International Journal of Engineering & Scientific Research
Vol.10 Issue 12, Dec 2022
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

An Analytical Study of Various Methods for Audio Steganography in Data Security

Pankaj Nandan, Associate Professor
Department of Computer Science, GCW, Kathua, J&K
Rakhi Billawaria
Lecturer in Computer Science, GDC Reasi, J&K

Abstract

In the current era of digital world, particularly in the field of entertainment industry, and organizations, one is concerned with the secrecy of data. The discrepancies in the human voice lead to the difficulties to yield the watermark to the audio signals in order to protect them from unauthenticated access. The important purpose of the steganography process is to increase the security of the transmitted data. The unauthorized user cannot reach or misuse the steganographic file. Audio steganography is also relevant to the non-technical spheres 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 focus on different types of audio steganographic techniques along with their consequences i.e. both negative and positive. There is a necessity to unearth technique so that the data concealing is done more protectively and it is not possible for the third parties to identify the data in bits.

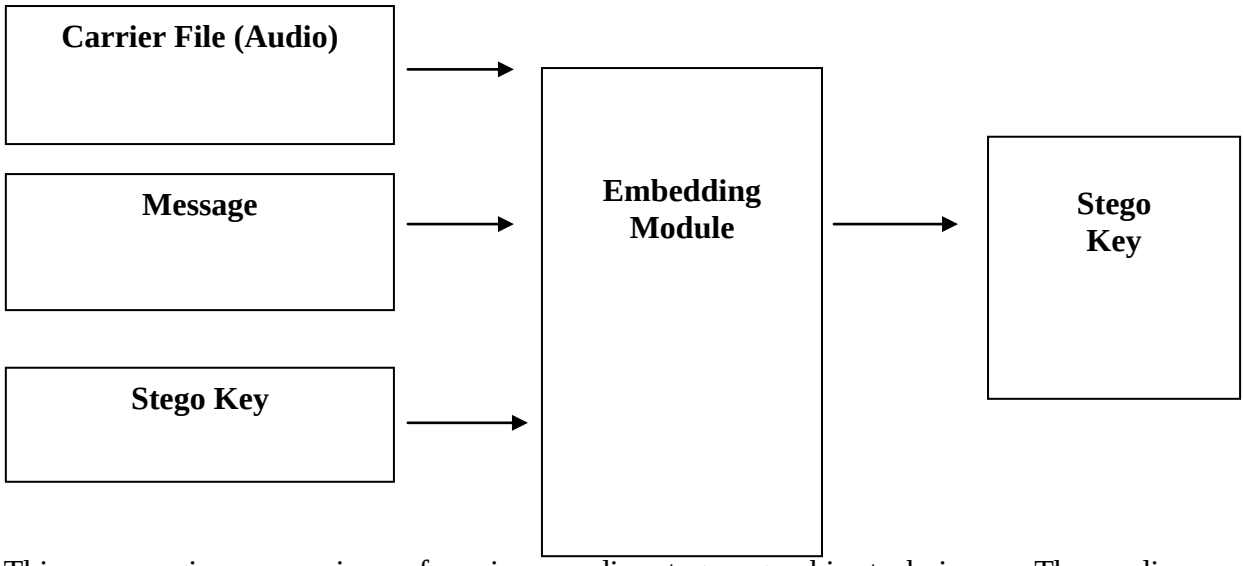
Keywords: Audio Steganography, Bit, LSB, Security, Watermarking.

Introduction

Hiding data, in order to protect the data from malevolent activities, is the part of the information security. "Steganography" is an idea to conceal the data in a cover file with the purpose of preserving the secret data from the third party intervention through illegal way. The steganography can be defined as an art or science as well that protect the data by hiding confidential data to a cover file. The concealed data can only be seen to the sender and the receiver of the message. The hidden information is encrypted by employing encryption methods 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 methods can also be applicable to the data. The data compression techniques are used to compress the data so that a large quantity of data can also be encrypted and inserted upon the cover file. The use of data compression techniques along with the data encryption methods ensures the highest security level of the information.

The sound files holding the information are depicted 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 used. The evaluation of audio system is done on the basis of the analysis of critical band that exists in the internal segment of the ear. In critical band frequency to location, conversion takes place beside the basilar membrane. The obtained sound power spectra depicted on limited frequency bands called critical bands [6]. The generalized model for audio steganography includes message, a password and a carrier file [7]. The carrier file can also consider as the cover file also. The cover file is employed to conceal the data that is important and secret to the user and the receiver of the data. The message is the information that is going to insert behind the cover file. It can be text, audio, video or image, etc. The password is defined as a stego-key that is used for inserting and collecting the data from the cover file. It is compulsory that the sender and the receiver of the data must be cautious of the stego-key so that data can be reached by both of them. The cover file that is received 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 given in fig.1.

