Efficient and Secured Audio Steganography with Text Message

Priyanka Sengar[1], Prof. Bhupchandra Kumhar[2]

[1]*M-Tech Research Scholar,* [2]*Research Guide & HOD,*

Department of Computer Science and Engg. IES College of Science & Technology, Bhopal

Abstract - The security of the information is first and foremost need while transmitting from one place to another place or stored somewhere. Steganography is the art of hiding messages inside an image file/Audio file or a Video file such that the very existence of the message is unknown to third party. Cryptography is used to encrypt the data so that it is unreadable by a third party. Such techniques will facilitate various secret information sharing strategies. From the outcomes it is also clear technique has no effect on audio quality even after information hiding.

Keywords - Audio, Speech, Steganography, Secret Information.

I. INTRODUCTION

In this electronic era, in which computers, a digital medium, are its main protagonists, and more with the birth of digital storage devices, as compact discs, the processes of digitalization of analog signals, the processes which take as input an analog signal (with continuous domain and range) and produce as output a digital signal (with discrete domain and range) are living a great growth. But, with the relentless advance of the Internet, in which unlike in computers themselves (for which it is said that memory is "free") we have the need to care about reducing as much as possible the amount of data to transmit due to the current limitations of bandwidth. So, now it is not enough just to digitalize the analog signals: now we have to remove from the signals every single component that is not indispensable, everything that, if removed, will produced a notable loss in the signal quality. To the influence made by the Internet we have to add the one made by the audio players, commonly known as mp3 players due to the first (or at least the first to be globally known) compressed audio format.

Here we'll carry out a brief study of the main elements which take part in the audio signals processing and coding, and also the main properties of the Human Auditory System (HAS) which let us differentiate the indispensable components from the dispensable ones and which have helped to and create more efficient audio compression algorithms and formats. The purpose of this part is to present certain necessary principles needed to the next parts. Therefore, despite signal processing and coding is a very complex and advanced science, we won't spend as much time as will be necessary to get a deep knowledge of the aspects here introduced. For a deeper study on the matters dealt in the following chapters, we recommend the reader to consult references therein.

Until now he have spoken about steganography as a set of methods for hiding information. Strictly speaking this is not a hundred percent correct definition, as the set of methods used to hide information is in fact called information hiding methods, being steganography a subset of them. Information hiding is the science that includes any method that serves for hiding any type of information, whatever its nature is, its means, or its purposes. Therefore, inside the information hiding we can speak of watermarking, which consists in introducing little amounts of information to serve as copyrights to protect authors' rights; fingerprints, also small amounts of information but this time with the purpose to identify a concrete object, in a way that afterwards it is possible to trace a chain of illegal copies to the original source (a technique known as traitor tracing [34]; the steganography, strictly speaking, focuses in transmitting high amounts of information in an imperceptible manner, although less robust; and yet another field, totally different, but still information hiding, is the anonymity, which with techniques like Onion Routing allows the original sender of a given information to hide his identity to the recipient.

Each one of the mentioned information hiding branches has its characteristics in terms that we'll see next (robustness, capacity...) and that made certain algorithms more or less appropriate to achieve the desired purpose. In the last years, information hiding techniques have been subject to a great increase due to some factors tightly related to the digital information.

Obviously, and like for practically every science branch, all information hiding applications may have legitimate and illegitimate uses, although not for every case the division is quite clear. Of course, the use that the terrorist organizations is totally undesirable, what makes the advancements in the countermeasures (steganalysis, i.e., the techniques that study how to break or cancel steganography effects) to be a very important element for intelligence and defense services. In other situations, like the inclusion of watermarks or fingerprints into songs or videos to avoid illegal copies, the border between what is right and wrong is much fuzzier (the majority of the

authors and disco graphic companies consider wrong, while the majority of the consumers have a much more relaxed concept of illegality). Whatever the case is, it is not the objective of this work to analyze ethical questions, although, in the other hand, science advancement is difficult to avoid, so all this ethical digressions may not lead to fruitful completions. Therefore, and leaving aside all this matters, we'll introduce here the terminology, characteristics and methods of steganography, studying the most relevants in a little more detailed level.

