Vol. 2, Issue IV, April 2014
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

A Survey on Various Methods of Audio Steganography

Ms. Lalita[1], Mr. Sumit Wadhwa[2]

[1]M.Tech Student, CSE Department
[2]Assistant Professor,CSE Department
[1,2]Samalkha Group of Institution, Kurukshetra University

Abstract: *In this paper, we have presented different types of steganography techniques. The different categories of steganography have been discussed in brief and main focus is put on audio steganography technique. Initially, we have surveyed about text steganography and then move to another steganography technique i.e. image steganographyand its techniques are discussed in brief. During image steganography, Least Significant Bits, Masking and filteringand Transformations will be subjected. Finally, audio steganography which contains LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding techniques is described.*

1. INTRODUCTION

The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”defining it as “covered writing” [1]. Steganography is one such pro-security innovation in which secret data is embeddedin a cover [2]. The notion of data hiding or steganography was first introduced with the example of prisoners' secretmessage by Simmons in 1983 [3].Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot beunderstood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of themessage in the first place. In some situations, sending an encrypted message will arouse suspicion while an ”invisible” message will not do so. Both sciences can be combined to produce better protection of the message. In this case, whenthe steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptographytechniques. [4]There exist two types of materials in steganography: message and carrier. Message is the secret data that should behidden and carrier is the material that takes the message in it [5]. Fig. 1 below shows the different categories of file formats that can be used for steganography techniques.

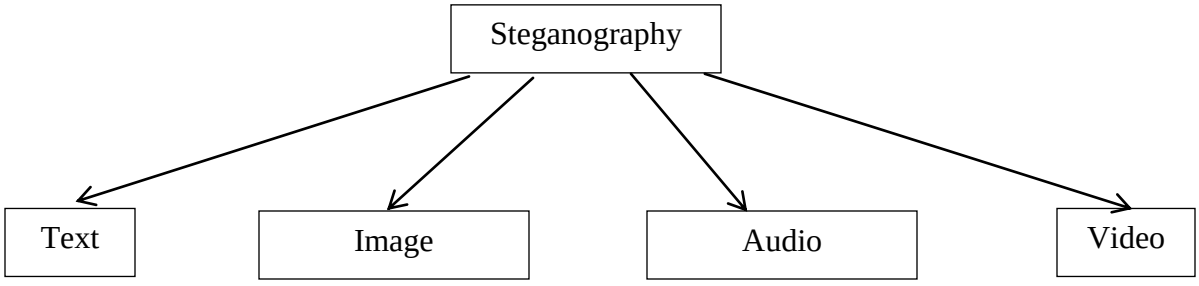

Figure 1: Different categories of file formats that can be used for steganography techniques.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

TABLE 1
COMPARISON OF SECRET COMMUNICATION TECHNIQUES [6].

Communication Technique	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/ No	Yes

Comparison of secret communication techniques is shown in Table –I.
Steganography can be split into two types:
a) Fragile:This steganography involves embedding informationinto a file which is destroyed if the file is modified.
b) Robust: Robust marking aims to embed information into afile which cannot easily be destroyed.
The comparison of various methods of steganographyand their advantages is as shown in the Table 2.

TABLE 2
COMPARISON OF VARIOUS METHODS OF STEGANOGRAPHY [6]

No	Technique of Steganography	Cover Media	Technique of Embedding	Advantage
1.	Text Technique	Document	To embedinformation insidea document we cansimply alter some of itscharacteristics.i.e.either the text formatting orcharacteristics of the characters	Alterations not visible to the human eye
2.	Image Hiding: 1)LSB(Least Significant Bit Image)	Image	It works by usingthe leastsignificant bits ofeach pixel in oneimage to hide themost significantbits of another.	Simple & easiest way of hiding Information.
	2) DCT (Direct Cosine Transform)		Embeds theinformation by altering thetransformed DCT coefficients.	Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.
	3) Wavelet Transform		This techniqueworks by taking many wavelets toencode a whole image.	Coefficients of the wavelets are altered with the noise within tolerable levels
3.	Sound Technique	MP3 files	Encode data as abinary sequence which sounds likenoise but which can be recognized by a receiver with	Used for watermarking by matching the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

			the correct key.	narrow bandwidth of the embedded data to the large bandwidth of the medium
4.	Video Technique	Video Files	A combination ofsound and image techniques can beused	The scope for adding lots of data is much greater

2. DATA HIDING

Various schemes are used for data hiding in audio,such as echo hiding[7], time domain modification[8],and spread spectrum technology[9]. Data hiding in audiomust satisfy at least the three constraints of securityor imperceptibility, robustness, and capacity. Theseterms are commonly used to describe the properties ofdifferent data hiding schemes.

