Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

GA Based Audio Steganography

Abhishek Kumar
M tech(IT),CDAC
Noida, India

Ramneet S Chadha
Computer Sc. & Engg, CDAC
Noida, India

Chandra Prakash Shukla
M tech(IT),CDAC
Noida, India

Abstract: Steganography is an ancient art. It is used for security in open systems. It focuses on hiding secret messages inside a cover medium. The most important property of a cover medium is the amount of data that can be stored inside it without changing its noticeable properties. There are many sophisticated techniques with which to hide, analyze, and recover that hidden information.

An encoding mechanism is used for embedding the message into the audio file with an exploration use of Genetic Algorithm operators on the cover medium. We worked with audio as cover medium with the aim of increasing robustness and capacity of hidden data. Elitism is used for the fitness function. The model presented here is applied on text files, though the idea can also be used another file types. The quality of the audio file after encoding remains unaffected. An Asymmetric Encryption algorithm, RSA was also used to ensure greater security.

Keywords: Steganography; LSB; Genetic Algorithm.

I. INTRODUCTION

With the widespread use of Internet and wireless networks, and the blooming growth in consumer electronic devices and advances in multimedia compression techniques, multimedia streams are easily acquired nowadays. In an attempt to ensure protection of the a fore mentioned multimedia contents and effective hiding of additional data into such digital content, several techniques emerged. steganography is one of the techniques. The term steganography comes from Greek word as “stegos” means “cover” and “grafia” means “writing” means “covered writing”[1]. Steganography is the art and science to hide in a cover media such as text, audio, video, etc[2] Steganography is a technique used to transmit hidden information by modifying an audio signal in a imperceptible manner[3].

Steganographic techniques are a very important part of the future for security and privacy on internet because important data can be hidden inside a cover medium so that only the parties intended to get the message knows that a secret message exists. The message is being hidden in such a way that the existence of secret message is unknown to the observer and the carrier signal is modified in an imperceptible manner [4]. Many different medium have been employed to embed messages for example images, audio, and video as well as file structures. The resulting media after the text message has been hidden in cover medium is called stego object.

II. PROPOSED METHODOLOGY

Fig 1 and fig 2 represents the complete working of the proposed audio stegnography process for embedding and extraction of the secret data (text file) in a audio file (carrier file).

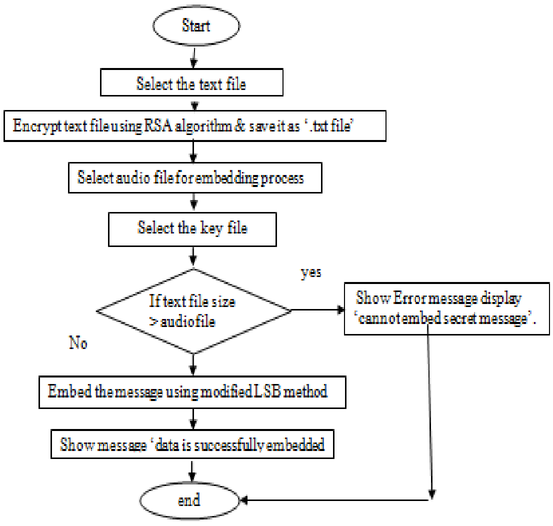

Start
Select the text file
Encrypt text file using RSA algorithm & save it as ‘.txt file’
Select audio file for embedding process
Select the key file
yes
If text file size > audio file
Show Error message display ‘cannot embed secret message’.
No
Embed the message using modified LSB method
Show message ‘data is successfully embedded
end

