

Real Time Audio Steganography

S.Rajesh, Mr.Vinay Kumar Jain

Student, ME Communication¹, Associate Professor², ETC Department, SSTC, SSGI, Bhilai, India

Email: rajesh.mpcet@gmail.com

Email: vinayrich_17@yahoo.co.in

Abstract

Today the present scenario is the information world. We see every format of the information require digital safety for the sake of privacy. In digital world everything is done with the help of computer and we send information from this medium through email id to other individual, groups, delegates' etc. But there is not surety of privacy when we sending information through email. So keep the security tight over digital site we make ensure our information is well secured by any efficient algorithm or by any means of process. So we develop the GUI related to security purpose for achieving our goals and How to achieve this security in this project is elaborated and explained. Audio steganography is the process of hiding the secret information by concealing in into another medium such as audio file. Least Significant Bit (LSB) modification technique is the most simple and efficient technique.

Keywords: Steganography, Audio Steganography, LSB, carrier & Data Hiding

Introduction

Steganography or Stego as it often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". In a digital world, Steganography and cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security

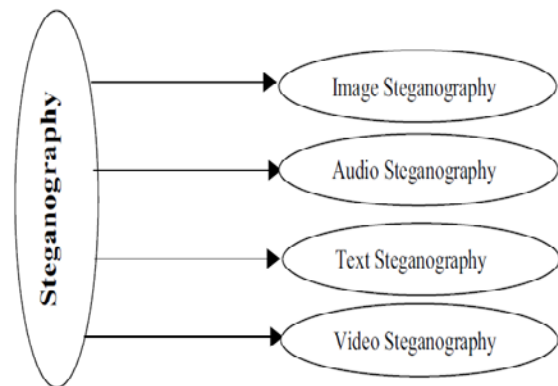


Figure 1: Types of Steganography

BLOCK DIAGRAM

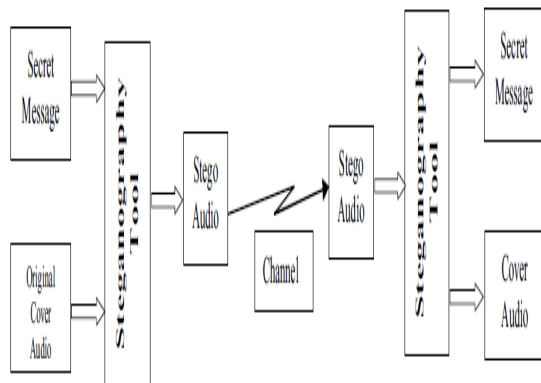


Figure 2: Basic block diagram of Audio Steganography

Algorithm

The aim of this project is to implement an algorithm for an information hiding technique using LSB in digital wave files. The proposed systems in information hiding algorithm consist of two main algorithms. The first one interested in hiding text in wave cover file called hiding algorithm and the second one is specialized in extracting data from the stego wave file called the extracting algorithm.

Data Hiding Algorithm

1. Audio file is converted into the data samples.
2. First 40 bytes are allocated for header part.
3. The compressed text message is converted as binary.
4. The length of text message is also converted as binary.
5. The identifier is selected to hide the text message.
6. An identifier helps in the recovery of text.
7. If there is no identifier in audio file, audio file no hidden text message.
8. The identifiers binary is 10101010.
9. Identifier can be hidden in 8 data samples.
10. The next 10 data samples will serve as the length of text message.
11. The next 10 data samples will be as the width of text message.
12. The compressed text message in the remaining data samples LSB is to be hidden.