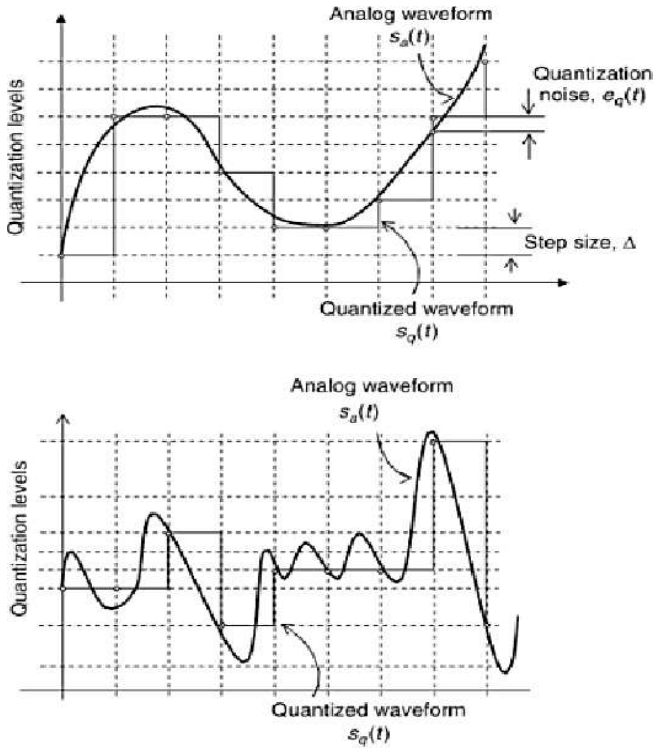


Fig 1.1: Examples ([40]) of uniform (up) and not uniform (down) quantization of an analog signal.

II. ANALOG SIGNALS DIGITALIZATION

So we have a real valued signal in continuous domain that, because of all this of the digital world, we want to transform into a signal of discrete domain also with discrete values. The process by means of which we choose what instants of the continuous time domain we are going to represent in the new discrete time domain is called sampling. The PCM technique and its derivatives are techniques of scalar quantization, i.e., a single sample is quantified per time, while in vector quantization several samples composing a vector are quantified per time. In this sense, we can think of the signal as being divided in blocks of N samples, represented by N-dimensional vectors, and with a codebook available, with L entries also of N dimensions, we will assign the input vector the codebook which minimizes some measure, known as distortion, which can be, e.g., the MSE (Mean Squared Error, the square of the difference of two vectors) in a N-dimensional space.

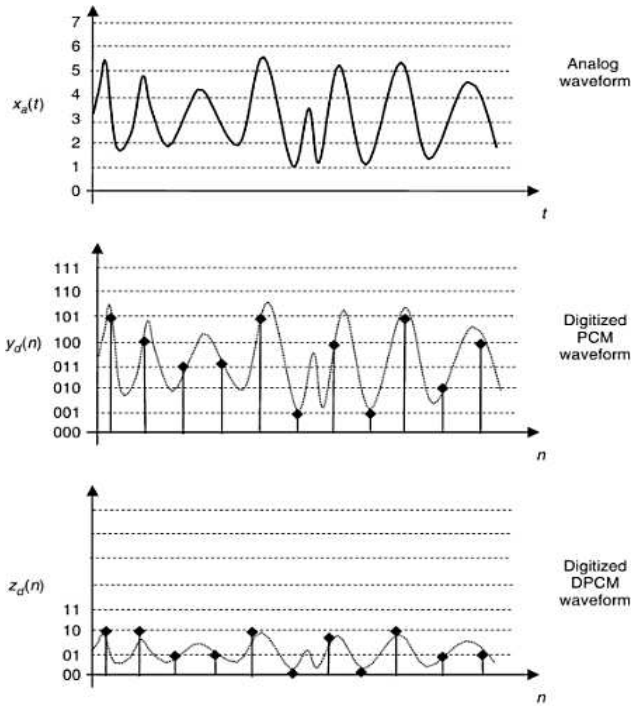


Fig 1.2: Examples ([40]) of PCM (center) and DPCM (down) of an analog signal.

