ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers

Padmashree G, Venugopala P S

***Abstract*— Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Audio steganography is a young branch of this discipline. An encoding mechanism is used for embedding the message into the audio file. I used the 4th Bit LSB method to do it. The quality of the audio file after encoding remains unaffected. A public key cryptographic algorithm, RSA was also used to ensure greater security.**

***Index Terms*— Steganography, Audio Data Hiding, LSB Algorithm, Cryptography, RSA.**

I. INTRODUCTION

People use cryptography to send secret messages to one another without a third party overseeing the message. Steganography is a type of cryptography in which the secret message is hidden in a digital picture. While cryptography is preoccupied with the protection of the contents of a message or information, Steganography concentrates on concealing the very existence of such messages from detection.

The term Steganography is adapted from the Greek word *steganographia*, meaning "covered writing" and is taken in its modern form to mean the hiding of information inside other information. Naturally these techniques date back throughout history, the main applications being in couriering information during times of war.

With the invention of digital audio and images files this has taken on a whole new meaning; creating new methods for performing "reversible data hiding" as it is often dubbed. This has many possible applications including the copyright watermarking of audio, video and still image data. In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another.

Steganographic algorithms can be characterized by a number of defining properties. [2] Three of them, which are most important for audio Steganographic algorithms, are Transparency, Capacity and Robustness.

In the proposed system, all these properties are taken into consideration and care is taken for not having too much quantization error, which makes stegnography more secure. By embedding secret message at the 4th bit reduces embedding distortion of the host audio.[1] Similarly, embedding at the 4th and 5th bit LSB of the original audio file with same data and different data also reduces distortion of the host audio.

The paper is organized in the following manner. Section 2 describes the proposed system where audio steganography has been implemented. Section 3 deals with the literature survey of Steganographic methods. Section 4 describes the methodology that has been implemented in this paper. Experimental results are described in section 5. Section 6 contains some concluding remarks of the experiments conducted.

II. PROPOSED SYSTEM

Figure 1 and figure 2 represents the complete working of the audio stegnography process of embedding the encrypted secret message using public key cryptographic algorithm, RSA into the 4th and 5th layers of the audio file.

In the sender side, the text file which has to be embedded into an audio file is encrypted using public key cryptographic algorithm, RSA. The cipher text obtained is then embedded in the 4th AND 5th 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 4th and 5th LSB bit of the original wave.

SENDER

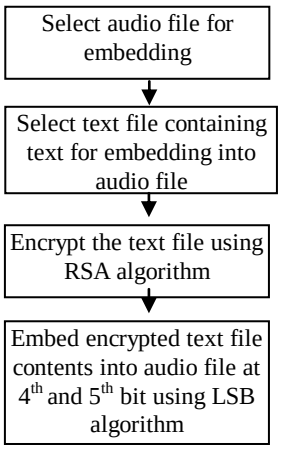

Fig .1: Sender

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

RECEIVER

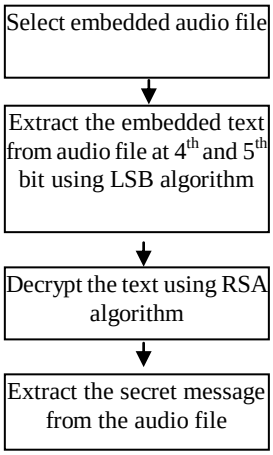

Fig.2: Receiver

III. LITERATURE SURVEY

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio 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

LSB Coding [5]

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. Figure 3 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method.

In LSB coding, the ideal data transmission rate is 1 kbps per 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.

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would-be attacker will suspect secret communication.

