International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 1128-1133

A Review of MP3 Steganography Methods

Latifah Uswatun Hasanah[1], Tito Waluyo Purboyo[2] and Randy Erfa Saputra[3]

[1]College Student, [2,3]Lecturer,
[1,2,3] Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia.

Orcid IDs: [1]0000-0002-6798-4396, [2]0000-0001-9817-3185, [3]0000-0002-8537-2086

Abstract

Nowadays, information security is an important thing. Much confidential information such as personal data, financial data, and even state secrets of confidential data needs to be protected so that it cannot be misused by others who are not authorized to do. One step for maintaining the security of information is by using steganography technique. Steganography image is the development of science from steganography. The first part of this paper explains what steganography means in general. Then proceed with the explanation of the study of the application of steganography on MP3 (MPEG Layer3) audio. Many methods can be used in steganographic techniques on MP3 files as though Least Significant Bit (LSB), Spread Spectrum, Direct Sequence Spread Spectrum (DSSS), Parity Coding, Phase Coding, Echo Hiding, DCT and DWT. The final part of this paper will explain the future work on steganography.

Keywords: Steganography, MP3, LSB, Spread Spectrum, DSSS, Parity Coding, Echo Hiding, DCT, DWT.

INTRODUCTION

Today, the development of all-digital technology is growing so fast. Communication technology is one of them. Many messages are delivered in digital media. Digital communication technology is a computer-based electrical communication technique using the binary number system. Binary numbers will form the codes that represent a certain information. After going through the process of digitization, the incoming information will turn into a series of binary numbers that form information in the form of digital code. Digital messages can be text, images, audio or video. The security of digital messaging, especially confidential digital messaging, is necessary. With the continuous development of digital image processing, the security techniques for digital messages can be solved. Digital secret messages can be inserted into a digital image using a technique called steganography. Many methods can be used in steganographic techniques on MP3 files such as Least Significant Bit (LBS), Spread Spectrum, Direct Sequence Spread Spectrum (DSSS), Parity Coding, Phase Coding, Echo Hiding, Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

There are several criteria that must be met in the making steganography. These criteria are : Impercepbility, is the existence of a message can not be perceived by the senses. If the message is inserted into an image, the image has been inserted message must be indistinguishable from the original image by the eye. So it is with sound, the ear must find the difference between the original sound and the sound that it has inserted message. Fidelity, ie the quality of the container media does not change much effect insertion. Changes that occur should not be perceived by the senses. Recovery, the hidden message must be reveals. The purpose of steganography is to hide information, then at any time the hidden information must be retrievable to be able used further as necessary [1,3].

Steganography is a technique that allows concealment of information or data on various types of digital media. Steganography requires two properties of the container media (images, audio, video, and text) and secret messages to be hidden. By using steganography, a secret message can be hidden by the sender unnoticed by anyone other than the recipient. Steganography techniques commonly used for the benefit of communication and information on a particular company that is confidential [1].

STEGANOGRAPHY CONCEPT

The general steganography system as: First, create a message on the cover media. The second, a stego message is created by hiding a secret message placed on the cover via message using a stego message, and then the receiver get the stego message from the channel that not secure. Lastly, a pre agreed stego key are uses for extracts secret message when receiver already receive the message [4].

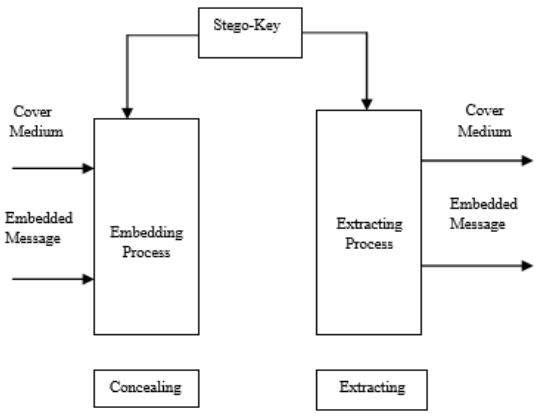

Figure 1: Steganography Process [4]

Steganography has two main processes namely embed or insertion and extract, as shown in the figure 1. The insertion process is a process of inserting (hidden object) or information or messages to be inserted, into a cover object to produce new files that have been inserted messages in it which called the stego file. While the extract process is the process of returning the hidden object as a whole after inserted into the cover object [4].

