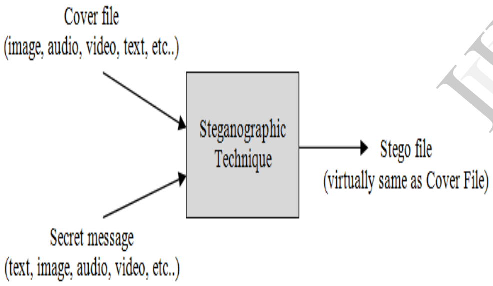
CONCEALING DATA USING AUDIO STEGANOGRAPHY

K. ASHWINI, achuchweety@yahoo.in, M. KEERTHANA, keer22294@gmail.com
MARIA CATHERINE, maria.caterine93@gmail.com
KUMARAGURU COLLEGE OF TECHNOLOGY

ABSTRACT: Steganography is the science of "invisible" communication. The purpose of Steganography is to maintain secret communication between two parties. The secret information can be concealed in content such as image, audio, or video. It is an important part of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies and government. Steganography's ultimate objectives are un-detectability, robustness and capacity of hiding data which are the main factors that separate it from techniques such as watermarking and cryptography. This paper specifically deals with the concealment of secret messages within audio signals and the various techniques used for implementing them.

I. INTRODUCTION

Steganography has a long history of been used as a way to protect security and privacy of valuable information. While cryptography focuses on protecting the secret message by jumbling its content, steganography concerns on protecting the secret message by concealing its mere existence. The concealment of secret messages is achieved by embedding them into other host mediums.


Cover file
(image, audio, video, text, etc..)
Steganographic Technique
Stego file
(virtually same as Cover File)
Secret message
(text, image, audio, video, etc..)

. Fig. 1 Fundamental scheme of steganography process.

Steganographic application can hide different types of data within a cover medium. The resulting stego message contains the hidden information, even though it is seemingly identical to the cover medium. Steganography basically exploits human awareness and observation because human senses are not qualified to seek files that have information hidden inside them, while there are many third party programs can do what is called Steganalysis, which an art of inverse steganography aims to analyze and break a specific steganographic system. Normally, steganography is required where cryptography techniques are ineffective. Generally, all digital mediums, signals, or files can be used in steganography process as cover media, but some formats are more suitable than others depending on the level of redundancy. For instance, text steganography is believed to be the hardest type of steganography because of the low degree of redundancy in text as compared to image, audio or video.

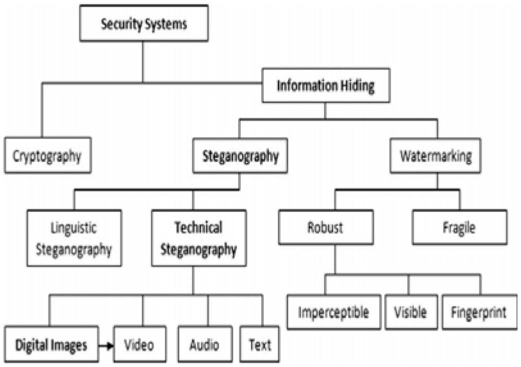


Fig.2 Nomenclature for security systems.

Redundancy can be described as the bits of a media, signal or file that offer accuracy more than needed for the object's use. The redundant bits of an object may also be defined as those bits that can be easily altered without this change being noticed easily. Image, video and audio files in particular fulfil this requirement, while studies have also revealed other file formats that are suitable to be used for information hiding.

II. ANCIENT STEGANOGRAPHY

The word steganography is originally derived from Greek which means ''Covered Writing''. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back. In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany. Five hundred years ago, the Italian mathematician Jerome Cardanre invented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blank so that the message appears as an innocuous text. This method is credited to Cardanand which is called Cardan Grille. It was also reported that the Nazis invented several steganographic methods during World War II such as Microdots, and have re-used invisible ink and null ciphers.

