Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Recent Steganography Technique Using Audio Carrier

Satish Singh Verma
M. Tech Scholar, CSE. Dept.
RKDF Institute of Science & Tech
Bhopal, M.P., India

Mr. Ravindra Gupta, Mr. Gaurav Shrivastava
Computer Science & Engg. Dept.
RKDF Institute of Science & Tech
Bhopal, M.P., India

Abstract— Steganography is a branch of cryptography, which literally means "hidden writing", is about hiding the existence of a message inside text, images, audio, video. Audio as a cover medium in steganography has its own place due to its bigger size compare to other carrier's file like (text, image, etc.). So we can hide large amount of data inside audio as a cover. Steganographic algorithms can be characterized by a number of defining properties like Transparency , Capacity, Robustness. In this paper we will survey the general principles of hiding secret information using audio technology, and provide an overview of current functions and techniques.

Keywords— Audio Steganography, Information Hiding, Least Significant Bit Coding, Parity Coding, Phase Coding, Spread Spectrum, Echo data hiding

I. Introduction

In the present communication era, protection of our secret information is primary aim when we want to send some secret information to other. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the privacy and data integrity are required to protect against illegal access. This has resulted in an explosive expansion of the field of information hiding [1]. Information hiding is the process of hiding the details of an object or function. The hiding of these details results in an abstraction, which reduces the external complexity and makes the object or function easier to use.

Steganography is a way to protect security and privacy of valuable information. While cryptography is the process to protecting the secret data by encrypt the content, steganography concerns on protecting the secret message by hiding the content. The concealment of secret messages is achieved by embedding them into other digital mediums as cover [1], [2]. Fig. 1 shows the Fundamental scheme of stegnography process. In the Embedded section we need a secret message and a cover signal to hide the secret message. Size of the cover signal must be sufficient to hide the secret message. ouput of the embedded section is a stego-signal which is the modified cover signal containing secret message. In the recovery section we need the original cover signal and the stego-signal. Cover signal must be same as used in embedded section. We got the secret message as output of this section by performing some operation which is depending on the technique we use for stegnography

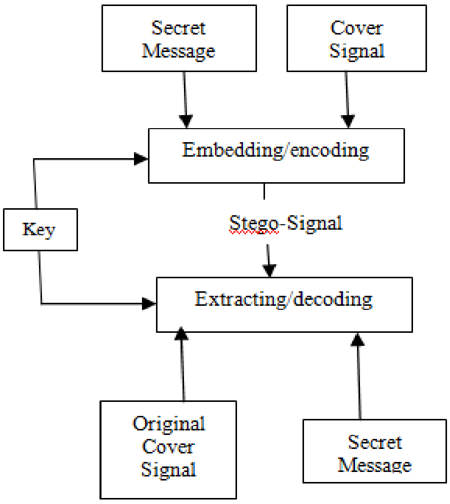


Figure 1. Fundamental process of steganography

There are four ways to implement steganography as shown in fig. 2:

- Using text.
- Using images.
- Using audio files.
- Using video files.

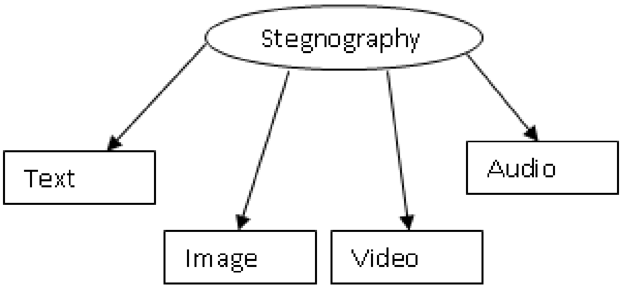


Figure 2. Classification of Steganography

Generally, in steganography the following operations are performed:

- Write a non-secret cover message.
- Produce a stego-message by concealing a secret embedded message on the cover message by using a stego-key.
- Send the stego-message over the insecure channel to the receiver.
- At the other end, on receiving the stego-message, the intended receiver extracts the secret embedded message from the stego-message by using a pre agreed stego-key.