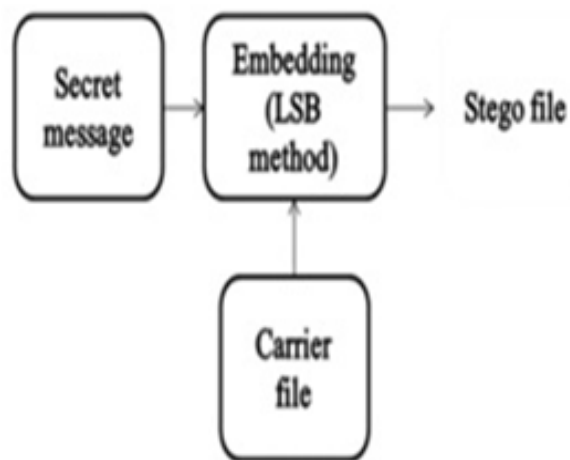


Figure 3: Data Hiding Process

4.3.2 Data Extraction Algorithm

1. Text can be recovered in a reverse way of how the text is hidden.
2. Now check the received audio file whether identifier present or not.
3. Without identifier, there can be no hidden text in data samples.
4. Both the length and width of the text message from the data samples lsb are to be measured.
5. The lsb bit of data samples should be taken until the length of the message received
6. Then the message in the lsb bit is to be converted into text.

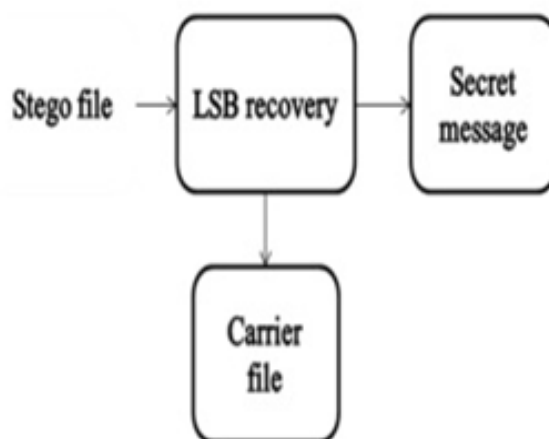


Figure 4: Data Extraction Process

Table 1: Literature Review

S. No	Title	Author	Publication/Year	Remarks
01	Multi Agent Based Audio Steganography	Kekre H. B, Athawale, A.Rao, Athawal U.	2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)	In this research paper, we simply present a multi-agent based system that enables secure communication for audio Steganography
02	Safe Transmission of text files through a new Audio Steganography Technique	Mohamed A. Ahmed, Laiha Mat Kiah, B.B. Zaidan	2014 2nd International Symposium on Computational and Business Intelligence	The core idea of the steganography algorithm used here is that if the shape of the amplitude-sample curve remains nearly unchanged then the percipience of human audibility system remains unchanged.
03	Hiding Text in Audio Using LSB Based Steganography	K.Adhiya Swati A. Patil	IEEE 2011	In this paper, steganographic system, 16bit WAV and 8bit WAV audio file are supported and the secret message can be hidden in the audio file with less storage capacity
04	A Novel Hybrid Audio Steganography for Imperceptible Data Hiding	Samir Kumar, BandyopadhyayBarnali	IEEE ICCSP 2015 conference	IEEE ICCSP 2015 conference
05	A Variable Higher Bit Approach to Audio Steganography	K.Priya ,K.Avinash	2013 International Conference on Recent Trends in Information Technology (ICRTIT)	This algorithm does not store any information in the LSB so to increase the hiding capacity the algorithm, it can be modified to hide a second bit of data in the LSB.
06	Increasing the Hiding Capacity of Low-Bit Encoding Audio Steganography Using a Novel Embedding Technique	Mohan Kumar, Suresh Babu	World Applied Sciences Journal 21 (Mathematical Applications in Engineering): 79-83, 2013	The method does not Changed the size of file even after encoding process, thus This method is suitable for hiding any type of audio data
07	Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique	K.Adhiya Swati A. Patil	International Journal of Innovative Research in Computer Engineering Vol.3, Issue 7, July 2015	The paper has possibility of improvements with respect to different type of data hiding like hiding of image into audio, Hiding of audio inside audio

08	An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution	Samir Kumar, BandyopadhyayBarnali	International Journal of Computer Applications Volume 77– No.13, September 2013	International Journal of Computer Applications Volume 77– No.13, September 2013
09	Secure Audio Steganography for Hiding Secret information	K.Sakthisudhan, P.Prabhu, P.Thangaraj	International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012)	The message signal is transmitted with utmost security and can be retrieved without any loss in transmission in this method.

METHODOLOGY

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 digit in the ones (right-most) position.

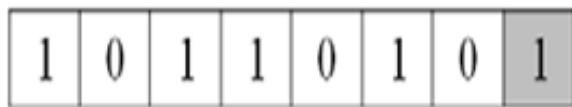


Figure 5: Binary representation of decimal 181

Figure 3.5.1.2 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. 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.