It is quite common to chain several vector quantization processes, giving place to structures with different hierarchies (sequential, trees ...). For example, in the so called multi-step vector quantization, several vector quantizers are sequentially chained, quantizing with the first one the input vector, and with the following the error committed by the immediately previous quantizer.

III. PROPOSED MODEL

For the better Steganography in audio signal we have proposed a methodology to significantly improve the peak signal to noise ratio even after hiding information in audio signals.

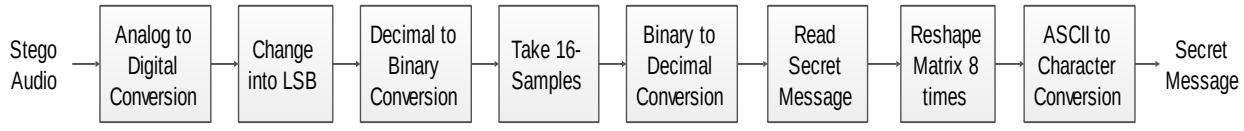


Fig. 1.3 Block Diagram of the Embedding Process

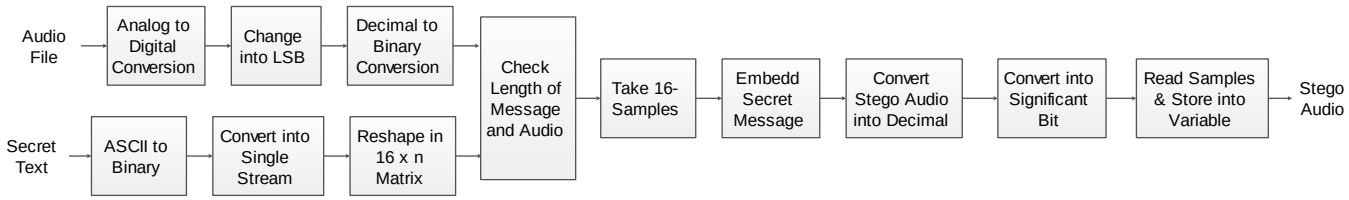


Fig. 1.4 Block Diagram of the Extraction Process

Fig. 1.5 Flow Chart of the Embedding Process

The block diagram of the proposed system is shown below. The complete system has two modules first is embedding of secret information behind audio signal and getting stego audio, second is extraction of secret information from the stego audio signal.

The execution proposed methodology is explained with flow chart shown in figure 1.5 and 1.6. Fig. 1.5 shows the embedding process of the secret message behind audio signal where have to exercise bunch of matrix operations and conversion process to get the stego audio which means the audio signal with secret message have in it.

Fig. 1.6 shows the extraction process of methodology. Where we extract the secret information hidden in stego audio signal. The extracted information should be as same as embedded with audio otherwise there is no use of the methodology if we lose information.