Figure 1. The basic audio stenography model



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.

II. AUDIO STEGANOGRAPHIC METHODS AND APPLICATIONS

A. Techniques of Audio Steganography: The watermarking of audio signals is a tough challenge because we have to focus on some issues very significantly such as the quality of signal should not decrease inserting messages in the shape of a watermark on it. The power range for sound should be larger 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 methods available that can be applied to conceal the information behind an audio cover file without changing its signal quality. These methods allow the sender to hide the data so effectively that the changes performed on the audio file are unclear and it is not traceable by the third party [6], [8]. The classification of audio steganographic methods can be done on the basis of diverse domains such as time-based domain, frequencybased domain, transformation-based domain, etc. These domains have more sub-types like transform domain which is further divided to the wavelet and frequency domain and its major relative methods are defined as follows:

A. LSB Coding

It is the earliest method of hiding audio information which is called least significant bit (LSB) algorithm. In this method, the user can transform the image into audio and audio into the image by changing the least significant bits in the cover file just to insert an order of bytes [3]. This is performed to increase the security by reordering the information message before concealing it to the audio document. This is done to protect the data from the attacker. In case the attacker is aware about the hidden data, then he will not be able to decode the originality of data as it is in the coded format. This takes place because of the shuffling of the message that is performed by the dynamic production of the random order.

B. Parity coding

Parity coding is a vigorous audio steganographic method. It doesn't rupture the signal into single samples; inspite of this, in this method, a signal is broken into many samples and every bit of the secret message from a parity bit is inserted. For instance, if somebody wants to decipher the signal and parity bit of a chosen 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 option of programming the secret bits information, it will not be encoded easily in another way. The main drawback is that they are not strong and suppose if the information is resampled some of the data may be lost.

C. Phase coding

This is also an important technique of watermarking. First, we transform the message into blocks and after that insert in to phase, further, the user changes the phase of first audio

signal with a reference phase consisting hidden data. The relative period among different parts is adjusted and arranged by employing the remaining phase. This method of coding is considered as useful and prominent once with respect to the signal to noise ratio (SNR). This method suffers from slight phase dispersion in the setting 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 achieved. The major limitation of this technique is that it witnesses the issue of ineffective payload.

D. Spread spectrum

Spread spectrum steganography provides a safe communications to send the information in the frequency spectrum of audio systems. The speed spectrum methodology has been employed in this technique which means that concealed data or secret data is proliferated over the wide frequency bandwidth. The main idea behind employing this method is that the SNR ratio in every frequency is very meager, which means that noise in the signal is too high due to which it is unable for anyone to sense the presence of data. If some of the data parts are eliminated from several bands, but still enough information is present on other bands in order to recover the data. Thus, it is an important benefit as without obliterating the cover, complete data cannot recover. Consequently, it is a healthy way mostly used in military communication.

B. Audio Steganographic Applications

In today's world cheating, manipulating and copying of data is frequent and for these reasons we required to conceal the data as it is beneficial in providing secret communication and secret data storing from unauthorized persons. Moreover, our data can be protected from outside threats and deliberate transformation in addition to this access to control the system for the personal application in the media can be curbed. Audio steganography is also valid to the non-technical spheres in order to keep the privacy and security of the data. For instance, the terrorists are also employing the audio steganography in order to encrypt their communication. Information concealing by using the audio or video cover file is majorly done by the entertainment world to secure the copyright of the digital media files. It is also employed by the government in order to copyright legal documents. Its other application spheres are medical science and research fields.

III. RUN-LENGTH ENCODING

Run-length encoding consisting of the runs of data which are arranged with similar data value appearing in several subsequent data elements, and it is one of the easiest data compression techniques. Data values are protected as a single digit instead of the original

one. It is quite useful for data comprise of multiple such runs. Most of the structures of bitmap files such as .tiff, .bmp, .pcx and .rle are supported by this method. The compression ratio is affected by the content of the data achieved by RLE. The operation of RLE decrements the physical size of a reiterating string of characters referred to as run typically encoding into two bytes. The numbers of characters in the run called the run count are depicted in the first byte. The encoded run generally consisted 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.

CONCLUSION: The main issue discussed in this paper is data security when the data hiding process is performed. The data is hidden on LSB of the bits, but this technique is not that much effective as the bits are identified the data will no longer remain protected. The concealed 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.

References

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.

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

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

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

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

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

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.

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.