International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

A Review of an Extensive Survey on Audio Steganography Based on LSB Method

Hariom Dudhwal, Asst. Prof. Jayshree Boaddh
Dept. of Computer Science & Engineering
Mittal Institute of Technology Bhopal,
Madhya Pradesh, India
hariomdudhwal@gmail.com, jayshree.boaddh@gmail.com

Asst.Prof. Jashwant Samar
Dept. of Computer Science & Engineering
UIT-RGPV
Bhopal, Madhya Pradesh, India
jashwantsamar.samar2@gmail.com

Abstract- There is issues and challenges regarding the security of information in transit from senders to receivers. The major issue is the protection of digital data against any form of intrusion, penetration, and theft. The major challenge is developing a solution to protect information and ensure their security during transmission. In audio steganography, the cover is an audio and the secret information can be a text file, an image, or an audio. In this work, some audio steganography techniques are explored taking cover audio in WAV and MP3 format. WAV files produce integer samples and MP3 files give floating point numbers as samples. The secret information considered is the text file, the image, and the audio. The embedding and extracting algorithms of the different audio steganography techniques are discussed in this examination. This work presents a survey of literature on MP3 Steganography Based on Modified LSB Method.

Keywords- Steganography, MP3, Audio Steganography, LSB Method, LSB technique in MP3 steganography.

I. INTRODUCTION

The word steganography comes from the Greek Stegos, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. Secret information is encoded in a manner such that the very existence of the information is concealed.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the trans mission of a hidden data. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed.

In order for a data hiding technique to be successful it must adhere to two rules:

1. The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/ auditory system or in increased file size for the carrier file.
2. The embedded data must maintain its integrity within the carrier and should be easily removable, under the right circumstances, by the receiving party.

Steganography is a powerful tool which increases security in data transferring and archiving. Steganography is a technique of information hiding in which the existence of secret message is hiding. In this hide the existence of secret message by embedding it into cover media object. Embedding is a technique to fix firmly in surrounding mass, e.g. to embed nail into wood. Figure 1.1 shows that steganography secret message is called message object or media in which data is to be embedded called as cover object or output produced after steganography is called stego object. Cover object can be audio, video, text, and image. Data is embedded in cover object in such a way that quality of cover object is not affected.

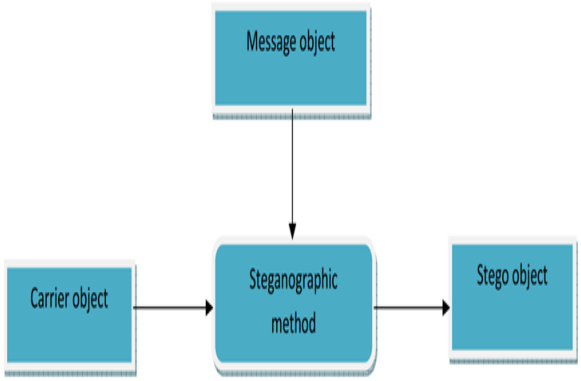

Fig 1. Block diagram of audio steganography.

The main goal of steganography is to hide a message m in some audio or video (cover) data d to obtain d', practically indistinguishable from d, so that the secret listener to this conversation cannot detect the presence of mind'.
Moreover, the modification of the carrier caused by inserting steganograms cannot be "visible" to the third party observer, i.e., he/she cannot point to the difference between modified and unmodified carrier if he/she is not

aware of the steganographic procedure. Generally, in steganography the following operations are performed.

In Audio Steganography, the weakness of the Human Auditory System (HAS) is used to hide information in the audio. That is, while using digital images as cover files the difficulty of the human eye to distinguish colors is taken advantage of, while using digital audio one can count on the different sensitivity of the human ear when it comes to sounds of low and high intensity; usually, higher sounds are perceived better than lower ones and it is thus easier to hide data among low sounds without the human ear noticing the alteration. In audio steganography data is embedded in digital audio signal. Here secret message is embedded by small change in binary sequence of sound file. Audio file can be WAV, AU, or MP3 sound files. Audio steganography is more difficult than other methods of steganography.

II. LSB METHOD

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, or it allow high embedding rate without degrading quality of audio file. Use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps.In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise.

On the other hand, the same noise would be audible in a sound file containing a piano solo. To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded; leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples.

Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would be attacker will suspect secret communication. This technique ensures that the same index is never generated more than once.

1. Advantages:
- It is easy to implement.
- It provides very high channel capacity.
- It is easy to combine with other hiding techniques.