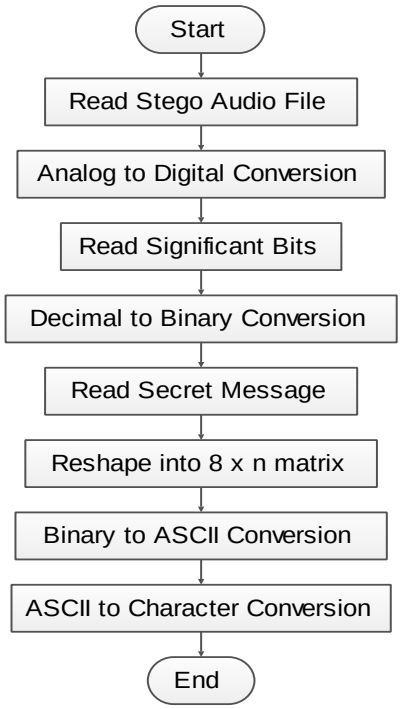


Fig. 1.6 Flow Chart of the Extraction Process

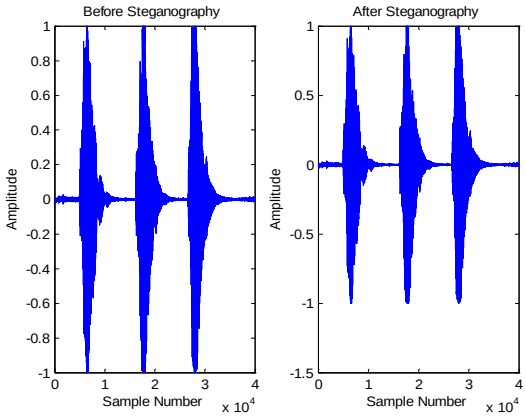
IV. SIMULATION RESULTS

The proposed methodology mentioned in previous section has been implemented and the PSNR is calculated for each audio file after steganography.

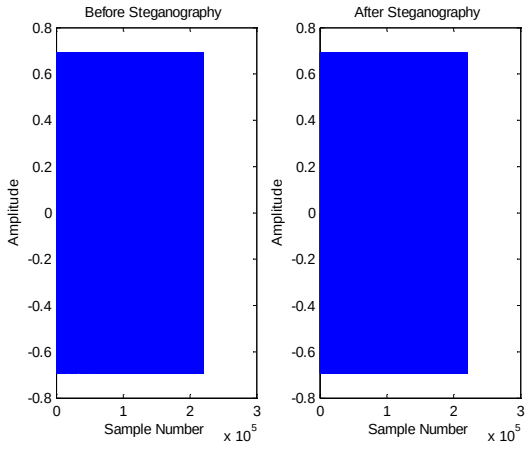
Table 1: Comparison of PSNR Values

Audio File	Audio File Size	Secret Message Size	PSNR Value
1.wav	79 KB	3 KB	89.94 dB
2.wav	435 KB	3 KB	100.16 dB
3.wav	108 KB	3 KB	49.76 dB
4.wav	184 KB	3 KB	54.31 dB
5.wav	71 KB	3 KB	44.34 dB
6.wav	30 KB	3 KB	40.44 dB
7.wav	75 KB	3 KB	41.70 dB
8.wav	41 KB	3 KB	46.07 dB
9.wav	119 KB	3 KB	51.73 dB
10.wav	40 KB	3 KB	45.65 dB

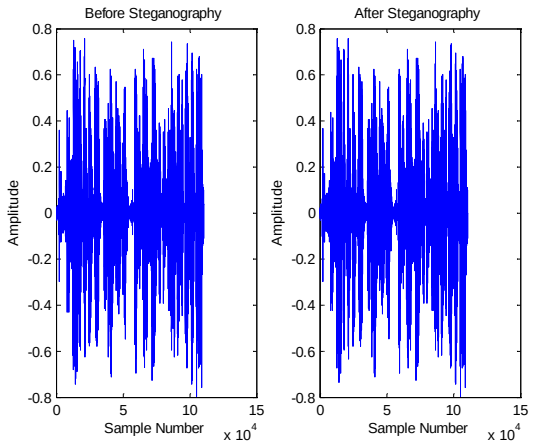
Peak signal-to-noise ratio (PSNR) is a parameter used to calculate the quality of reconstruction of Loss compression example: for image compression. A signal in this case is the original data, and the noise is the error introduced by compression. In Table 1 we take different size of audio files with same secret message and get different PSNR values.