There are some important things to be kept in mind before applying or performing procedure of steganographic : Embedding Capacity, where the data is hidden in larger data volumes called cover or carriers. The embedded capacity is the amount of data can be hidden or embedded on the cover and will be compared to the cover size, because if the size of data that will be inserted on the cover is greater than the cover size then steganography can't be done. Undetectability, where the data should be hidden into carrier file in such a way that any confidential information can't be seen acciedently in the original file. If anyone detects the message in the original file then the steganography is fails. Robustness, the ability of the embedding algorithm to store embedded data even after going through the compression and decompression process. Security, in most cases, security, including perceptional transparency of the hidden data is considered the most important issue of hiding data in any different formats [3, 12].

Steganography requires two properties of the container media (images, audio, video, and text) and secret messages to be hidden.

Steganography in Images

Hiding messages in images is the most commonly used technique today. The image with a secret message in it can be easily disseminated via the web or forum. The application of steganography techniques has been investigated by Niels Provos, a German Steganographer. The usual methods used to hide information in images are LSB, masking and filtering, and transformation on the cover image. This technique can be used with various degrees of success on different types of image files [21].

Steganography in Audio

In steganography that based on audio files, secret messages are embedded into digitized audio signal which results into altering binary sequence of corresponding audio files [4]. An audio file, typically has a fairly long duration, by manipulating timing and sound frequency using a specific steganographic algorithm, the message can be passed unsuspectingly to the person who is listening to the audio file.

Steganography in Video

Steganography in video basically deals with hiding of information in each frame of video. This type reveals more information instead of hiding [4]. Steganography in the video is very similar to steganography in the picture, except the information is stored on each video frame. When the information is kept only slightly, the changes to the video will not appear, but if the information is saved a lot, the changes to the video will become more clearly involved. To reduce the size of video files without compromising image quality. Steganography can utilize the algorithm to insert secret messages into the video.

Steganography in Text

Encoding secret messages in a text can be a very challenging task. This is because text files contain redundant data to replace with a secret message. Another cons is the ease of which text-based Steganography can be altered by unwanted parties by just changing the text itself or reformatting the text to some other form (from TXT to PDF, etc.) [4].

Steganography on Audio

Steganography audio is the development of science from setagnography. The audio file can be used to hide information or secret messages. Audio Steganography methods can embed any messages in MP3 sound files. The steganography of audio, secret messages are insert into digital audio signal which results into altering binary sequence of corresponding audio files. The basic model of steganography on audio consists of carrier (Audio file), message and password. Carrier or usual called a cover file, which stores confidential information.

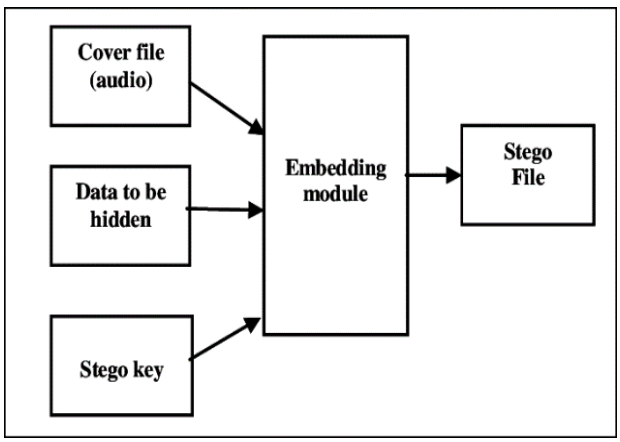

Figure 2: Basic Audio Steganography [5]

Basically, the model for steganography is present in Figure 2. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which make sure that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file [5].

STEGANOGRAPHY METHODS

LSB (Least Significant Bit)

Least Significant Bit (LSB) is part of the binary data row that.has the lowest value and is located to the right of the bits. LSB is the opposite of MSE (Most Significant Bit), which is the bit that has the highest value in the binary sequence. For the example there are as follows.

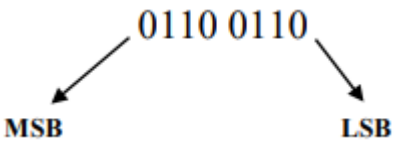

Figure 3: MSE vs LSB [2]

Figure 3 show the difference between MSE and LSB. The LSB method in audio is by changing the last bit values in a byte into one byte of audio data. Figure 4 describe the LSB Coding Procedure where the byte values of the audio data will be arranged in a random way so as not to be seen by people who are not entitled to access it [2.3].