Security Data hiding in audio is also called inaudibility.In most cases, security, including perceptualtransparency of the hidden data, is considered to be themost important issue. In other words, the noise introducedby the hidden data should be almost inaudibleand should not degrade the audio quality. The statisticalproperties of the embedded audio signal should beexactly the same as the original audio to ensure that thehidden data is imperceptible and undetectable by thirdparties [10].

Robustness The algorithm should be robustenough to withstand unintentional or intentional attemptssuch as removal or alteration of the hidden data.Even with unfavorable conditions such as bad wirelesschannels which degrade the audio quality, the hiddendata should be recovered successfully.

Capacity Often, the capacity of the hidden data isalso a very demanding aspect. Capacity refers to thenumber of bits per second that can be transmitted bythe data hiding system. This depends on the underlyingtechnology and the choice of parameters for the hidingscheme. At present, the data rates reach several hundredbits per second.

Security, robustness, and capacity have contradictoryarguments so they cannot be adjusted independently.For instance, increases of the data hiding capacitywill degrade the robustness and security. This trade-offs form the triangle shown in Fig. 2 with anappropriate operating point within the limits of the trianglechosen for different applications.

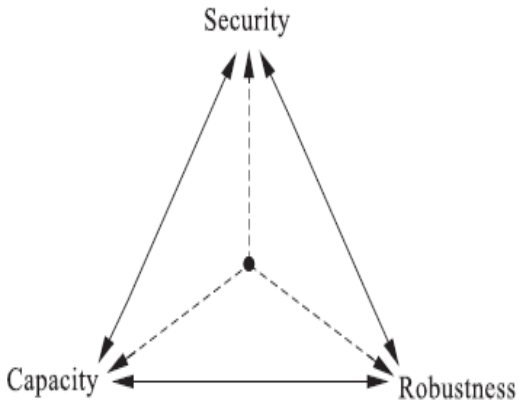

Figure 2: Trade-off between security, robustness, and Capacity [10]

3. METHODS OF AUDIO STEGANOGRAPHY

This section presents some common methods used in audio Steganography

3.1 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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

large amount of data to be encoded [8]. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method (Fig. 3) :

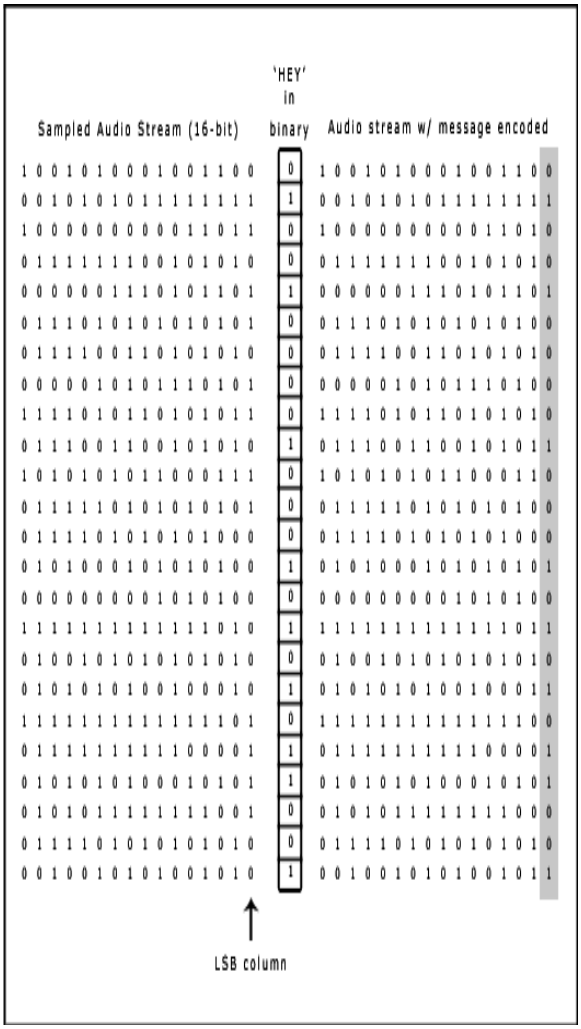

Figure 3: LSB CODING

Standard LSB ALGORITHM:

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

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. 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 [8].

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.

3.2 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 (fig. 4) , achieving an inaudible encoding in terms of signal-to-perceived noise ratio [8].