2. Disadvantage:
- It has considerably low robustness against attacks.
- Perceptual transparency of stego objects is decreased

III. LITERATURE REVIEW

R. Indrayani, H. A. Nugroho and R. Hidayat, [1] Least significant bit (LSB) is one of the classical methods commonly used for steganography audio. Because of its simplicity, many researchers have interested to develop it. This investigation aims to determine the maximum limit of adding bits and its effects on audio quality based on modified LSB method consisting of LSB+1, LSB+2 and LSB+3. Then, this method is evaluated by counting steganography capacity, peak signal to noise ratio (PSNR) and bit error rate (BER) values. Evaluation results show that LSB+3 has the best performance by obtaining the maximum bit of steganography capacity and acceptable of PSNR value.

B. Datta, P. K. Pal and S. K. Bandyopadhyay,[2] LSB techniques generally embed data in the same LSB position of consecutive samples which helps intruders to extract secret information easily. This examination solves this problem by introducing a robust audio steganography technique where data is embedded in multiple layers of LSB chosen randomly and in non-consecutive samples.

The choice of random LSB layers and non-consecutive pixels for embedding increases robustness as well as the strength of proposed steganography algorithm. It is seriously a problem that the data hiding at non-contiguous sample locations loses the capacity of stego audio. This problem is solved here by embedding three bits within a target samples. The capacity is also increased by using 6 bits ASCII representation of secret message instead of 7. The proposed technique is tested by embedding text of different payloads within the cover audio and also compared with existing techniques based on quality and capacity.

M.T.Al-Bayati and M. M. Al-Jarrah,[3] Steganography, the technology of protecting a secret message by embedding it inside a cover image, continues to be

investigated and enhanced as an alternative data protection method. This examination work deals with hiding multimedia files in true color RGB cover images with an emphasis on reducing the cover size, increasing hiding capacity and enhancing security of the hidden data.

A proposed model (DuoHide) is presented in which a secret multimedia file, regardless of its type, is processed without un-compression, and divided between two cover images of equal size and dimensions. The multimedia file is read as a stream of bytes and split vertically into two parts, one part contains the least significant half-bytes, and the other part contains the most significant half-bytes. The two parts are hidden inside two uncompressed RGB cover images using a least significant 4-bit replacement technique. The resulting dual stego images are expected to be sent separately, through different channels, to avoid capture of both stego files by an adversary. Extraction of the secret file is achieved through merging LSB half-bytes from the two stego files. The extracted file is identical in content and structure with the original secret file. The implemented DuoHide system was evaluated using a set of public multimedia files, images, audios, and videos, of various sizes. The secret file sizes ranged from 5% to about 100% of the cover image's size.

The experimental results showed that even at the highest embedding ratio, which is based on the secret-to-cover ratio, there were no perceptible visual differences between cover and stego images. The PNSR value was calculated as PSNR1, for cover1 and stego1, and PSNR2 for cover2 and stego2. The lowest PSNR value was around 31 dB for the highest embedding ratio, which is considered acceptable concerning statistical imperceptibility.The PSNR value increased as the embedding ratio decreased, reaching around 65 Decibel (dB) for the case of 5% secret-t- -cover ratio. The integrity of the extracted secret file was verified through a bit wise comparison between original and extracted files, which showed zero differences. The Duo Hide model is expected to provide better security for the hidden file, in case an attacker manages to capture one of the stego images and recover the hidden content because the attacker will only get an incomprehensible set of half-byte bits. An additional advantage of using a pair of stego files is that of reducing stego file size by 50%, to avoid problems and limitations of transmitting large files, especially that multimedia files are often large, and they cannot be compressed because they are already compressed. Security of the DuoHide system can further be improved by randomizing storage locations within the two stego images.

V.Sharma and R. Thakur, [4] In the present scenario of extensive mediums for communication technologies, it has always been a challenging task to ensure the confidentiality of the sensitive information that is transmitted over a secured channel. Amongst various reliable and efficient techniques to secretly exchange information, Audio Steganography is considered very promising. LSB technique for Audio Steganography is very efficient that embeds the secret message with an audio file by replacing LSBs of that audio. In this investigation Random Key Indexing method is proposed to replace the LSBs of the carrier audio with secret message. The bit replacement is guided by primary key that is provided by TTP (Trusted Third Party) and secondary key that will be generated at encoder end during embedding process and is supplied to the decoder end. The proposed method also uses message retrieval code that adds another layer of protection to the process.

The method is successfully tested on various 32 bit & 16 bit stereo wave files with different payloads. The SNR dB values comes out be in the range 139 dB to 142 dB for 32 bit and 67 dB to 85 dB for 16 bit stereo files. The Bit Error Rate (BER) comes out be in the range 0.23 to 0.32 percent for 32 bit and 0.018 to 0.028 percent for 16 bit files.

E.T.B. Abdelsatir, N. C. Debnath and H. Abushama [5] he use of audio as a host medium for steganography is relatively unpopular in comparison with Image steganography. However, Audio data can provide higher payload rates for data hiding. Among many steganography schemes in the spatial domain, LSB-based coding is widely used because of its good hiding capacity and transparency. In this exploration work, a new scheme for audio steganography in the spatial domain using a transparent LSB matching approach is reported and then tested the performance of the scheme with standard LSB substitution algorithms and well known audio steganography tools. By using a data hiding approach similar to image LSB matching, it has been observed that the proposed scheme provides the highest transparency rates compared to other existing tools.