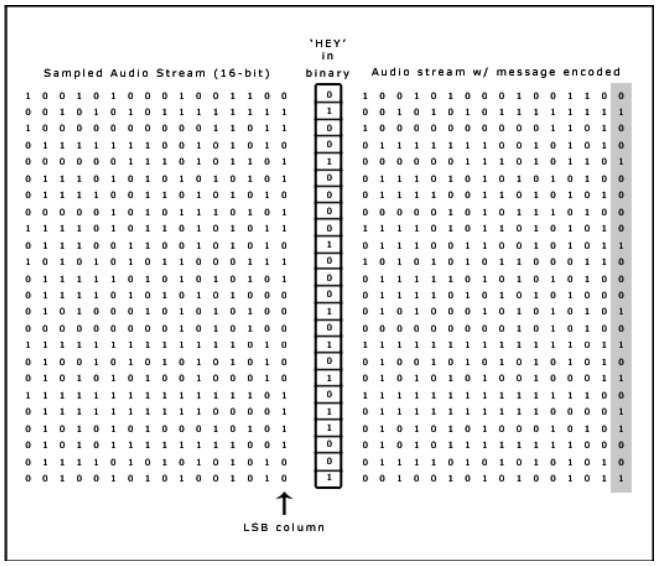

Fig.3. Message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method

IV. PROPOSED METHODOLOGY

A. Algorithm For Embedding Text File Content Into Audio File At The Sender Side. [12]

Step1: Select the audio file for embedding the secret message.

Step2: Play the audio file so that it sounds clear to the end user.

Step3: Select the text file containing the secret message.

Step4: Encrypt the text file contents.

Step5: Compare text file and audio file size.

If text file size > audio file contents

Error message displayed indicating cannot embed secret message.

Else

Embed secret message in the audio file in the 4th and 5th LSB bit of every sample.

Step6: Display message to user of the new audio file created after embedding secret message.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

*B. **Algorithm For Extracting The Embedded Text From Audio File At The Receiver Side.*** [4]

Step 1: Select the new audio file for extracting the secret message.

Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.

Step3: If secret message present in audio file

Then

Display message to end user after extracting message.

Else

Display that no hidden data is present in the text.

Step4: Decrypt the secret message.

Step5: Display message to end user after decrypting the message.

C. Compare PSNR and SNR of the original and embedded audio files and display their values respectively.

V. RESULTS

Different experiments were conducted to prove that the proposed method of embedding audio file. [1] The following experiments were conducted by modifying the 4th and 5th bit LSB with 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 the text content and Figure 5 shows the audio file after embedding the text content. The results show that the size of the audio file remains same even after embedding the secret message.

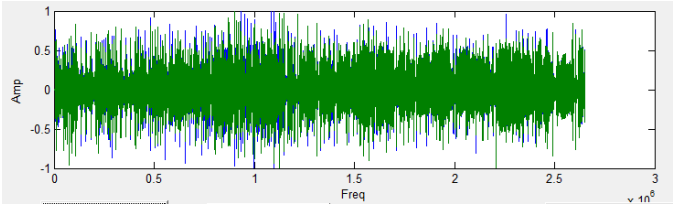

Fig. 4 .Original audio file

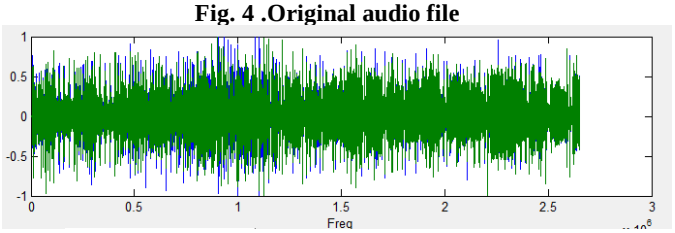

Fig. 5 .Embedded audio file

The results of the experiment conducted by changing the 4th and 5th LSB bit with same data have been tabulated in Table I, Table II and Table III and their graphical representations of the same in Figure 6, Figure 7 and Figure 8 respectively.

