSBs to hide the data. The implementation analysis was done for multiple lengths and variable length LSBs. On the basis of the obtained results, it was concluded that the data hiding capacity of the proposed work was 35% to 70% higher than the standard LSB algorithm.

A. Nagarajan and K.Alagarsamy [19], gave a novel idea for audio steganography by utilizing the enhanced run length encoding algorithm. The author had focused to overcome the backlogs of run-length encoding scheme with the perspective of data compression. The major steps of the technique were to apply the ERLE encoding to the byte level, layer partition, to assign alpha index value, to organize the separated layer the link list data structure was used, data storage and decoding. S. Joseph et al [20] invented an approach named modified RLE to provide high-speed data compression. The study had also discussed the generalized concept of compression and its features. The author had suggested that the respective compression mechanism is suitable for the application where the data redundancy is higher. In previous researches in this domain, the compression rate was lower. Thus in present work, the author had used the FIFO concept to store the input and output sequences. As per the obtained results, the compression rate of the technique was increased and the memory requirement was decreased than standard RLE approaches.

A. Ramachandran and A. K. Rajamohan [21] generated a new indexing method known Binary search tree indexing. Along with this, the RLE was also applied. The author had proved that the data compression of the embedded text can be achieved without affecting the other aspects such as insertion, update, and deletion of the content. As in the BST tree, the indices are used to access the stored values, thus in this work, the author had applied the concept of linked lists for developing the database of respective indices. As per the simulation results, it was observed that the technique provided a good level of data compression.

V. PROBLEM FORMULATION

Data security is a major concern, as a large amount of data travels over the internet in order to reach its destination. Securing the data is mandatory in order to make it secure from malicious activities and unauthentic users. To implement the data security the major task for securing the data transmission between two parties. Steganography is used for data hiding, it prevents from the outer threats and hacking of the audible message in so efficient manner that the attacker cannot even come to know about the existence of any information. The embedment of textual data to the digital signals is known as the concept of audio steganography. The process of audio steganography is a little different and difficult from other kinds of steganographic techniques since in it the data is embedded over the digital signals. There are a lot of audio steganographic techniques available. LSB is the most preferred and prominent method. The working criteria of LSB are to replace the least significant bits to the bytes of the available cover file [1], [17]. Though it was an efficient technique the problem was that it does not provide security that is required. The data can be easily detected by the third party if the LSB bits are known. It does not provide the security which is needed. So there is a need to find the method so that data hiding is efficient. A technique is to be introduced so that the data hiding is done more securely and it is not possible for the third parties to detect the data in bits. The new approach is to be made to resolve this problem.

VI. CONCLUSION

The main problem is of data security when data hiding is performed. The data is hidden on LSB of the bits, but this method is not that much efficient as the bits are identified the data will no longer remain safe. The hide the textual data behind an audio file is known as audio steganography. This is a tedious steganographic approach in comparison to other steganographic approaches such as image steganography, video steganography, etc. As LSB coding is an efficient method, but it's not that secure. So to provide security to data a technique is introduced in which before hiding the data, encoding of data is done. Encryption is the process of encoding signals so that a third party should not intervene in the data. After studying many approaches and taking them in consideration it is concluded that a technique is to be introduced so that the data hiding is done more securely and it is not possible for the third party to detect the data in bits.

REFERENCE

[1] N. Gupta, N. Sharma, "*Hiding Image in Audio Using DWT and LSB*", International Journal of Computer Applications, Vol.81, No.2, pp. 11-14, 2013.

[2] R. Kaur, J. Bhatia, H.S. Saini, R. Kumar, "*Multilevel Technique to Improve PSNR and MSE in Audio Steganography*", International Journal of Computer Applications. Vol.103. pp.1-4, 2014.
10.5120/18067-9008

[3] R. Kaur, A. Thakur, H.S. Saini, R. Kumar, "*Enhanced Steganographic Method Preserving Base Quality of Information Using LSB, Parity and Spread Spectrum Technique"*, 2015 Fifth International Conference on Advanced Computing & Communication Technologies IEEE, pp.148 – 152, ISBN:978-1-4799-8487-9, 2015. DOI: 10.1109/ACCT.2015.139

[4] M. Nosrati, R. Karimi, M. Hariri, "*Audio Steganography: A Survey on Recent Approaches*", World Applied Programming, Vol.2, No.3, pp.202-205, 2012.