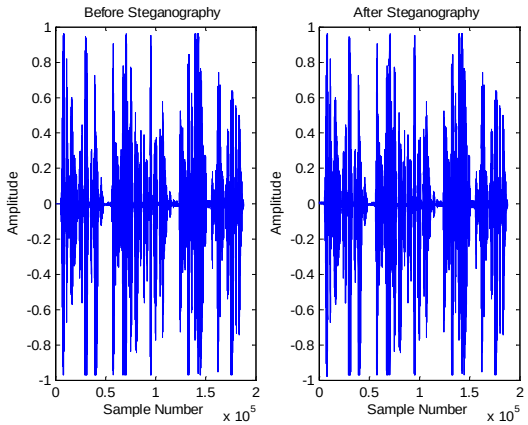
(a)



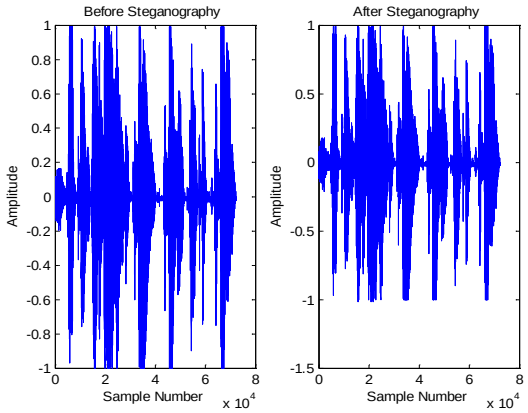
(b)



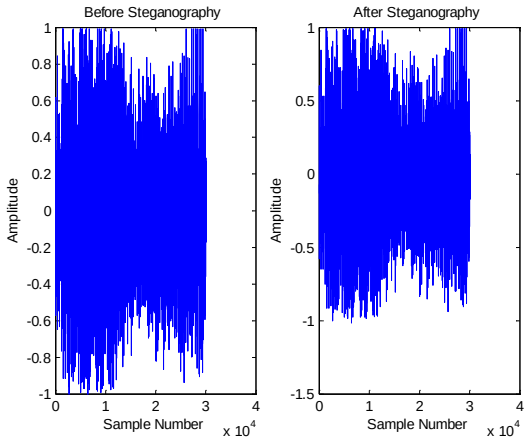
(c)



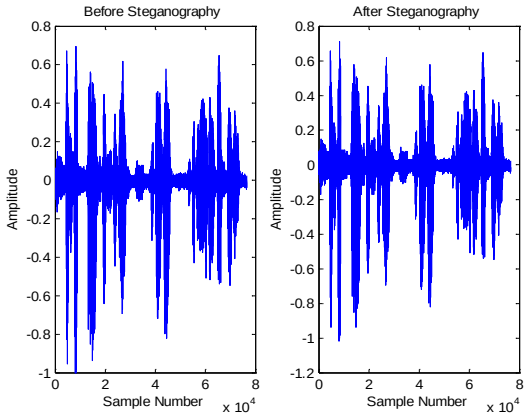
(d)



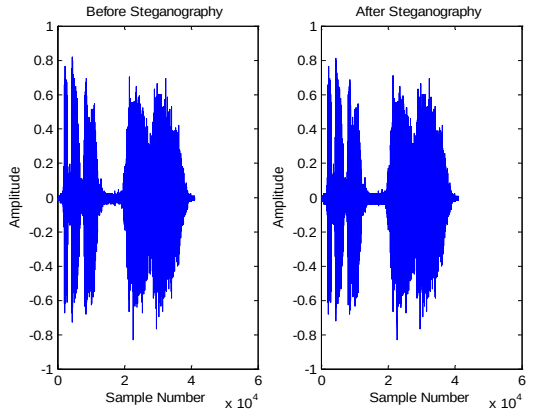
(e)



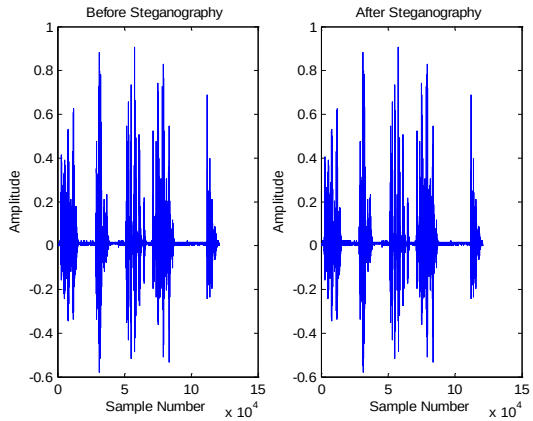
(f)