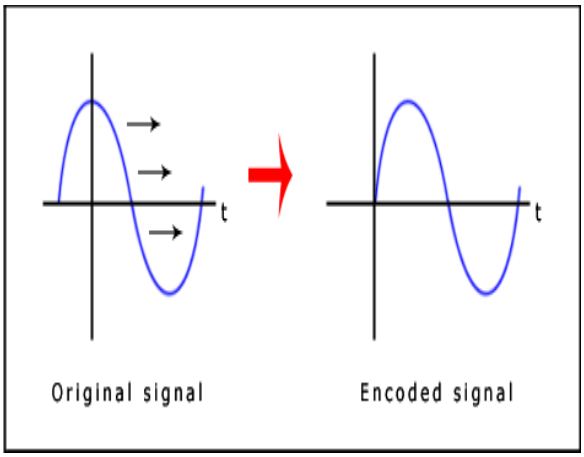

Figure 4: PHASE CODING

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

Vol. 2, Issue IV, April 2014
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

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[8].

This method has many advantages over Low Bit Encoding, the most important being that it isundetectable 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.

3.3 ECHO HIDING

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of thisartificial 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 [7].

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 as shown in fig. 5.

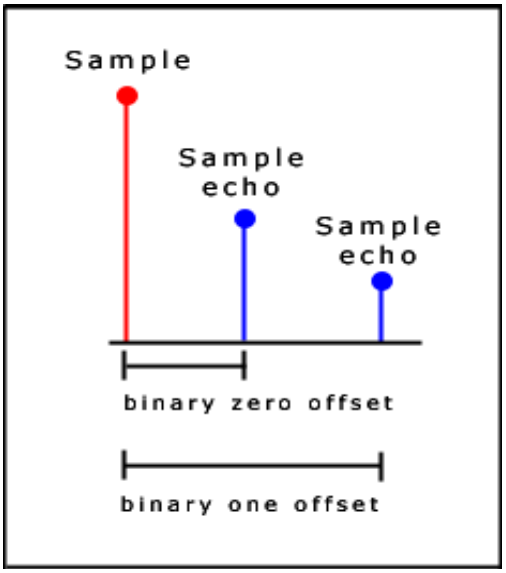

Figure 5: ECHO HIDING

The blocks are recombined to produce 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 as shown in fig. 6. 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 [7].

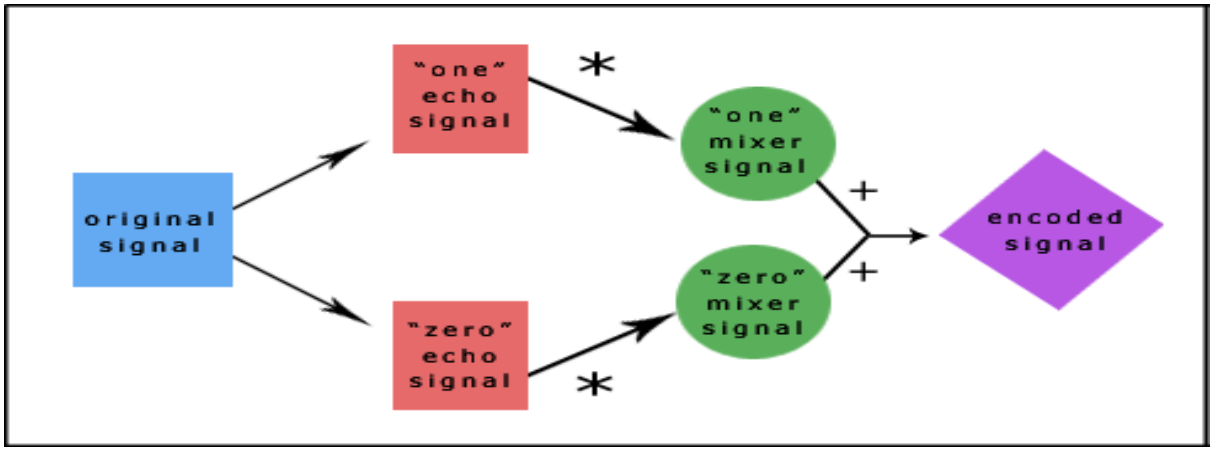

Figure 6: ECHO HIDING

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

These two characteristics of the mixer signals produce smoother transitions between echoes.

The following diagram summarizes the second 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 [7].

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.

3.4 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 [9].

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 [9].

Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, 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 [9].