Now, even if the hidden message were to be discovered the person trying to get the message would only be able to lay his hands on the encrypted message with no way of being able to decrypt it.

1) Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as .WAV and .AIFF.

2) Temporal Sampling uses selectable frequencies (8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz.) to sample the audio. Sampling rate puts an upper bound on the usable portion of the frequency range. Generally, the higher the sampling rate is, the higher the usable data space gets.

3) Perceptual Sampling format changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3).

The four transmission mediums are discussed below.

1) Digital end-to-end environment: If a sound file is copied directly from machine to machine, but never modified, then it will go through this environment.

2) Increased/decreased resampling environment: In this environment, a signal is resampled to a higher or lowers sampling rate, but remains digital throughout. Although the absolute magnitude

3) Analog transmission and resampling: This occurs when a signal is converted to an analog state, played on a relatively clean analog line, and resampled. Absolute signal magnitude,

4) "Over the air" environment: This occurs when the signal is "played into the air" and "resampled with a microphone".

Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover audio. The LSB or in other words 8-th bit of some or all the bytes inside an audio file is changed to a bit of the secret message. Let us consider a cover audio contains the following bit patterns:

Byte-1	Byte-2	Byte-3
10100110	11000100	00001100
Byte-4	Byte-5	Byte-6
00101101	00011100	11011100
Byte-7	Byte-8	
11010010	10101101	

Suppose a number 200 is to embed in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information at least 8 bytes in the cover file is needed, hence taken 8 bytes in the cover file. Now modify the LSB of each byte of the cover file by each of the bit of embed text 11001000. Now Table 5.4.1 shows what happens to cover file text after embedding 11001000 in the LSB of all 8 bytes.

Here out of 8 bytes only 3 bytes get changed only at the LSB position. Since changing the LSB hence either changing the corresponding character in forward direction or in backward direction by only one unit and depending on the situation, there may not be any change also as seen in the above example.

Table 2: Illustration of LSB technique

Before replacement	After Replacement	Bit Inserted	Remarks
00101101	0010110 1	1	No change in bit pattern
00011100	0001110 1	1	Change in bit pattern (i)
11011100	1101110 0	0	No Change in bit pattern
10100110	1010011 0	0	No change in bit pattern
11000100	1100010 1	1	Change in bit pattern (ii)
00001100	0000110 0	0	No change in bit pattern
11010010	1101001 0	0	No change in bit pattern

RESULT

The proposed technique is simulated in Graphical User Interface by using MATLAB 2011a. The result is expected to be better relative to previous work done on existing method. It may be expected:

1. Data privacy is expected more stringent as compared to LSB techniques

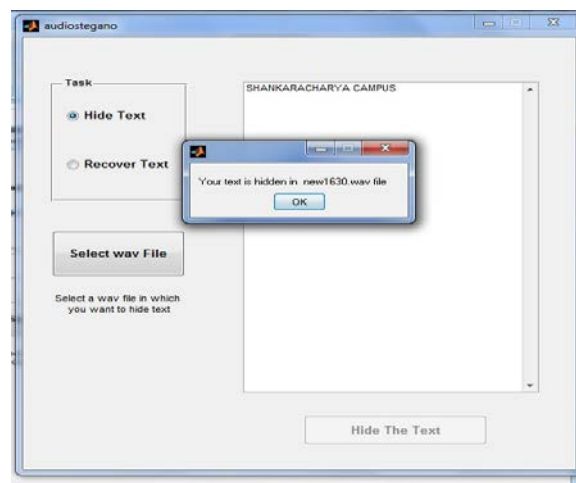


Figure 6: Select Wave File

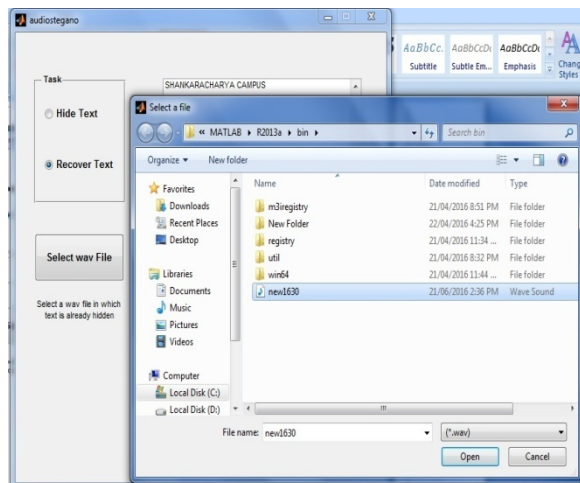


Figure 7: Recovering Text from Audio

ACKNOWLEDGMENT

I THANKFUL TO MR. VINAY KUMAR JAIN FOR HIS SUPPORTING IN THIS PROJECT.

REFERENCES

1. Priyanka R. Katariyavrushabh R. Patilkomal K. Shashikantm. Pinglesanghavimaheshr. "audio steganography usinglsb" ,1st international conference on recent trends in engineering& technology, mar-2012
2. Dr .DularKar, Drlaungjuangli and Dr.Ajaykatangur, "Astegnographic application using audio files", TEXAS A.MUniversity ,2009 .
3. Mahalakshmi., Selvarani, Thilagam , and N.Tharminie,"AUDIO STEGNOGRAPHY USING AES",International Journal of Innovative Research in Science, Engineering and Technology, 4SEPT 2015.
4. Deepak, Karthik, AND Manjunath , " Efficient Method toIncrease Robustness in Audio Steganography", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue6, December 2012
5. Prof. Samir Kumar, BandyopadhyayBarnali, and Gupta Banik. "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer
6. R.F. Olanrewaju, Othman Khalifa and Husnabinti AbdulRahman Suliman, "Increasing the Hiding Capacity ofLow-Bit Encoding Audio Steganography Using a Novel Embedding Technique", World Applied Sciences Journal21

(Mathematical Applications in Engineering): 79-83,2013

7. JyotiBahl and Dr. R. Ramakishore "Audio Steganographyusing Parity Method at higher LSB layer as a variant of LSB Technique", International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2015.
8. Ankit Chadha, NehaSatam, RakshakSood and Dattatray Bade," An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB)Substitution", International Journal of Computer Applications (0975 – 8887) Volume 77– No.13,September 2013.
9. Jayaram, Ranganatha, and Anupama, "Information hiding using audio Steganography – a survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3,No.3, August 2011
10. Md. ShafakhatullahKhan, V.Vijaya Bhasker and V.ShivaNagaraju. "An Optimized Method for Concealing Data using Audio Steganography". International Journal of Computer Applications (0975 – 8887) Volume 33–No.4, November 2011.
11. Mohammed Salem Atoum, Mamoun Suleiman AlRababa, Dr.Subariah Ibrahim, and OsamahAbdulgaderAhmed,"A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", IJCSNSInternational Journal of Computer 184 Science andNetwork Security, VOL.11 No.5, May 2011.
12. Ramandeepkaur, and Jitender Sharma, "Information hiding by using Multiple techniques of audio steganography", ICRTEDC-2014.
13. Tanmaiy G. Verma, ZohaibHasan, and Dr.GirishVerma," A Unique Approach for Data Hiding Using Audio Steganography" International Journal of Modern Engineering Research (IJMER) ,Vol. 3, Issue. 4, Jul -Aug. 2013 pp-2098-2101.(IJSCE), Volume-1, Issue-5, November 2011.
14. Bhagyashri A. Patil and Vrishali A. Chakkarwar, "Reviewof an Improved Audio Steganographic Technique over LSB through Random Based Approach", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 9, Issue 1(Jan. - Feb. 2013).
15. S.S. Divya and M. Ram Mohan Reddy, "Hiding text in audio using multiple lsb steganography and provide security using cryptography", International journal of scientific& technology research volume 1, issue 6, july2012, IJSTR2012

16. K.Sakthisudhan, P.Prabhu and P.Thangaraj "Secure Audio Steganography for Hiding Secret information", International Conference on Recent Trends in Computational Methods, Communication and Controls, ICON3C 2012.
17. M. Nutzinger, " Real-time Attacks on Audio Steganography", Journal of Information Hiding and Multimedia Signal Processing ,Volume 3, Number 1,