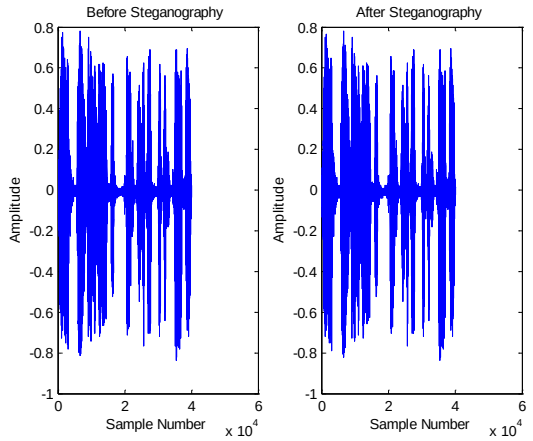
(g)



(h)



(i)



(j)

Fig. 1.7 (a) to (j) are waveforms of the audio signals before and after steganography the respectively from file 1.wav to 10.wav.

The audio file before and after hiding the image into the audio file sounds same. It means there is no audible difference in audio file before and after hiding the data in to file.

V. CONCLUSION AND FUTURE SCOPE

The proposed method is analyzed and we can say that the audio steganography without losing significance audio quality is better over previous methodologies and has better capacity to hide information then existing methodologies. The proposed method can be utilized to share very secret information. The security aspects can also be increased with the increase in multi stage security methodologies.

REFERENCES

[1] Gupta, N.; Sharma, N., "Dwt and Lsb based Audio Steganography", Process of IEEE Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.428,431, 6-8 Feb. 2014.

[2] Bugár, G.; Bánoci, V.; Broda, M.; Levický, D.; Dupák, D., "Data hiding in still images based on blind algorithm of steganography" Radioelektronika (RADIO ELEKTRONIKA), In proc. 24th IEEE International Conference , vol., no., pp.1,4, 15-16 April 2014.

[3] Geethavani, B.; Prasad, E.V.; Roopa, R., "A new approach for secure data transfer in audio signals using DWT" In Proc. IEEE Advanced Computing Technologies (ICACT), 15th International Conference on , vol., no., pp.1,6, 21-22 Sept. 2013.

[4] Khademi, Mahdi; Tinati, M.A., "Audio steganography by using of linear predictive coding analysis in the safe places of discrete wavelet transform domain" In Proc. IEEE Electrical Engineering (ICEE), 19th Iranian Conference on , vol., no., pp.1-5, 17-19 May 2011.

[5] Zhang Kexin, "Audio steganalysis of spread spectrum hiding based on statistical moment" In Proc. IEEE Signal Processing (ICSPS), 2nd International Conference on , vol.3, no., pp.V3-381,V3-384, 5-7 July 2010.

[6] Cairong Li; Wei Zeng; Haojun Ai; Ruimin Hu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM" In Proc. IEEE Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09. International Conference on , vol.1, no., pp.240,243, 25-26 April 2009.

[7] Wang Junjie; Mo Qian; Mei Dongxia; Yao Jun, *"Research for Synchronic Audio Information Hiding Approach Based on DWT Domain"* In Proc. IEEE E-Business and Information Scheme Security. EBISS '09. International Conference on , vol., no., pp.1,5, 23-24 May 2009.

[8] Johnson N & Jajodia S, Steganalysis: *the investigation of hidden information*. In: Proc. IEEE Information Technology Conference, Syracuse, NY, p 113–116, 3 Sept. 1998.

[9] Katzenbeisser S & Petitcolas F, *Information Hiding Techniques for Steganography and Digital Steganography*. Artech House, Norwood, MA. 1999.

[10] Bender W, Gruhl D & Morimoto N, Anthony lu, *"Techniques for data hiding"*. IBM Journal 35(3): p 313–336,1996.