The following procedural figure illustrates the design (fig. 7):

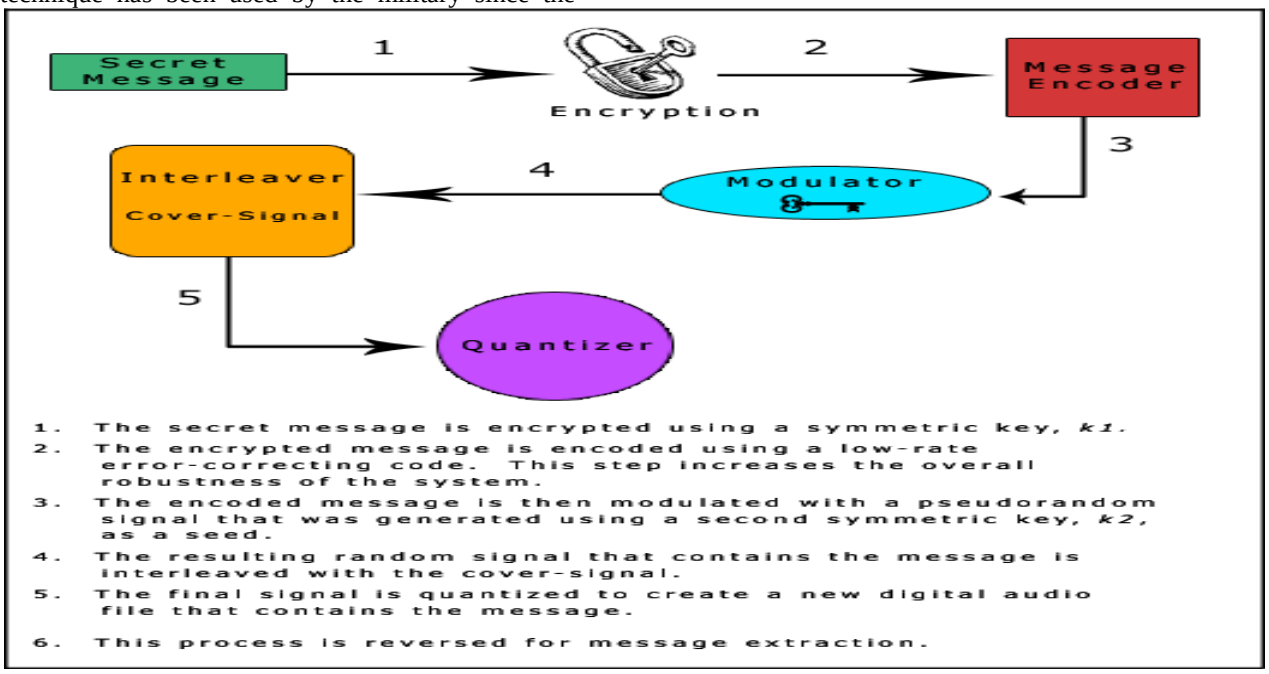

Figure 7: Spread Spectrum

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

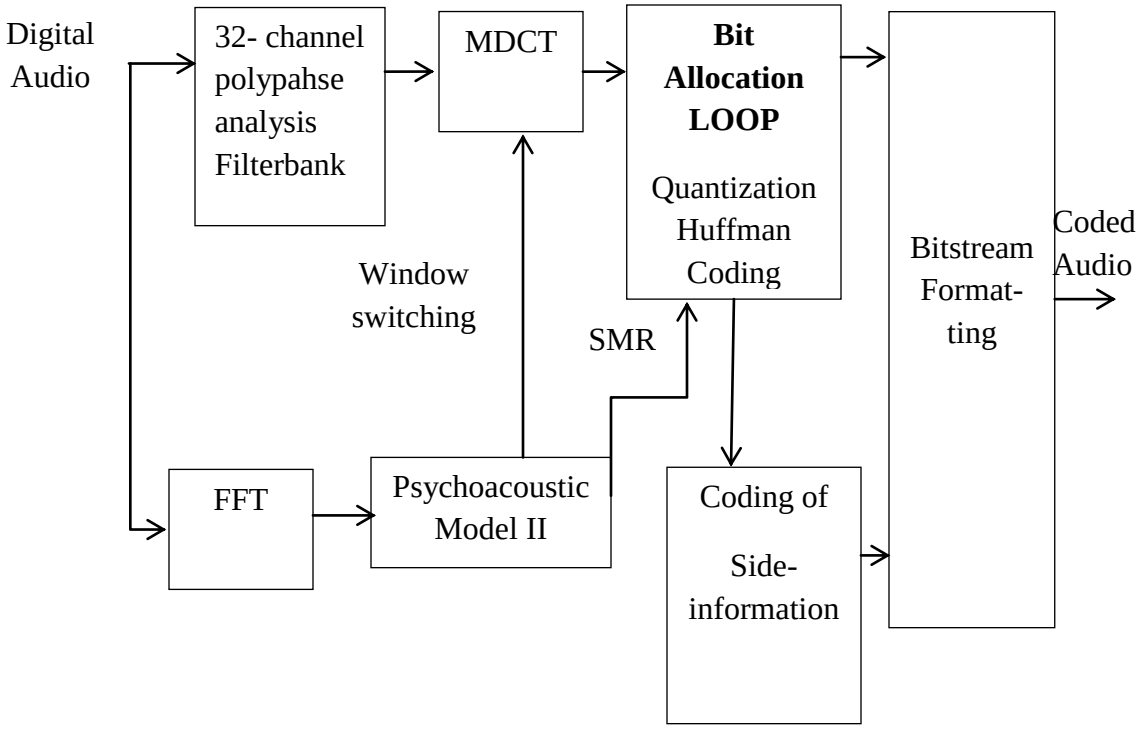

Figure 8: MP3 audio encoding process [11]

MPEG-1 Audio Layer 3 (MP3) [11] is a digital audioencoding format using lossy compression algorithm , whichremarkably reduces the amount of data required to representthe audio and still provide audio quality comparable touncompressed audios for most listeners. To ensure that thedegradation of the audio quality is imperceptible to theauditory resolution ability of most people, perceptual codingis introduced to analyze a short term time or frequencywindow, and reduce less audible detail components withinthe signal.

Figure 8 illustrates the entire MP3 audio encoding process,which consists of following steps:

(I) Through filter bank analysis, a 16-bit PCM(Pulse-code Modulation) signal is converted to 32 sub-bandsignals with same bandwidth.

(2) A sub-band signal is further divided into 18 signals byapplying Modified Discrete Cosine Transform (MDCT).

(3) According to the Signal-to-Mask Ratio (SMR)generated by Psychoacoustic Model II, a certain number ofbits is assigned to represent the signal.

(4) Quantize and Huffman encode the signal, and finallyconstruct the file according to the MPEG-1 format standard.

4. CONCLUSION

This paper has looked in detail at the major techniques used for data hiding in audio files. Section I gave an overview of Steganography and in particular the concept of Audio Steganography. Section II described in detail, various Audio Steganography algorithms namely LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding. At the end,Audio encoding process was discussed with the help of its block diagram.It can be concluded that, steganography does in fact have a number of disadvantages i.e. it has high overhead for hiding a few bits of information. This disadvantage can be overcome relatively easily. Another problem is that a steganographic system is rendered useless once it has been discovered. This also can be overcome by utilizing a key for the insertion and extraction of the hidden data. Also, Spread Spectrum method is known to be very robust, but as a consequence the cost is very large, the implementation is relatively complex,