II. OVERVIEW OF AUDIO STEGANOGRAPHY

Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and strongly. Communication security and robustness are vital for transmitting important information to authorized entities, while denying access to not permitted ones. By embedding secret information using an audio signal as a cover medium, the very existence of secret information is hidden away during communication. This is a serious and vital issue in some applications such as battlefield communications and banking transactions [11]. In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU and even MP3 sound files.

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.. 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 ensures 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. The information hiding process consists of following two steps [10].

- Identification of redundant bits in a cover-file. Redundant bits are those bit that can he modified without corrupting the quality or destroying the integrity of the cover-file.
- To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected [13]. Basic Audio steganography model is shown in Fig. 3.

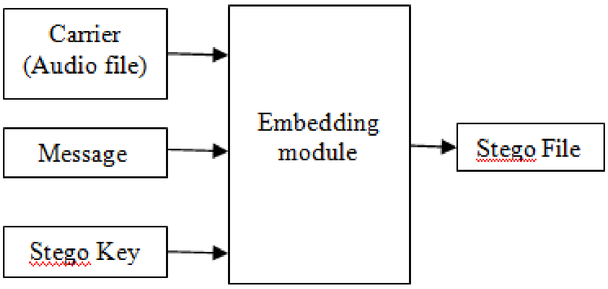


Figure 3. Basic Audio steganography model

III. AUDIO STEGANOGRAPHIC TECHNIQUES

An audio steganography technique can be classified into two groups based on the domain of operation. One type is time domain technique and the other is transformation based method. The time domain techniques include methods where the embedding is performed without any transformation. Steganography is employed on the original samples of the audio signal. One of the examples of time domain steganography technique is the least significant bit (LSB) method. In LSB method the watermark is embedded into the least significant bits of the host signal. As against these techniques, the transformation based steganography methods perform steganography in the transformation domain. Few transformation techniques that can be used are discrete cosine transform and discrete wavelet transform. In transformation based approaches the embedding is done on the samples of the host signal after they are transformed. Using of transformation based techniques provides additional information about the signal. In general, the time domain techniques provide least robustness as a simple low pass filtering can remove the watermark. Hence time domain techniques are not advisable for the applications such as copyright protection and airline traffic monitoring; however, it can be used in applications like proving ownership and medical applications [40].

A. LSB Coding

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

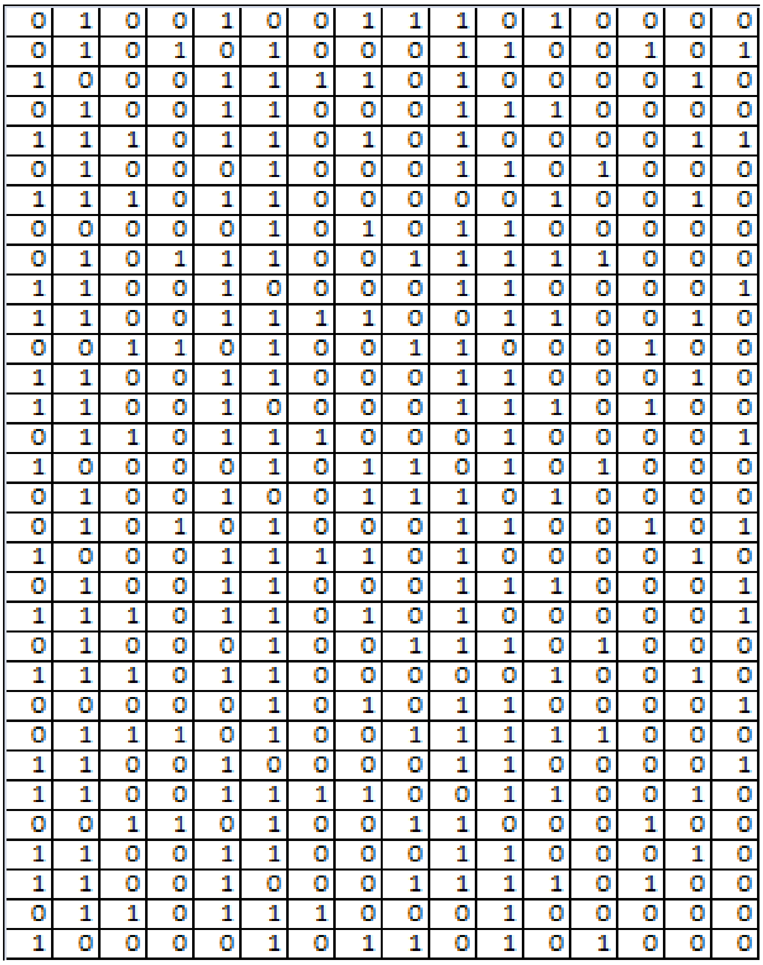
Standard LSB Algorithm:

It performs bit level manipulation to encode the message. The following steps are

- Receives the audio file in the form of bytes and converted in to bit pattern.
- Each character in the message is converted in bit pattern.
- Replaces the LSB bit from audio with LSB bit from character in the message.

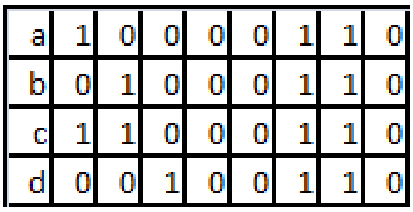
In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in 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.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage : As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable [5].



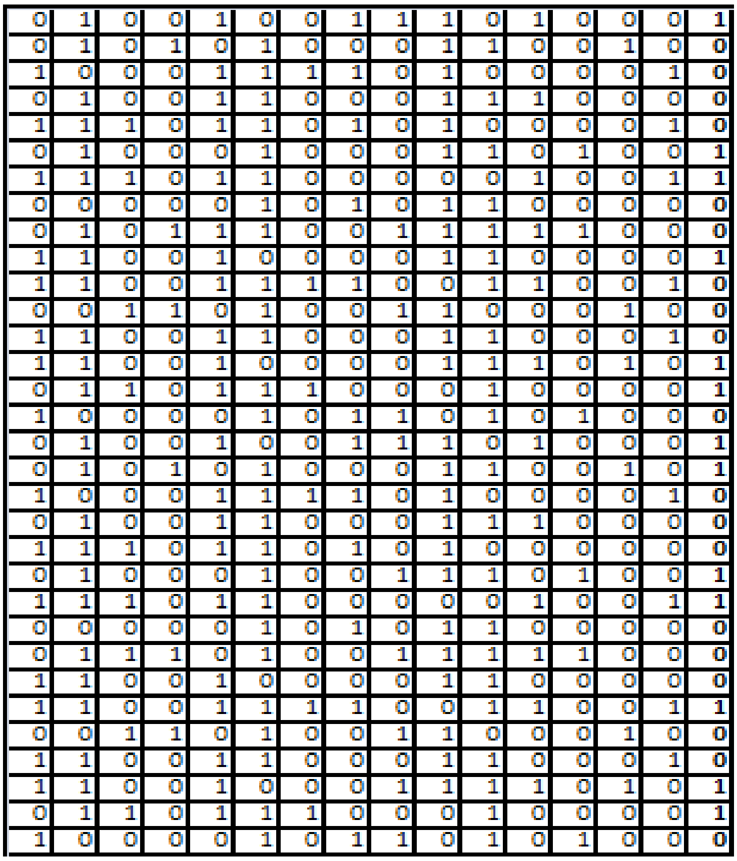
0	1	0	0	1	0	0	1	1	1	0	1	0	0	0	0
0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	1
1	0	0	0	1	1	1	1	0	1	0	0	0	0	1	0
0	1	0	0	1	1	0	0	0	1	1	1	0	0	0	0
1	1	1	0	1	1	0	1	0	1	0	0	0	0	1	1
0	1	0	0	0	1	0	0	0	1	1	0	1	0	0	0
1	1	1	0	1	1	0	0	0	0	0	1	0	0	1	0
0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0
0	1	0	1	1	1	0	0	1	1	1	1	1	0	0	0
1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1
1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	1	0	0	1	1	0	0	0	1	0	0
1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	1	0	1	0	0
0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	1
1	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0
0	1	0	0	1	0	0	1	1	1	0	1	0	0	0	0
0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	1
1	0	0	0	1	1	1	1	0	1	0	0	0	0	1	0
0	1	0	0	1	1	0	0	0	1	1	1	0	0	0	1
1	1	1	0	1	1	0	1	0	1	0	0	0	0	0	1
0	1	0	0	0	1	0	0	1	1	1	0	1	0	0	0
1	1	1	0	1	1	0	0	0	0	0	1	0	0	1	0
0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	1
0	1	1	1	0	1	0	0	1	1	1	1	1	0	0	0
1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1
1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	1	0	0	1	1	0	0	0	1	0	0
1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	0
1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	0
0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0
1	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0