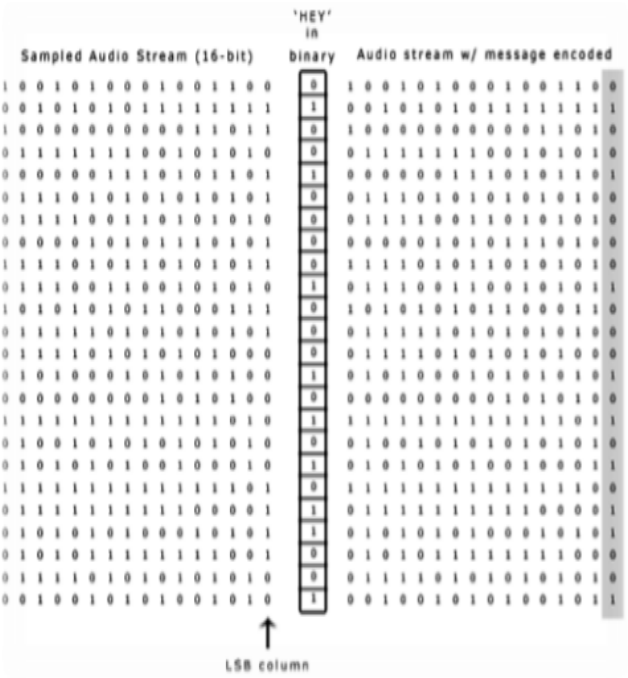

Figure 4: LSB Coding Procedure [3]

Spread Spectrum

Spread spectrum is a steganography method that inserts data by spreading secret data along the audio cover signal. In Spread Spectrum method can be done with procedure as follows. The first step, the secret information or message is represented in the form of a binary number. Secondly, information or secret messages in the form of binary numbers are duplicated with chips. Then, the secret message is modulated with a random signal so that it generates a pseudorandom signal. The secret message is dispersed by using direct sequence spread spectrum, with binary 1 being represented by 1 and the binary number 0 being repressed with -1. Confidential data valued 1 is represented by an imaginary form 1i and whose value is -1 is represented in imaginary form -1i. The cover signal is represented in the form of Fast Fourier Transform (FFT). Confidential data is inserted into the cover signal. Finally, the inserted secret data is converted to amplitude so as to produce an audio signal containing secret data.

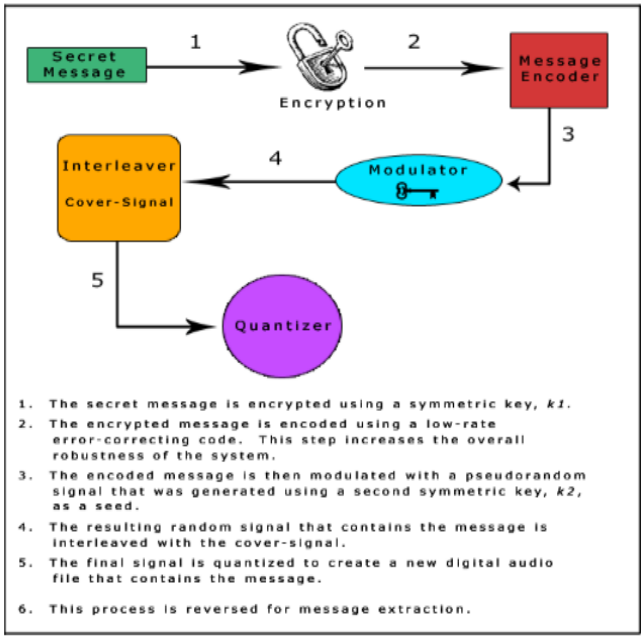

Figure 5: Spread Spectrum Procedure [4]

Figure 5 show the procedure performed by the Spread Spectrum method, the secret message is encrypted using a symmetric key. The encrypted message is encoded using a low-rate error correcting code. This step increases the overall robustness of the system. The encode message is then modulated with a pseudorandom signal that was generated using a second symmetric key as a seed. The resulting random signal that contains the message is interleaved with the cover-signal. The final signal is quantized to create a new digital audio file that contains the message. This process is reversed for message extraction [4].