III. THE DIGITAL ERA OF STEGANOGRAPHY

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone ‘‘digital’’. In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh, who proposed a method which resembles embedding into the 4LSBs(least significant bits). They examined image down grading and contamination which is known now as image-based steganography. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern was shown on the possible use of steganography by terrorists following a report in USA TODAY. Cyber-planning or the ‘‘digital menace’’ as Lieutenant Colonel Timothy L. Thomas defined it, is difficult to control. Provos and Honeyman, at the University of Michigan , scrutinized three million images from popular websites looking for any trace of steganography. They have not found a single hidden message. Despite the fact that they attributed several reasons to this failure it should be noted that steganography does not exist merely in still images. Embedding hidden messages in video and audio files is also possible. Examples existing for hiding data in music files, and even in a simpler form such as in Hyper Text Mark up Language (HTML) executable files(.EXE) and Extensible Mark up Language(XML) . This shows that USA TODAY’s claim is not supported by a strong evidence, especially knowing that the writer of the above report resigned about two years later after editors determined that he had deceived them during the course of their investigation.

IV. STRUCTURE OF STEGANOGRAPHY

Given the increased general attention over steganography technique and practices, some common terminology that most of the applications have in common have been discussed and determined. The items are:

Emb (*m*): Some information data or signal to be hidden in other media.
Stego (*s*): The output of the steganography process which is the signal, file or data that has the embedded message hidden in it.
Cover (*c*): The input to the information hiding process which represents the innocent carrier signal or file.
Stego key or simply **key (*k*):** This is additional un-imbedded secret data which may be needed in the information hiding process. In particular, this key is typically needed to extract the embedded message again in the final destination.

In general, steganographic system consists of embedding or encoding phase and extracting or decoding phase.

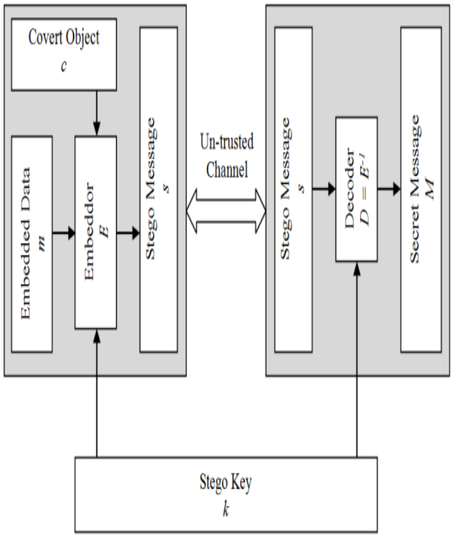


Fig . 3 Steganography terminology.

As illustrated in Figure 3, the embedding process is accomplished by encoding or embedding the secret message into a covert innocent message using a stego key. The result of this process is the stego message which contains both cover and secret messages combined according to the stego key. On the other hand, the decoding phase requires having the same stego key in order to be able to extract the embedded secret data from the stego message. In most steganography techniques, failing to have the stego key will make the process of extracting the secret message almost impossible.

V. OVERVIEW OF AUDIO STEGANOGRAPHY

Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly. 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. The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file. Hiding secret information into digital audio media is generally more complicated than hiding secret information into other media, such as digital images. In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message.

VI. DIGITAL AUDIO SIGNAL

Digital audio signals are different from other traditional analogue sounds in the fact that they are discrete signal rather than continuous ones. Discrete signals are produced by sampling continuous analogue signals at specific rates. For instance, the typical sampling rate for CD digital audio is 44 kHz. Figure 4 below, shows a continuous analog audio signal wave being sampled to create digital audio signal wave.

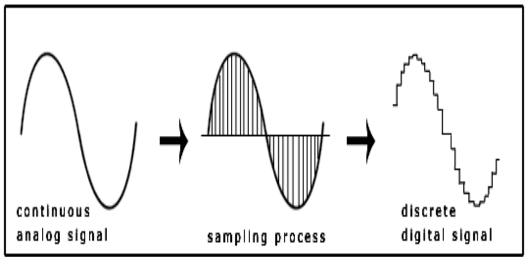


Fig. 4 Sampling of audio signal.

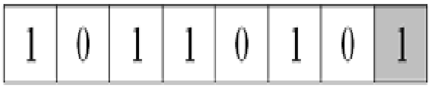
Figure 4 above emphasizes the discrete nature of digital audio signals. Nonetheless, typical sampling rate is generally set at a level in which the produced discrete signal is not imperceptibly distinguishable from the original continuous signal. Digital audio files are stored in computers as a series of 0's and 1's. With a correct tool, it is possible to change the bits that structure a digital audio file. Such accurate controls permit changes to be performed to the binary bits that are not perceptible to the human sense.