[5] Sheelu, "*Enhancement of Data Hiding Capacity in Audio Steganography"*, IOSR Journal of Computer Engineering (IOSR-JCE), Vol.13, No.3, pp.30-35, 2013.

[6] N. Cvejic, T. Seppanen, " *Digital Audio Watermarking Technique and Technologies: Applications and Benchmarks*", Book 2007. doi: 10.4018/978-1-59904-513-9

[7] F. E. M. Al-Obaid, A.J.M. Ali, "*Which Bit is Better in the least Significant Bit*", Journal of information security (Scientific research publishing), Vol.6, No.3, pp.161-165, 2015. doi: 10.4236/jis.2015.63017

[8] A. Singh, " *Self Study Seminar Report Steganography*", Department of Computer Technology, Delhi Technological University, Delhi

[9] C. R. Nagrecha, P. B. Swadas, "*Audio Steganography with Various Compression Algorithms to Improve Robustness and Capacity*", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 4, Issue 5, 243-247, 2014.

[10] T.H. Hiralal, N. Gopal, V.V. Sasikumar, *"Audio Steganographic Approaches: A Review",* International Journal of Engineering and Innovative Technology (IJEIT), Vol. 4, Issue 11, pp.199-203, 2015

[11] P. Dutta, D. Bhattacharyya, T. H. Kim, "*Data Hiding in Audio Signal: A Review*", International Journal of Database Theory and Applications, Vol.2, No.2, 2009.

[12] G. Nehru, P. Dhar, "*A Detailed Look of Audio Steganography Techniques Using LSB and Genetic Algorithm Approach*", IJCSI International Journal of Computer Science Issues, Vol.9, No.2, pp. 402-406, 2012.

[13] P. Jayaram, H. R. Ranganatha, H.S. Anupama, *"Information Hiding Using Audio Steganography –A Survey",* International Journal of Multimedia & Its Application, Vol.3, No.3, pp.86-96, 2011.

[14] S. Kumar, "*LSB Modification and phase encoding technique of audio steganography revisited*", International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, No.4, pp.1-4, 2012.

[15] A.Binny, M. Koilakuntla, "*Hiding secret information using LSB based audio steganography",* IEEE International Conference on Soft Computing & Machine Intelligence, pp.56-59, 2014. doi: 10.1109/ISCMI.2014.24

[16] K. Kaur, D. Verma, "*Multi-Level steganographic algorithm for audio steganography using LSB, parity coding and phase coding technique*", International Journal of Advanced Research In Computer Science and Software Engineering, Vol.4, No.1, 2014.

[17] P. Chandrakar, M. Choudhary, C. Badgaiyan, *"Enhancement in the security of LSB based audio steganography using multiple files",* International Journal of Computer Applications, Vol.73, No.7, pp.21-24, 2013.

[18] S. Divya, M. R. M. Reddy, "*Hiding text in audio using multiple LSB steganography and provide security using cryptography*", International Journal of Science and Technology Research, Vol.1, No.6, 2012.

[19] A. Nagarajan, K.Alagarsamy, "*An Enhanced Approach in Run Length Encoding Scheme (EARLE)",* International Journal of Engineering Trends and Technology, pp.43-48, 2011.

[20] S. Joseph , N. Srikanth , J. E. N. Abhilash, *"A Novel Approach of Modified Run Length Encoding Scheme for High Speed Data Communication Application*", International Journal of Science and Research (IJSR), Vol.2, No.12, 2013.

[21] A. Ramachandran, A. K. Rajamohan, "*Integrating Run Length Encoding and Column oriented database execution using Binary Search Tree*", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 9, 2013.

Authors Profile

Manisha Verma pursed Bachelor of Technology in Electronic & Communication Engineering from Haryana Engineering College, Jagadhri, Yamunanagar, Haryana (India) in 2006 and currently she is pursuing M.Tech from Indo Global College of Engineering, Abhipur, Mohali (Punjab).

Hardeep Singh Saini has a total experience of 20 years, presently working as Professor at Indo Global College of Engineering, Abhipur (New Chandigarh), PUNJAB (INDIA) since June-2007. He is author of 6 books in the field of Electronics & Communication Engineering. He has presented 74 papers in international/national conferences and published 57 papers in international journals *(SCI/SCOPUS/Peer-reviewed Journal)*. He is a fellow and senior member of various prestigious societies like IETE (India), IEEE, IETI China, SCIEI USA and he is also editorial member of various international journals and conferences.