Moreover, in subjective listening tests it is found that the hidden information does not leave a sign of steganography use and there was no auditable noise introduced in the host audio signal.

A. Binny and M. Koilakuntla,[6] Audio signals have a characteristic redundancy and unpredictable nature that make them ideal to be used as a cover to hide secret information. A Steganographic technique for embedding text information in audio using LSB based algorithm is presented in this research. In the reported method each audio sample is converted into bits and then the text data is embedded. In embedding process, first the message character is converted into its equivalent binary. By using proposed LSB based algorithm, the capacity of stego system to hide the text increases. The performance of the proposed algorithm is computed using SNR values for various audio input.

A.K. Mandal, M.Kaosar, M.O. Islam and M.D. Hossain[7] Concealing a message and ensuring its

security is inevitable in data transmission. Among various concepts, one approach is steganography that encodes secret message in indiscernible way. In this investigation, an audio steganographic technique has reported and proposes a novel approach to hide data in the least significant bit (LSB) of the stereo-audio samples with CD-quality. Here, on the basis of stego-key and its parity, message bits are encoded into cover audio samples. In terms of security and imperceptibility, this method is a significant improvement of LSB method for hiding information in audio.

IV. PROBLEM STATEMENT

Audio steganography is an efficient method to secure embedded data and sent it through internet. Unfortunately the integrity message method is not focuses in steganography technique as well as LSB technique is not introduced encrypted method before embedding secret message.

As result this work introduces the examination and analysis of various algorithm and recent work in the field of Least Significant (LSB) MP3 audio steganography method to addresses the security problems. Furthermore, to ensure the integrity messages are received correctly or not various experiments are performed in previous work such as an integrity part is added at the receiver. The fundamental objective of this work to find a suitable steganography algorithm based on the LSB technique to address the security issues.

V. CONCLUSION

This exploration investigates the audio steganography approaches based on LSB. The sensitivity of Human Auditory System (HAS) makes the information hiding in the audio files a tricky task. But, a few general environmental distortions are left unnoticed by listeners in nearly all cases. These properties are exploited by researchers to hide the secret information using audio signals as carriers. This work introduces the examination of a Least Significant Bit (LSB) technique; to solve the low security and capacity problems of the conventional used LSB techniques. The technique based on LSB includes three main steps; preprocessing, embedding and extracting and message validation. In the first stage, the main purpose is to improve the security of messages to be hidden in an MP3 file.

REFERENCES

[1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, 2017, pp. 257-260.

[2] B. Datta, P. K. Pal and S. K. Bandyopadhyay, "Multi-bit Data Hiding in Randomly Chosen LSB Layers of an Audio," 2016 International Conference on Information Technology (ICIT), (ICICS) 2009 2009, pp. 1-4. Bhubaneswar, 2016, pp. 283-287.

[3] M. T. Al-Bayati and M. M. Al-Jarrah, "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images," 2016 9th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, 2016, pp. 138- 142.

[4] V. Sharma and R. Thakur, "LSB modification based Audio Steganography using Trusted Third Party Key Indexing method," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 403- 406.

[5] E.T.B. Abdelsatir, N.C. Debnath and H.Abushama, "A multi layered scheme for transparent audio data hiding," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-6.

[6] Binny and M.Koilakuntla, "Hiding Secret Information Using LSB Based Audio Steganography," 2014 International Conference on Soft Computing and Machine Intelligence, New Delhi, 2014, pp. 56-59.

[7] A.K. Mandal, M.Kaosar, M.O. Islam and M.D. Hossain, "An approach for enhancing message security in audio steganography," Computer and Information Technology (ICCIT), 2013 16th International Conference on, Khulna, 2014, pp. 383-388.

[8] K. Srinivasan, V. Ramamurthi, and K. S. Chatha, "A technique for energy versus quality of service trade-off for MPEG-2 decoder," in IEEE Computer society Annual Symposium on VLSI, 2004, 2004, pp. 313-316.

[9] A. Delforouzi and M. Pooyan, "Adaptive and efficient audio datahiding method in temporal domain," in 7th International Conference on Information, Comm unications and Signal .

[10] H.B. Kekre, A.Athawale, B.S. Rao, and U. Athawale, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding," in 2010 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 196-201.

[11] R.Sridevi, A.Damodaram, and S.Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security," Journal of Theoretical & Applied Information Technology, vol. 5, 2009.

[12] M. S. Atoum, M. Suleiman, A. Rababaa, S. Ibrahim, and A. Ahmed, "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III," Journal of Computer Science, vol. 11, pp. 184-188, 2011.