VII. METHODS OF AUDIO STEGANOGRAPHY

There are many steganographic techniques for hiding secret data or messages in audio in a way that the modifications made to the audio file are perceptually indiscernible. Several recent methods necessitate previous familiarity with signal processing techniques, Fourier transform, and other high level mathematics areas.

A. LEAST SIGNIFICANT BIT(LSB) CODING:

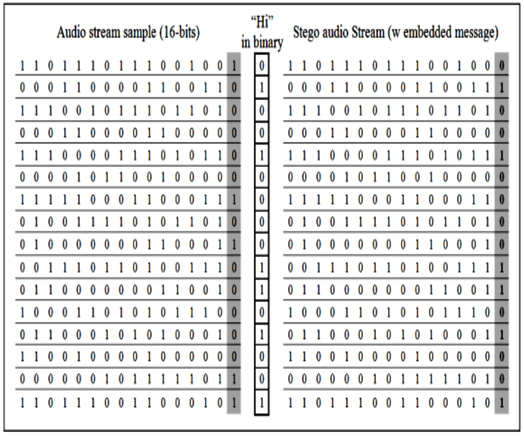
Least significant bit (LSB) coding is the easiest and simplest method to hide secret data in a digital audio media. By replacing the least significant bit of each sample words with a bit of the secret data, LSB coding permits a big size of secret data to be embedded. LSB audio steganography techniques have the same previously discussed advantages and disadvantages of common LSB steganography techniques on other cover media. In computing, the least significant bit (LSB) is the bit in the right most position of a binary number, which also determines whether the number is even or odd. It is equivalent to the least significant digit of a decimal number, which is the ones in the right most position.



1	0	1	1	0	1	0	1

Fig. 5 Binary representation of decimal 181.

Figure 6 illustrates how the message “Hi” is encoded in a 16-bit quality audio sample using the LSB method. Here the secret information is “Hi” and the cover file is an audio file. “Hi” is to be embedded inside the audio file. First the secret information “Hi” and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information “Hi”. The resulting file after embedding secret information “Hi” is called Stego-file.



Audio stream sample (16-bits)	“Hi” in binary	Stego audio Stream (w embedded message)
1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1	0	1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 0
0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0	1	0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1
1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 0	0	1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 0
0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0	0	0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0
1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 0	1	1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1
0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 0	0	0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 0
1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 1	0	1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 0
0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 0	0	0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 0
0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 1	0	0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 0
0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 0	1	0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 1
0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 0	1	0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 1
1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 0	0	1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 0
0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 0	1	0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 1
1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0	0	1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0
0 0 0 0 0 0 1 0 1 1 1 1 1 0 1 1	0	0 0 0 0 0 0 1 0 1 1 1 1 1 0 1 0
1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 1	1	1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 1

Fig. 6 LSB audio coding example.

In LSB coding, the idyllic secret data communication rate is 1 kbps for 1 kHz. In some variations of LSB coding, however, the two least significant bits of a sample word are use to hide two bits secret message data. This increases the capacity of embedded data but also increases the nose and therefore increases risk of being perceptible and eventually breakable. Using LSB is possible, as modifications will typically not create perceptible changes to the sounds. Another method involves taking advantage of human sound system limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks.

B. 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. Fig.7 illustrates the parity coding procedure in detail.

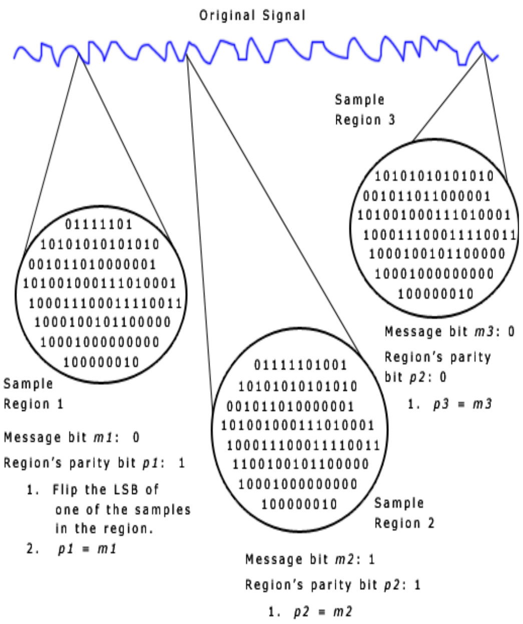


Fig.7 Parity coding procedure.