Figure 4. Sampled Audio Stream (16 bit).



a	1	0	0	0	0	1	1	0
b	0	1	0	0	0	1	1	0
c	1	1	0	0	0	1	1	0
d	0	0	1	0	0	1	1	0

Figure 5. Binary value of message “abcd”



0	1	0	0	1	0	0	1	1	1	0	1	0	0	0	1
0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0
1	0	0	0	1	1	1	1	0	1	0	0	0	0	1	0
0	1	0	0	1	1	0	0	0	1	1	1	0	0	0	0
1	1	1	0	1	1	0	1	0	1	0	0	0	0	1	0
0	1	0	0	0	1	0	0	0	1	1	0	1	0	0	1
1	1	1	0	1	1	0	0	0	0	0	1	0	0	1	1
0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0
0	1	0	1	1	1	0	0	1	1	1	1	1	0	0	0
1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1
1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	1	0	0	1	1	0	0	0	1	0	0
1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	1	0	1	0	1
0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	1
1	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0
0	1	0	0	1	0	0	1	1	1	0	1	0	0	0	1
0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	1
1	0	0	0	1	1	1	1	0	1	0	0	0	0	1	0
0	1	0	0	1	1	0	0	0	1	1	1	0	0	0	0
1	1	1	0	1	1	0	1	0	1	0	0	0	0	0	0
0	1	0	0	0	1	0	0	1	1	1	0	1	0	0	1
1	1	1	0	1	1	0	0	0	0	0	1	0	0	1	1
0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0
0	1	1	1	0	1	0	0	1	1	1	1	1	0	0	0
1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0
1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	1
0	0	1	1	0	1	0	0	1	1	0	0	0	1	0	0
1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	0
1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	1
1	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0

Figure 6. Audio stream with embedded message

B. Phase Coding

Phase coding addresses the disadvantages of the noise-inducing methods of audio Steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio. The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a 0 or a 1 and this indicates where the message starts.

This method has many advantages over Low Bit Encoding, the most important being that it is undetectable to the human ear. Like all of the techniques described so far though, its weakness is still in its lack of robustness to changes in the audio data. Any single sound operation or change to the data would distort the information and prevent its retrieval [8].

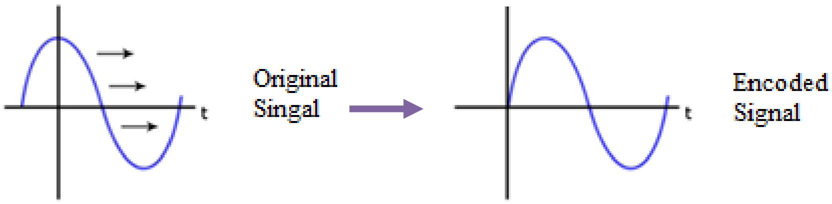


Figure 7. Phase Shift coding

C. Echo Hiding

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of this artificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude. As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually a created carrier sound's echo is just heard as extra resonance.

In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal. The "one" echo signal is then multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes.