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

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
Text1	103	-2.22E-08	16.66214531
Text2	100	-2.19E-08	16.66214531
Text3	75	-2.17E-08	16.66214531
Text4	50	-2.17E-08	16.66214531
Text5	25	-2.24E-08	16.66214531

Table II .SNR/PSNR Values For Different Audio Files Of Different Time Durations With Same Text Content

	Text File size :103 Bytes		
File Name	Duration (sec)	SNR	PSNR
Sample_15	15	-1.25E-07	17.50264063
Sample_30	30	-4.83E-08	17.16767049
Sample_60	60	-2.19E-08	16.66214531
Sample_80	80	-1.65E-08	16.6129556
Sample_90	90	-1.47E-08	16.61077829
Sample_100	100	-1.30E-08	16.63435136

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

.	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
HARDCORE	103	2.58E-06	11.2635686
HIPHOP	103	2.02E-06	10.98351
JAZZ	103	-9.66E-09	17.719165
METAL	103	-2.52E-08	10.6906624
POP	103	-3.38E-08	10.4659678
ROCK	103	-6.97E-08	13.5509855

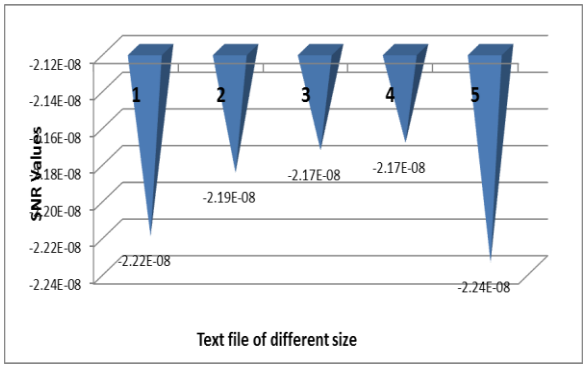

Fig 6.Graphical Representation For Same Audio File With Varying Text Content Sizes

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

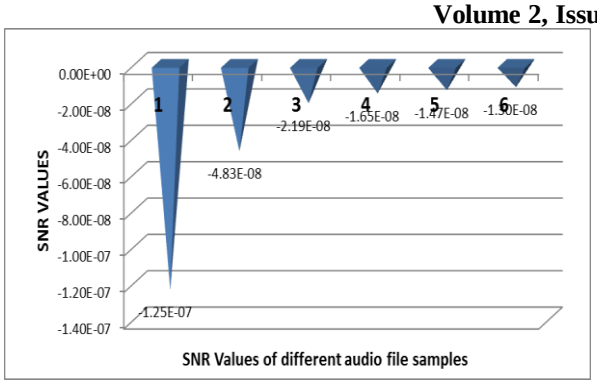

Fig 7 .Graphical Representation For Different Audio Files Of Different Time Durations With Same Text Content

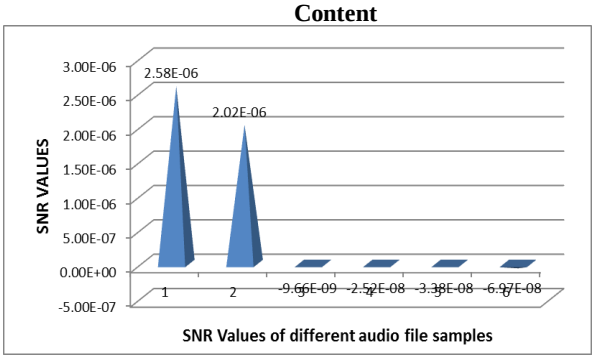

Fig 8.Graphical Representation For Different Categories Of Audio File With Same Text Content

The results of the experiment conducted by changing the 4th and 5th LSB bit with different data have been tabulated in Table IV, Table V and Table VI and their graphical representations of the same in Figure 9, Figure 10 and Figure 11 respectively.

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

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
Text1	103	-6.84E-09	16.66214532
Text2	100	-6.80E-09	16.66214532
Text3	75	-6.88E-09	16.66214532
Text4	50	-6.85E-09	16.66214532
Text5	25	-6.84E-09	16.66214532

Table V. SNR/PSNR Values For Different Audio Files Of Different Time Durations With Same Text Content

	Text File size :103 Bytes		
File Name	Duration (sec)	SNR	PSNR
Sample_15	15	-3.77E-08	17.50264072
Sample_30	30	-1.51E-08	17.16767052
Sample_60	60	-6.78E-09	16.66214532
Sample_80	80	-5.12E-09	16.61295561
Sample_90	90	-4.47E-09	16.6107783
Sample_100	100	-4.03E-09	1.66E+01