C. PHASE CODING

Phase coding deals with the weaknesses of the previously discussed audio steganography techniques which induce noises to the medium. Phase coding is based on the reality that, unlike noises, audio phase components are imperceptible to the human ear. Rather than adding noises, this technique encodes the secret data bits to phase shifts in the phase spectrum of the audio signal, attaining inaudible encodings in terms of signal-to-noise ratio.

$$phase_{new} = \begin{Bmatrix} \frac{\pi}{2} & if\ message \quad bit = 0 \\ -\frac{\pi}{2} & if\ message \quad bit = 1 \end{Bmatrix}$$

In phase coding, the phase of an initial audio segment is substituted with a reference phase that represents the data. Following segments phase is modified back to maintain the relative phase between segments. Phase coding, when applicable, is one of the most efficient audio steganographic methods in terms of the signal to noise ratio (SNR). When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. On the other hand, on condition that the alteration of the phase is small enough, an inaudible steganography can be accomplished.

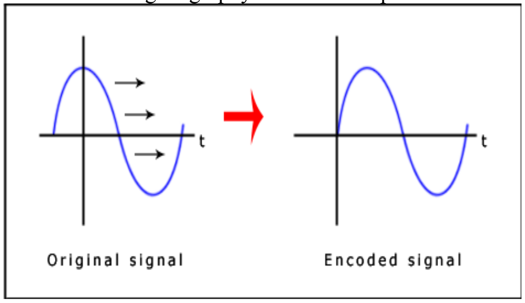
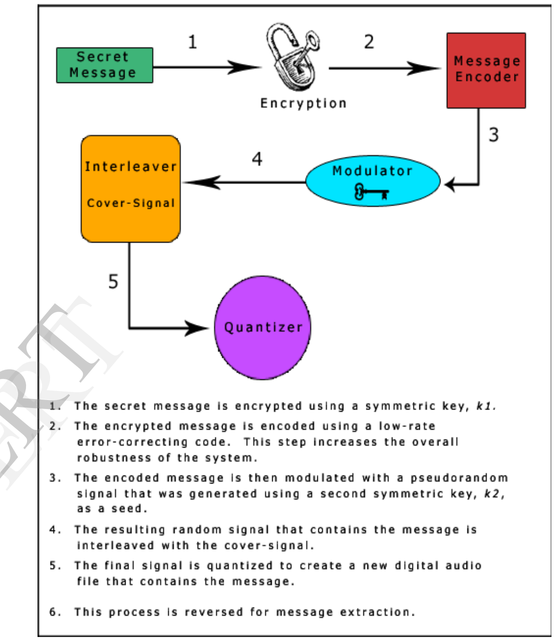


Fig.8 The signals before and after Phase coding procedure.

D. SPREAD SPECTRUM

In the field of audio steganography, fundamental spread spectrum (SS) techniques attempts to distribute secret data throughout the frequency spectrum of the audio signal to the maximum possible level. This is equivalent to implementing LSB coding by spreading the secret data bits over the entire audio signal. However, different from LSB coding, the SS techniques spread the secret bits over the frequency spectrum of the audio media by using a code that is not reliant on the genuine signal. Consequently, the resultant signal will utilize a bandwidth wider than what is essentially needed for communication.



1. The secret message is encrypted using a symmetric key, *k1*.
2. The encrypted message is encoded using a low-rate error-correcting code. This step increases the overall robustness of the system.
3. The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key, *k2*, as a seed.
4. The resulting random signal that contains the message is interleaved with the cover-signal.
5. The final signal is quantized to create a new digital audio file that contains the message.

6. This process is reversed for message extraction.

Fig. 9 Spread spectrum.

Two types of spread spectrum are utilizable in audio steganography: the direct sequence and frequency hopping schemes. In direct sequence spread spectrum, the secret data is distributed using a constant named the chip rate then adapted with a pseudorandom signal and then interleave with the cover signal. In frequency hopping spread spectrum, the frequency spectrum of the audio medium is changed so that it hops quickly among frequencies.