Fig. 9 summarizes the implementation of the echo hiding process. To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's spectrum (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed. Much like phase encoding this has considerably better results than Low Bit Encoding and makes good use of research done so far in psychoacoustics. As with all sound file encoding, we find that working in audio formats such as WAV is very costly, more so than with bitmap images in terms of the "file size to storage capacity" ratio. The transmission of audio files via e-mail or over the web is much less prolific than image files and so is much more suspicious in comparison. It allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods

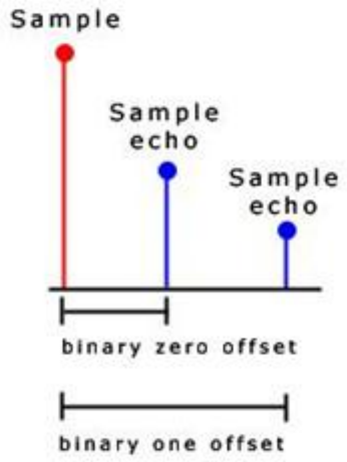


Figure 8. Example of Echo Hiding

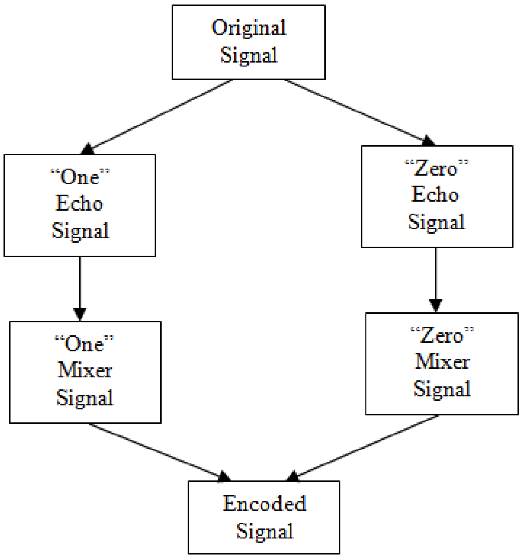


Figure 9. implementation of Echo Hiding process

D. Spread Spectrum

Spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key. The technique has been used by the military since the 1940s because the signals are hard to jam or intercept as they are lost in the background noise. Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium. Two versions of SS can be used in audio Steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

Spread Spectrum Steganography has significant potential in secure communications – commercial and military. Audio Steganography in conjunction with Spread Spectrum may provide added layers of security. Spread spectrum encoding techniques is most secure means by which to send hidden messages in audio as cover, but it can introduce random noise to the audio thus creating the chance of data loss. They have the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques

The following procedural diagram illustrates the design:

- Message is encrypted using a symmetric key, k1
- The encrypted message is encoded using a low-rate error-correcting code.
- The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key, k2.
- The resulting random signal that contain 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.

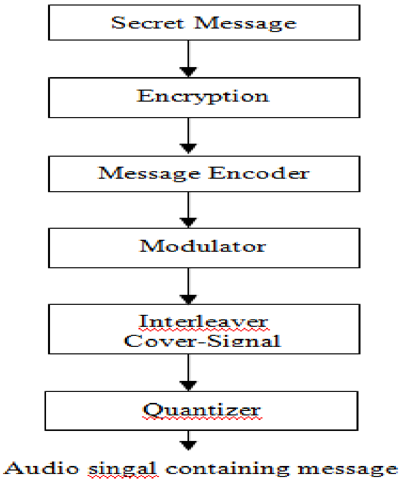


Figure 10. Procedural diagram of Spread Spectrum Design

E. Parity Coding

In parity coding, audio signal is broken down into separate areas of samples and hide the secret message in the parity bit of each sample area. If the parity bit of a sample area does not match the secret message bit to be embedded, the LSB of one of the samples in the area is inverted. Therefore, this will give a wider range of choices on where to hide the secret bit, and will keep the change in the signal more unobservable [5].