Direct Sequence Spread Spectrum

Direct Sequence Spread Spectrum (DSSS) is one of the spread spectrum methods used in spreading signals by multiplying the signal source with several pseudorandom sections known as chips. The sampling rate of this signal source will then be used as the rate of the chip in its coding process. In the DSSS scheme it is explained that we must transform the cover-object to the first-frequency domain with the aim of retaining the

message of the lossy process. At first, DSSS will generate pseudonumber number to be used to determine the modulation used. pseudorandom contains rows of numbers 0 and 1, where 0 indicates that the data will not be inserted in the interveal spectrum, in this case the spectrum used is the time-domain spectrum, and 1 indicates that the data will be inserted at the spectrum interval [10].

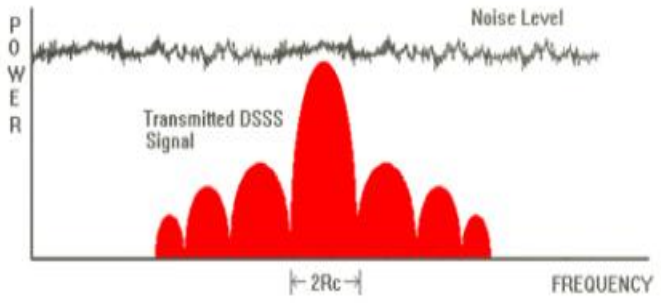

Figure 6: DSSS [10]

Figure 6 describe the data to be transmitted is divided into small pieces and each piece is allocated to a frequency channel across the spectrum. Transmitter utilizes a phase varying modulation technique to modulate each piece of data with a higher data rate bit sequence [10].

Parity Coding

One of the robust techniques on audio steganography is parity coding. The secret data embedded in parity coding is the text in the ASCII code and the bit combination dis in the bit parity. On this method original signal will be split into detached samples and parity bit of secret message will be inserted by every bit of detached samples rather then split it into an individual samples. If the secret bit that will be encoded are not compatible with selected parity bit, then the LSB of one samples in the region will be inverted. It means when secret bit will be encoded sender have more options [4].

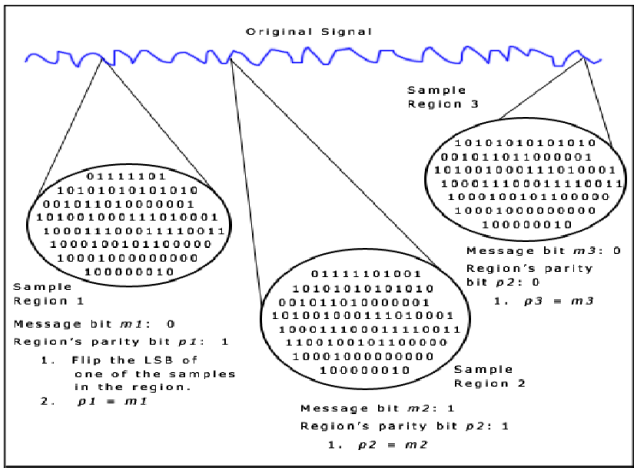

Figure 7: Parity Coding Procedure [4]

Figure 7 show the encode message in the parity bit region, and then the signal break down into separate region. Flipping to LSB is possible to get the required parity [4].

Phase Coding

Phase Coding is a method of hiding data by exchanging the original phase of the initial segment of the sound signal with the relative phase between the signal segments using the phase difference of the segment of the original signal. When the phase difference between the original signal and the modified signal is small, the resulting sound difference is not detected by human hearing. The Phase Coding method substitutes the initialization part of an audio file with another phase containing the data to be hidden. Phase coding is included in a group of frequency-based steganographic audio techniques that work by altering spectral content in the frequency domain of the signal. Phase coding is the most effective method in terms of noise signal ratio to perceived.

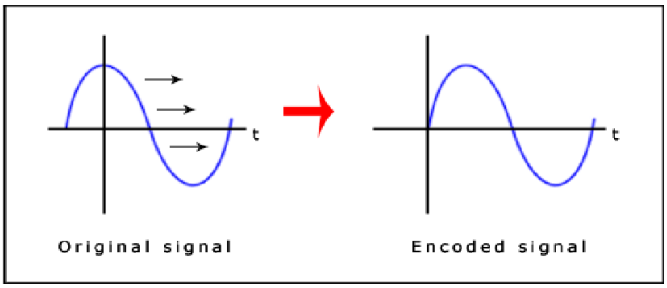

Figure 8: Phase Coding [4]

In phase coding, figure 8 show the original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded [4].