Fig 1: Embedding Process

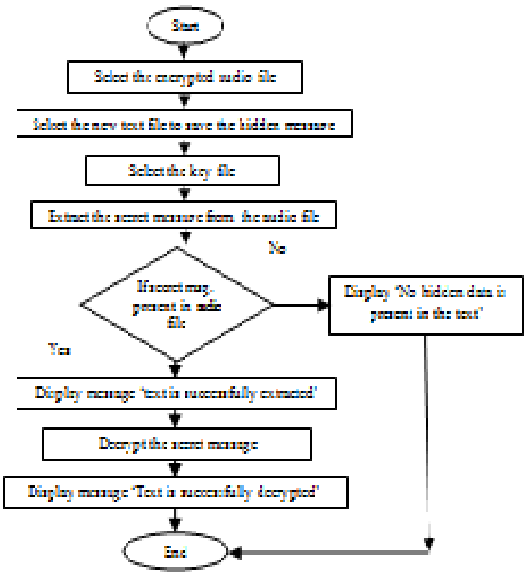

Start
Select the encrypted audio file
Select the new text file to save the hidden message
Select the key file
Extract the secret message from the audio file
No
If secret msg. present in audio file
Display ‘No hidden data is present in the text’
Yes
Display message ‘text is successfully extracted’
Decrypt the secret message
Display message ‘Text is successfully decrypted’
End

Fig2: Decryption Process

At the sender side, the text file which has to be embedded into an audio file is encrypted using Asymmetric key encryption algorithm (RSA) . The cipher text obtained is then embedded in the LSB bit using one of the Steganographic algorithms, LSB algorithm. The resultant audio file contains the secret message embedded into it.

On the receiver side, the embedded audio file is selected to extract the secret message. The secret message is decrypted using RSA decryption method and the secret messages are compared before embedding and after embedding. Also, comparisons are made based on PSNR of both original audio file and embedded audio file, to indicate that less noise intrusion even after changing the random position at LSB bit of the original wave file.

III. LITERATURE SURVEY

Audio steganography is the technique of hiding information inside an audio signal. In an 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.

There are several methods are available for audio steganography. Some of them are as follows:

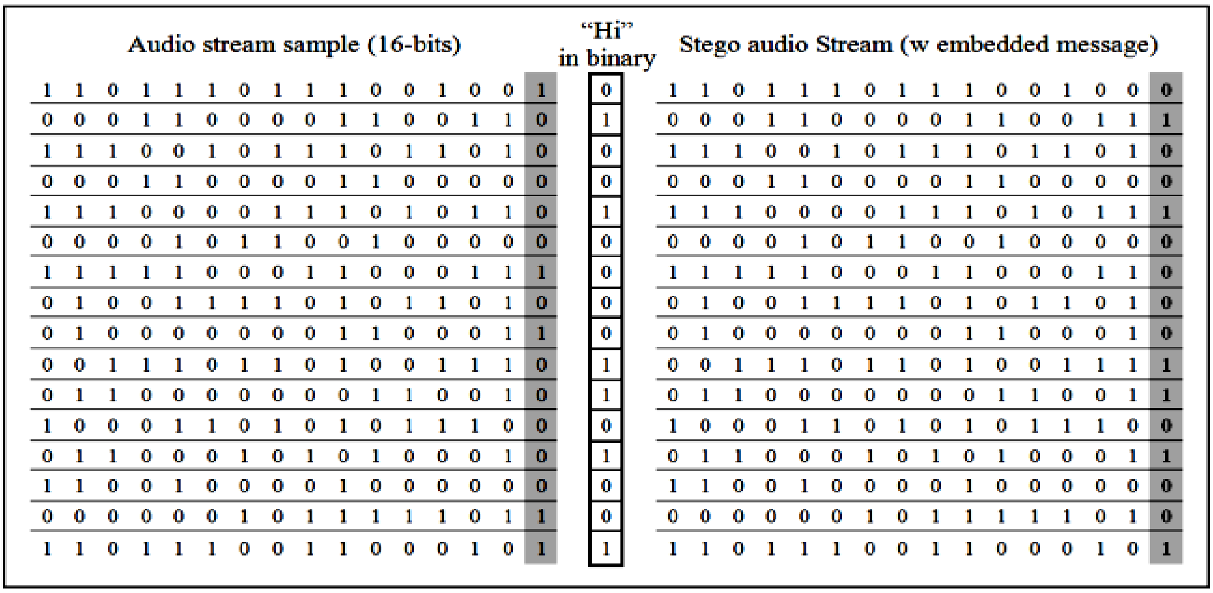
1. LSB Coding
2. Parity Coding
3. Phase Coding
4. Spread Spectrum

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.

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 digit in the ones (right-most) position.