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

less secure and the information capacity is very limited. Current spread spectrum stegano-graphic applications with audio media are primarily limited to providing proof of copyright and assurance of content integrity. There is the potential to expand the applications to include the embedding of covert communications. Above mentioned problems related to spread spectrum can be overcome by using Direct Sequence Spread Spectrum (DSSS). DSSS used to increase the security and robustness of the system. Improvement can be achieved in robustness on the expense of reducing the capacity of hiding.

REFERENCES

[1] Sara Khosravi, MashallahAbbasiDezfoli, Mohammad HosseinYektaie, " A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication" , Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA,2000.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.

[4] Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at:http://www.krenn.nl/univ/cry/steg/article.pdf

[5] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

[6] ShashikalaChannalli et al ," Steganography An Art of Hiding Data "International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[7] Gruhl D, Lu A, Bender W. Echo hiding. *Lecture Notes inComputer Science*, 1996, 1174: 295-315.

[8] Xu Chansheng, Wu Jiankang, Sun Quibin, et al. Applications of digital watermarking technology in audio signals. *Journal of Audio Engineering Society*, 1999, 47(10): 805-812.

[9] Garcia R A. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In: 107th AES Convention. New York, USA, 1999:2713-2720.

[10] XU Shuzheng, ZHANG Peng, WANG Pengjun, YANG Huazhong, "Performance Analysis of Data Hiding in MPEG-4 AAC Audio" TSINGHUA SCIENCE AND TECHNOLOGY Volume 14, Number 1, February 2009.

[11]MengyuQiao, Andrew H. Sung, Qingzhong Liu, "Steganalysis of MP3Stego" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009.