Echo Hiding

Echo data hiding technique is done by adding echo into the audio cover as a representation of the data entered. Data is hidden with three different echo parameters: Initial Amplitude, Decay rate and 22 offset, or delay. When the offset between the original audio data with its echo decreases, then the two signals will blend. At certain moments. Human hearing can not distinguish between two signals and echo is usually only considered resonance only. The use of this method depends on several factors such as the quality of the original recording, the audio type, and of course the listener.

Echo data hiding is one form of data insertion method on an audio signal [4].

This is done in the hope that the audio file that has been inserted will only decrease the sound quality to a minimum. This method has been widely used for ownership, information and assurance of data integrity. Therefore. data (inserted messages) should not be easily removed by the general transformation of the audio stego (an inserted audio signal), such as filtering, resampling, block editing or lossy data compression.

The insertion of messages on audio signals raises doubts regarding the difference in reach and ability of a human hearing system that is more dynamic than the other senses. The human auditory system can sense sounds with amplitude ranges of one billion to one and frequency range of one thousand to one. In addition, the sensitivity of the human auditory system to additional noise is also sharp.

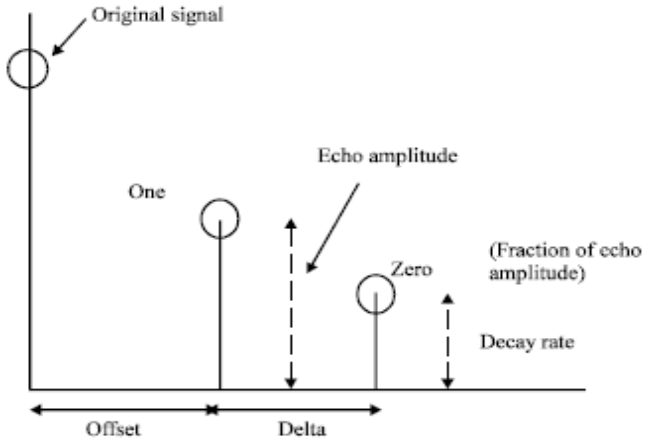

Figure 9: Echo Hiding [4]

In figure 9, echo is varied with three parameters: initial amplitude, decay rate and offset. If the offset or delay is short then the echo produced will be unperceivable. Depends on the quality of recording but max delay without effect is noted to be around 1 ms. Also, initial amplitude and decay rate can also be set below the audible threshold of the human ear. the audio signal is divided into multiple windows. Two delay times are used to encode the hidden data. Binary 0 encoded with delay=offset, binary 1 encoded with delay= offset+delta [4].

Discrete Wavelet Transform (DWT)

A Discrete Wavelet Transform is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet tranform, a key advantage it has over Fourier transform is temporal resolution. Majority of the signals in practice are represented in time domain. Time-amplitude representation is obtained by plotting the time domain signal.

DWT splits component into numerous frequency sub bands as LL (Horizontally and vertically low pass), LH (Horizontally low pass and vertically high pass), HL (Horizontal high pass and vertically low pass) and HH (Horizontally and vertically high pass) [8].

Discrete Cosine Transform (DCT)

The Discrete Cosine Tansform (DCT) is one method that can be used to perform signal and image compression. In this method only cosine functions are used in the calculation of complex numbersis. Audio and image that like one dimentional and two dimentional can be use on DCT. DCT packs the signal energy to a low frequency area that gives the option to reduce the signal size without degrading signal quality [9,13].

Advantages and Disadvantages of Steganography Methods

Table 1: Advantages and disadvantages of steganography

Methods	Advantages	Disadvantages
LSB [1]	easy to implement and fast encoding process	vulnerable to hearing by humans
Spread Spectrum [4]	secure communication and less likely to be detected	can cause noise
DSSS [10]	difficult to detected	can cause noise
Parity Coding [4]	secure communication and less likely to be detected	there is noise on the object steganography results.
Phase Coding [4]	the quality produced by mp3 files after the message inserted almost no detectable noise	can only be used when wanting to hide data of small size
Echo Hiding [4]	the human hearing system is difficult to distinguish between echo and the original signal	less good used on audio files that have a large enough silence gap because echo will sound obvious
DWT [8]	computationally very fast	suspected of having a lower load with spatial domain algorithms
DCT [13]	computationally very fast	Not resistant to changes in an object

FUTURE WORKS

Steganography is a technique of concealment of information or confidential data that is safe on digital media. There are constant advancements in the computer field, suggesting advancements in the field of steganography as well. Expected for the future the concept of steganography with various existing methods will continue to be developed again. For the sender of the secret message is expected to be smart and meticulous in using steganography techniques. For recipients of secret messages are also expected can understand to analyze the results of the insertion of the secret message. To the future, it is hoped that the technique of steganalysis will advance such that it will become much convenient to detect even small messages within an audio file.