Figure 3 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 [5]



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. 3 LSB audio coding

IV. EXPERIMENT ANALYSIS AND RESULTS

Different experiments were conducted to prove that the proposed method of embedding audio file.The following experiments was conducted on the same data and different data.

1. Same audio file is embedded with different text file with varying text content sizes.
2. Different audio files of different time durations are taken and embedded with same text content.
3. Different categories of audio file are considered and embedded with same text content.

In all the cases, SNR (Signal to Noise Ratio) and PSNR (Peak; Signal to Noise Ratio) area calculated. Figure 4 shows the original audio file before embedding process and Figure 5 shows the audio file after embedding process. The results show that the size of the audio file remains same even after embedding the secret message.

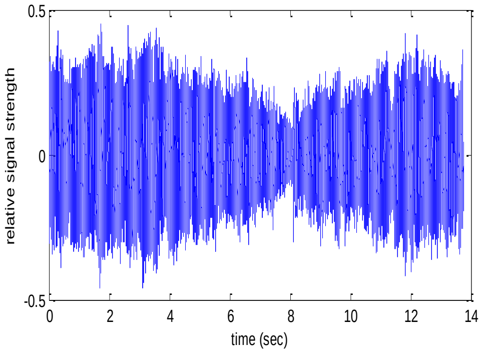


Fig 4: original Wave File

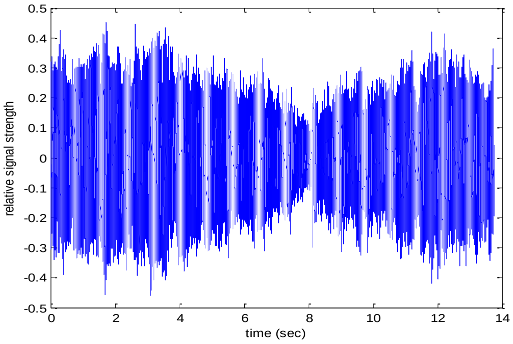


Fig 5: embedded Wave File

The results of the experiment have been tabulated in Table I & Table II respectively and their graphical representations of the same in Figure6 and Figure7 respectively.

Table I. SNR/PSNR Values For Same Audio File With Varying Text Content Sizes

	AUDIO FILE DURATION: 60 Sec		
File name	**Size(byte)**	**SNR**	**PSNR**
Text1	110 byte	1.0e-004 *	131.1512
Text2	100 byte	1.0e-005 *	131.9635
Text 3	75 byte	1.0e-005 *	133.3465
Text 4	50 byte	1.0e-005 *	134.7979
Text5	25 byte	1.0e-005 *	137.8777

Table II. SNR/PSNR Values For Different Categories Of Audio File With Same Text Content

	AUDIO FILE SIZE : 2-4 MIN		
File name	**Size(byte)**	**SNR**	**PSNR**
Classical	100	1.0e-007 *	141.9802
Hiphop	100	1.0e-007 *	141.3117
Jazz	100	1.0e-006 *	140.2171
Pop	100	1.0e-006 *	142.1379
Rock	100	1.0e-007 *	140.9060