E. ECHO HIDING

In echo hiding techniques, secret data is inserted into an audio medium by introducing an echo into the discrete signal. Similar to SS technique, it also offers benefits as it allows high data communication rates and offers greater robustness compared to the earlier noise-inducing techniques. In order to hide secret message effectively, three echo related factors are involved and changed: amplitude, decay rate, and offset (delay time) from the genuine audio signal. All of those factors should be set

lower than the human hearing threshold in order to keep the echo imperceptible.
Additionally, offset values are changed corresponding to the binary secret data targeted. A specific offset value represents a binary one, and another offset value represents a binary zero. Figure 10 illustrates the echo hiding process.

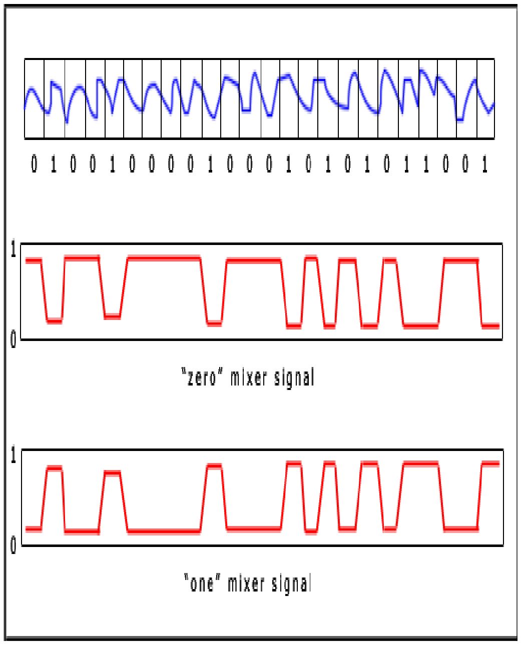


Fig. 10 Echo hiding.

VIII. STEGANOGRAPHY IN REAL TIME AUDIO SIGNALS

Real-time communications (RTC) is any form of telecommunications in which information can be exchanged among the users instantly or with insignificant latency. RTC may occur in half-duplex or full-duplex approaches. Data can be transmitted in both directions on a single carrier simultaneously in full-duplex mode, while in half-duplex RTC data can be transmitted in both directions on a single carrier but not in the same time. Any type of communication, especially digital real-time one, needs to have one or more protocols to control and standardize the communication process among the clients. Generally, theses protocols used to rule the segmentation, framing, sampling, transmission, traffic controlling, receiving, and other main protocol tasks. The protocols used to send the sampled data using packets. Packet payloads are basically encoded multimedia data and they may contain any type of multimedia data. Usually, protocol packets have some extra unused bits mainly for future use purposes as well as for some special situations. It is very useful and practical to hide secret information into these redundant bits allocated in the structure of every packet sent. This provides the ability to modify these bits to hide data without any perceptible change in the encoded multimedia contents. The sample word size, used by different multimedia encoding formats is an important aspect in finding out the maximum amount of available space in the cover medium for hiding the secret information. In general, least significant bits of each word value are probably usable to be modified with no perceptible change in the quality of the multimedia content. Thus, as an example, only half the amount of available space in a16-bit encoded audio cover medium will be available in comparison with a cover medium with an 8-bit word size.
The throughput of the real time communication system is another important factor used to define the performance of any proposed RTC steganography technique. As an example, utilizing the LSB of every sample in some kind of data compression protocol which has the packet size of 160 bytes, a suggested total of 20 bytes of secret data can be successfully embedded. If the throughput of this system is around 50 packets per second unidirectional, this results in approximately 1,000 bytes of full-duplex throughput of secret data within this covert communication channel.

IX. TEST AND EVALUATION

All steganography techniques have to fulfil a few specific and essential requirements. A set of criteria has been proposed to further describe the quality of a steganography algorithm as illustrated in Figure 11 and discussed below.