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

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
HARDCORE	103	1.52E-06	11.26356751
HIPHOP	103	1.29E-06	10.98350927
JAZZ	103	4.06E-09	17.71916498
METAL	103	-7.81E-09	10.69066241
POP	103	-1.01E-08	10.46596782
ROCK	103	-2.15E-08	13.55098551

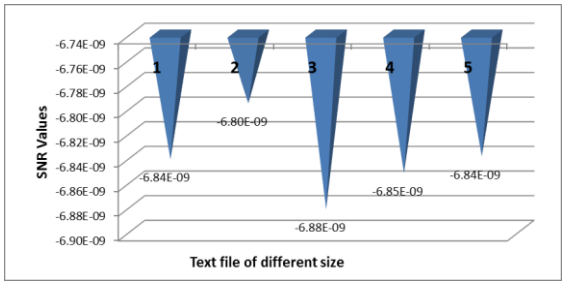

Fig 9 .Graphical Representation For Same Audio File With Varying Text Content Sizes

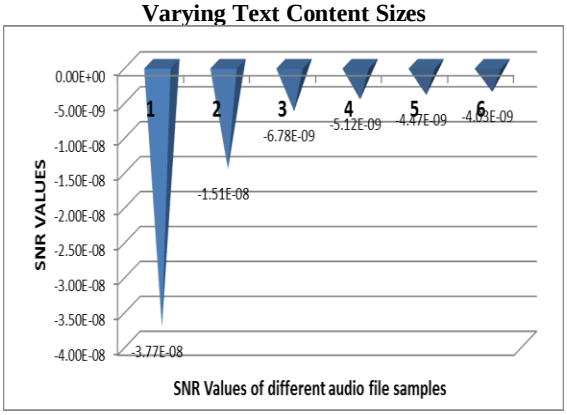

Fig 10 .Graphical Representation For Different Categories Of Audio File With Same Text Content

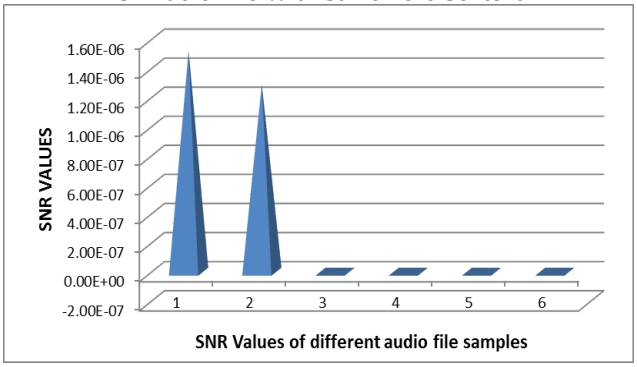

Fig 11 .Graphical Representation For Different Audio Files Of Different Time Durations With Same Text Content

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

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 higher layers.

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.

Acknowledgment

The author is thankful to Professor Venugopala P S, NMAMIT, Nitte faculty of Computer Science and Engineering for providing the necessary facilities for preparing this paper.

References

[1] Ajay.B.Gadicha1, "Audio Wave Steganography", and International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5, and November 2011.

[2] 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.

[3] R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham, "Efficient Method Of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enhanced", Journal of Theoretical and Applied Information Technology.

[4] K. Geetha and P.Vanitha Muthu, "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy" (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010, 1308-1313.

[5] Methods of Audio Steganography, Internet publication on www.Snotmonkey.com.

AUTHOR BIOGRAPHY

Padmashree G is working as an Assistant Professor in Mangalore Institute of Technology and Engineering, Moodabidri. She did her B E in AMCEC, Bangalore and M.Tech in NMAMIT, Nitte.Her research of interest are Security, Steganography, Network security.

Venugopala P S obtained his bachelor degree from VTU and M.tech from NITK, Surathkal. Working as Assistant professor in the department of computer science, NMAMIT, Nitte, with a teaching experience of ten years. Published 13 papers in national and international conferences and organized 4 training programs in the college. Area of interest includes image processing, data mining, nanotechnology and UNIX programming. Presently perusing Phd under VTU.