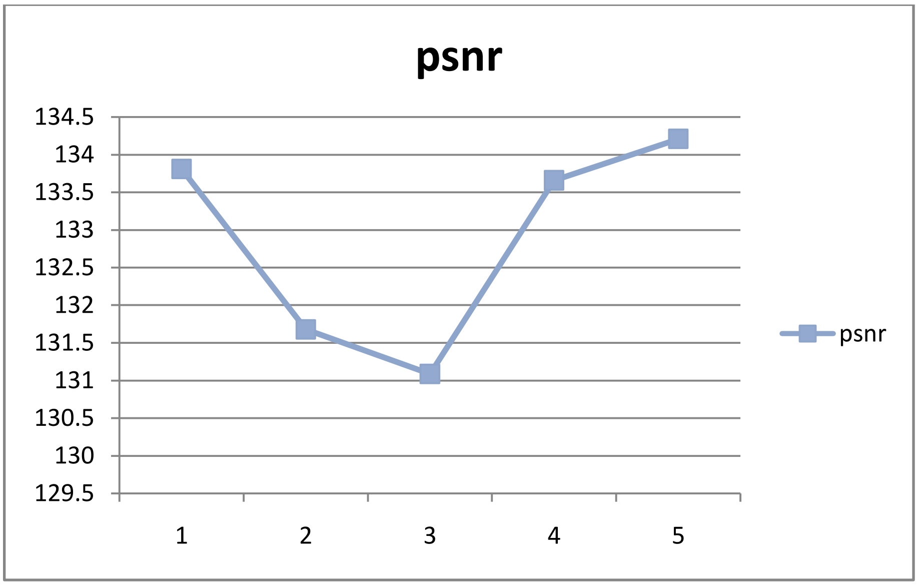


Fig 6 .Graphical Representation For Different Audio Files Of Different Time Durations With Same Text content

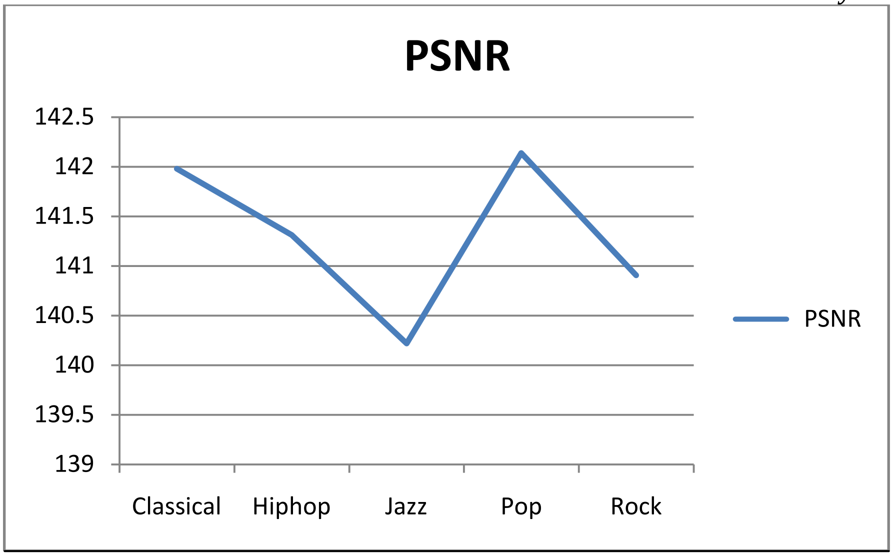


Fig7.Graphical Representation For Different Categories Of Audio File With Same Text Content

By these details we can see that the SNR and PSNR values reduce as the file size increases, indicating that weak noise is not harmful to the changed bits at random places.

VI. CONCLUSION

The proposed system is considered to be an efficient method for hiding text in audio files such that data can reach the destination in a safe manner without being modified. Using the method of embedding text in the 4th and 5th layer with same data and different data along with the encryption and decryption of the secret message using public key cryptographic algorithm, makes data more secure and transparency is minimized.

VII. FUTURE ENHANCEMENTS

Future Scope of this paper is the possibilities of improvements in audio steganography system with respect to different technique of data hiding in audio. This paper mainly concentrates on only .wav format of audio files and can extended to a level such that it can be used for the different types of audio wave file formats like .au, .mp3, wma etc., Also noisy audio files can be considered for making comparisons of SNR and PSNR after embedding message into the same.

REFERENCES

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

[2] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, “High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm”, Proceedings of the International MultiConference of Engineers and Computer Scientists Vol. 1, 2011.

[3] Zamani, M., Manaf, A.A., Ahmad, R.B., Zeki, A.M., & Abdullah, S. (2009) A genetic-algorithm-based approach for audio steganography. World Academy of Science, Engineering and Technology, 54.

[4] Westfeld A. and Pitzmann A. "Attacks on Steganographic Systems". Lecture Notes in ComputerScience, vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[5] A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation
Abdulaleem Z. Al-Othmani1, Azizah Abdul Manaf and Akram M. Zeki

[6] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, “A Genetic Algorithm Based Approach for Audio Steganography”, World Academy of Science, Engineering and Technology 54 2009.