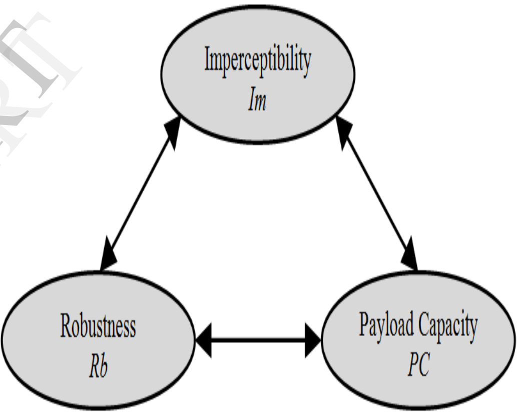


Fig. 11 Steganography requirements.

In this evaluation, since there are a number of sub layers, we think that it is better to measure each requirement separately.

X. IMPERCEPTIBILITY(Im)

The imperceptibility is the most important requirement of a steganography system, as the strength of steganography system depends on its ability to be unnoticed by the human senses (visually or acoustically). If it is noticed that the cover medium has been altered, the steganography
technique or system is not practical anymore. The steganography system is said to be accurately imperceptible only if it is impossible to distinguish the covert data from the hidden secret information. It is sometimes enough that the alterations in the stego message be unobserved, on condition that the embedded message is not compared with the original covert message.

XI. ROBUSTNESS(*Rb*)

Robustness defines how strong the used steganographic technique against changes. It measures the capability of the embedded secret data to endure different types of intentional and unintentional modifications. The hidden embedded message should be very hard to eliminate or modify without altering the quality of the covert medium. It is important for steganography techniques to be robust against both intentional and unintentional modifications to the message. Many steganography techniques leave some kind of 'signature' when embedding the secret information. Typically, these signature data can be easily identified using statistical analysis. It is necessary that a steganography algorithm does not leave such a mark in the covert medium in order to be able to avoid and pass by such statistically analysis without being detected. In the communication of a stego message by reliable systems, the message may go through manipulations in an attempt to remove potential hidden information. Data manipulation, such as compression or rotating, might be applied to the message prior reaching its final destination. Depending on the manner in which the message is embedded, these manipulations may or may not destroy the hidden message depending on the method or technique used to hide the secret message.

XII. PAYLOAD CAPACITY(PC)

Payload capacity is the size of embedded data that can be hidden into a particular innocent cover medium relative to the size of this medium. The real challenge is how to hide as much secret data as possible while keeping the quality of the medium untouched and without infringe the imperceptibility requirement. Generally, increasing the embedding capacity makes the secret hidden information more conspicuous in viewing. To calculate the embedding capacity of a particular steganography system, the size of the embedded secret message is divided by the total size of the cover medium.

$$\text{Payload Capacity} = \frac{\text{Total number of bits of hidden data}}{\text{Total number of bits of cover file}}$$

XIII. REAL TIME SUITABILITY(RTS)

Steganography in real time audio signals involves additional requirements such as system complexity, throughput, bandwidth, delay, absence of duplications, failure recovery, and service setup time. These requirements directly affect the real time communication process, and hence, may have influences on the real time steganography processes.

XIV. CONCLUSION

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. Although some data hiding techniques have been proposed by various researchers, the specific requirements of each data hiding technique vary from one application to another; with each of these techniques have some advantages and disadvantages. 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.

XV. REFERENCES

1. Zamani.M, Manaf.A. ; Ahmad, R.B. ; Jaryani, F. ; Taherdoost, H. ; Zeki, A.M.: A Secure Audio Steganography Approach, IEEE Xplore (2009).
2. Langelaar, G.C., I. Setyawan, and R.L. Lagendijk, Watermarking digital image and video data. A state-of-theart overview. Signal Processing Magazine, IEEE, 2000.
3. Gopalan, K. and S. Wenndt, Audio Steganography for Covert Data Transmission by imperceptible Tone Insertion. in Proc. The IASTED International Conference on Communication Systems and Application (CSA 2004),Banff, Canada.
4. Bhattacharyya, D., et al., Hiding Data in Audio Signal. Advanced Communication and Networking, C.-C. Chang, et al., Editors. 2010, Springer Berlin Heidelberg. p. 23-29.
5. Cvejic, N., Seppanen, T: Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, In: Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC(2004).
6. Aravind Kumar, KM. Pooja, Steganography- A Data Hiding Technique, research paper, International journal of Computer Applications(0975-8887) volume9-no.7, November 2010.
7. Ross J.Anderson, Fabien A.P Petricolas, In The Limits Of Steganography, IEEE Journel May-1998.