CONCLUSION

The advantage of steganography is that the message sent does not attract attention so that the container media carrying the message does not arouse suspicion for others. In this paper a review, has been discussed about audio data concealment techniques on mp3 files. This technique is better and efficient to hide secret data from hackers and sent to the destination in a safe way. Media that has been inserted a secret message will not resize the file significantly.

REFERENCES

[1] Surekha Shrivastava, Mr. Gajendra Singh Chandel, Mr. Kaislash Patidar, "A Modified Approch Audio Steganography Based on Technique LSB Coding", International Journal of Engineering and Applied Sciences (IJEAS), Volume-2, Issue-5, May 2015.

[2] Aquino, I. Rivera, S.A. Garcia, "Implementation of Lsb Steganography Algorithm in Mp3 Audio File", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 2, No.6, December 2012.

[3] Ms. Manisha, Ms. Maneela, "A Survey on Various Methods of Audio Steganography" International Journal of Advanced Research in Computer Science and Software Engineering" Volume 4, Issue 5, May 2014.

[4] Palwinder Singh, "A Comparative Study of Audio Steganography Techniques" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 04 | Apr-2016.

[5] Mohsen Bazyar and Rubita Sudirman, "A Recent Review of MP3 Based Steganography Methods" International Journal of Security and Its Applications, Vol.8, No.6 (2014).

[6] Nishant Sharma, Er. Gaurav Deep, "Review: To Study Scope of Data Hiding in MP3 Files", IJCSET(www.ijcset.net) | June 2015 | Vol 5.

[7] Gunjan Nehru1, Puja Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[8] Wei Zeng, Ruimin Hu, Haojun Ai, Cairong Li, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM", Networks Security, Wireless Communications and Trusted Computing, International Conference on, vol. 01, no. , pp. 240-243, 2009, doi:10.1109/NSWCTC.2009.78.

[9] Vanitha T, Anjalin D Souza , Rashmi B, Sweeta Dsouza, "A Review on Steganography - Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014.

[10] Rupanshi, Preeti, Vandana, "Audio Steganography by Direct Sequence Spread Spectrum", International Journal of Computer Trends and Technology (IJCTT) – volume 13 number 2 – Jul 2014.

[11] Wei Qin Cheng, Fei Han, Man Juon Tung, Kai Xu "Robust Audio Steganography using Direct-Sequence Spread Spectrum Technology", Fall 2007.

[12] Prashant Johri, Amba Mishra, Sanjoy Das, Arun Kumar, "Survey on Steganography Methods (Text, Image, Audio, Video, Protocol and Network Steganography" 2016 International Conference on Computing for Sustainable Global Development (INDIA.Com).

[13] Sumeet Gupta, Dr. Namrata Dhanda, "Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT)", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 32-44.

[14] Palak R Patel, Yask Patel, "Survey on Different Methods of Image Steganography", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue 12, December 2014.

[15] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Bamik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, Issue 4, June 2012.

[16] M.Baritha Begum ,Y.Venkataramani "LSB Based Audio Steganography Based On Text Compression", International Conference on Communication Technology and System Design 2011.

[17] Mohammed Salem Atoum, Mamoun Suleiman Al Rababaa, Dr. Subariah Ibrahim, "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011.

[18] Satish Singh Verma, Ravindra Gupta, Gaurav Shrivastava, "A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", 2014 Fourth International Conference on Communication Systems and Network Technologies.

[19] Linu Babu, Jais John S, Parameshachari B D,,Muruganantham C, H S DivakaraMurthy, "Steganographic Method for Data Hiding in Audio Signals with LSB & DCT", International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August- 2013.

[20] Miss Preeti Jain, Prof.Vijay Trivedi, "Effective Audio Steganography by using Coefficient Comparison in DCT Domain", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 8, August – 2013.

[21] Aryfandy Febryan, Tito Waluyo Purboyo, Randy Erfa Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey", International Journal of Applied Engineering Research (IJAER) Vol. 12 Number 21 (2017).