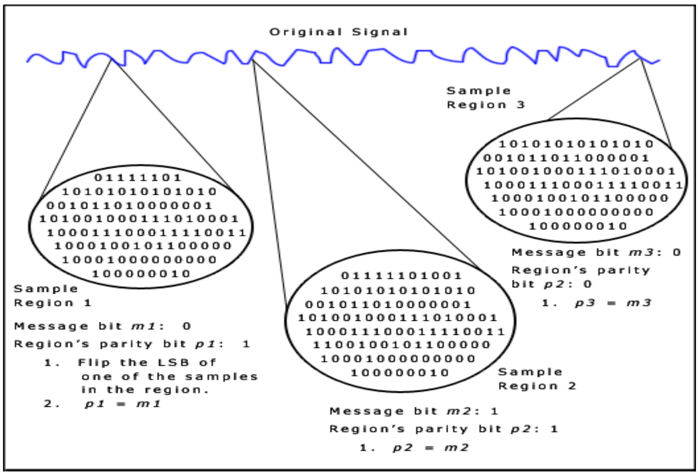


Figure 11. Procedural diagram of Parity Coding

IV. QUALITY CRITERIA

There are some basic criteria has been proposed to further describe the quality of a steganography algorithm[5] -

A. *Payload Capacity*

Payload capacity is defined as the the size of secret information or data that can be hidden into a cover medium relative to the size of this medium.

B. *Imperceptibility*

Imperceptibility is defined as the strength of steganography system depends on its ability to be unnoticed by the human senses.

C. *Robustness*

Robustness measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks

V. DISCUSSION

A. *LSB*

- High Payload Capacity
- Medium Imperceptibility
- Low Robustness

B. *Parity Coding*

- Medium Payload Capacity
- Medium Imperceptibility
- Low Robustness

C. *Phase Coding*

- Low Payload Capacity
- High Imperceptibility
- High Robustness

D. *Spread Spectrum*

- High Payload Capacity
- Low Imperceptibility
- High Robustness

E. *Echo Hiding*

- High Payload Capacity
- Low Imperceptibility
- Medium Robustness

VI. CONCLUSIONS

In this paper, several techniques are discussed as potential methods for embedding data in real time audio signals. While a degree of success has been achieved, each one of the proposed methods has its limitations. The ultimate goal of attaining protection of large amounts of secret data against deliberate attempts at removal may be still far from being obtained. The five techniques discussed above offer numerous choices and make this data hiding technology more obtainable and accessible. Prioritizing the importance of communication and security characteristics such as data rate, bandwidth, robustness, and noise audibility, must be done before choosing the steganographic technique which should completely fits the nature, environment and requirements of the application.The flexible nature of audio formats, signals and files, is what makes them good and practical medium for steganography. Another aspect of audio steganography that makes it so attractive and promising is the ability to combine steganography techniques with existing cryptography technologies. We do not have to depend on one technique only. Secret data not only can be encrypted, they can be hidden and encrypted at the same time

REFERENCES

[1] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan. O. Alanazi, Overview: Main Fundamentals for Steganography, journal of computing, volume 2, issue 3, march 2010, issn 2151-9617.

[2] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE" International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[3] Neil Jenkins, Jean Everson Martina ," Steganography in Audio" Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais page: 269-278,2007

[4] Prof. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul, Avishek Raychoudhury," A Robust Audio Steganographic Technique based on Phase Shifting and Psycho – acoustic Persistence of Human Hearing Ability", International Journal of Computing and Corporate Research

[5] Abdulaleem Z. Al-Othmani1, Azizah Abdul Manaf2 and Akram M. Zeki3," A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[6] Jayaram P, Ranganatha H R, Anupama H S, INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY, The International Journal of Multimedia & Its Applications (IJMA), Vol.3, No.3, August 2011

[7] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, Audio Steganography: A Survey on Recent Approaches, World Applied Programming, Vol (2), No (3), March 2012. 202-205 ISSN: 2222-2510.

[8] Lee, Y. K. and Chen L. H. “High Capacity Image Steganographic Model”. IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[9] Ronak Doshi, Pratik Jain, Lalit Gupta,”Steganography and Its Applications in Security”, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638.

[10] N. Taraghi-Delgarm, “Speech Watermarking”, M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006

[11] Kekre, H.B., A. Archana R. Swarnalata and A. Uttara, 2010. Information hiding in audio signals. Int. J.Comput. Appl., 7(9).

[12] Haider Ismael Shahadi, Razali Jidin,” high capacity and inaudibility audio steganography scheme”, 2011 7th international conference on information assurance and security (ias), 978-1-4577-2155-7/11/$26.00 c_2011 ieee.