Enhancement in Security of LSB based Audio Steganography using Multiple Files

Pooja Chandrakar
M.Tech Scholar
Dept. of Computer Science & Engineering,
R.C.E.T,Bhilai, India

Minu Choudhary
Asst. Professor
Dept. of Information Technology& Technology,
R.C.E.T, Bhilai, India

Chandrakant Badgaiyan
Asst. Professor
Dept. of Mechatronics Engineering,
C.S.I.T, Durg, C.G, India

ABSTRACT

Steganography is one of the best data hiding technique in the world which can be used to hide data without its presence felt. In today’s digital world most of us communicate via use of electronic media or internet. Most people among us remain unaware about the data loss or data theft which can happen on online transmission of data or message. Valuable information including personal data, messages transmitted through internet is vulnerable to hackers who may steal or decrypt our data or messages. This paper is about enhancing the data or message security with use of Audio Steganography using LSB algorithm to hide the message into multiple audio files. The message hidden by this application is less vulnerable to be stolen than other similar applications. This is due to following reasons: Firstly multiple files are taken to hide high amount of message which enhance information hiding capacity. Secondly before being hidden, the message is broken into parts and shuffled randomly based on permutation generated at runtime so even if the LSB gets encountered the message is still unarranged and meaningless which enhances its security. This application is capable to carry large amount of information with greater security.

General Terms

LSB; Least Significant Bit; Stego file; Encrypted audio file

Keywords

LSB, Random permutation, Stego file, Multiple audio file

1. INTRODUCTION

As world is changing fast, people wants to save their time and resources to keep pace with the fast growing technology for the fulfillment of their needs. As internet has become a working need of the people like electronic banking, mobile banking, online shopping, transferring data from one place to another, gathering or retrieving of information. Data Security need is also increasing due to risk of theft, hacker, intruders, eavesdroppers, sabotage and unauthorized user. Security can be achieved using cryptography which encrypts message and make it unreadable from unauthorized people or watermarking technique provides copyright protection and the third one is steganography. Steganography is a uniquetechnique coming from old times which help user to hide their critical information without creating any suspicion. Information hiding can be done in various cover mediums like image, audio, video, text etc. Cover is chosen according to the need like audio steganography is an interesting medium because latest song or famous songs can be used to hide messages. Embedding techniques are chosen according to requirement. Some of the techniques are LSB coding, parity coding, phasecoding, spread spectrum and echo hiding [1],[2]. It can be used for hiding any information like secret formulas, images,private communicationand forensic authentication [2]. As audio steganography uses audio as a cover medium,similarly this application too uses an audio as a platform for hiding the message. User provides input message in the form of text and chooses the audio wave file to hide the message. This application provides a smart and interactive interface for message hiding and its retrieval. Message is shuffled in random sequencebefore being hidden. Random sequence which is generated based on certain factors is used to shuffle the message before hiding it. This further enhances the data security.

2. RELATED WORK

The availability and the popularity of audio files make them more suitable to carry hidden information. Classification of various audio steganographic techniques are done on the basis of various domains like time domain, transform domain etc. Techniques under time domain are echo hiding, parity coding and LSB coding. Transform domain is further divided into wavelet domain and frequency domain. Techniques under frequency domain are phase coding and spread spectrum and under wavelet is wavelet coding [1]-[3]. Steganography does not cause original message to corrupt but help us to make use of any technique to hide data inside cover. Characteristic of steganography which is present in more or less is secrecy, imperceptibility, robustness, high hiding capacity, accurate extraction, transmission rate, noise resistance, real time suitability [3], [8]. Steganography help as to protect our intellectual property [2]. Steganography make use of perception and senses which are not trained to look for hidden information. Detailed working of various embedding technique has been shown in [1], [2]. LSB coding is suitable to work with any type of audio file format hence easily combinewith any technique. But at the same time due to simplicity, LSB encoding lack robustness and security and data is only hided in last bit which lower its importance. Many steps have been taken to improve performance of LSB coding. Dr. H.B.Kekre worked with LSB technique to increase the capacity of cover audio signal by making use of multiple LSB. Variable number and position of LSBs is used to hide message which facilitate more message to get hide [4]. More work has been done on different parameters of LSB to improve its performance. Embedding of secret message according to threshold gives new perspective to implement LSB [5]. Various audio steganographic techniques are available buteach of them has different strength and weakness [6]. One can choose encoding technique according to requirement, advantage and disadvantage. Various types of attack is possible some are stego only attack, known cover or message or stego attack [7]. As security is major aim ofsteganography extending the conventional LSB to achievemore security against steganalysis [9]. Use of secret key is also used to achieve security and authentication [10]. Image can also be hided in audio file [11]. Freedom of hiding text, image and audio inside audio file make audio steganography more famous and easy to use.

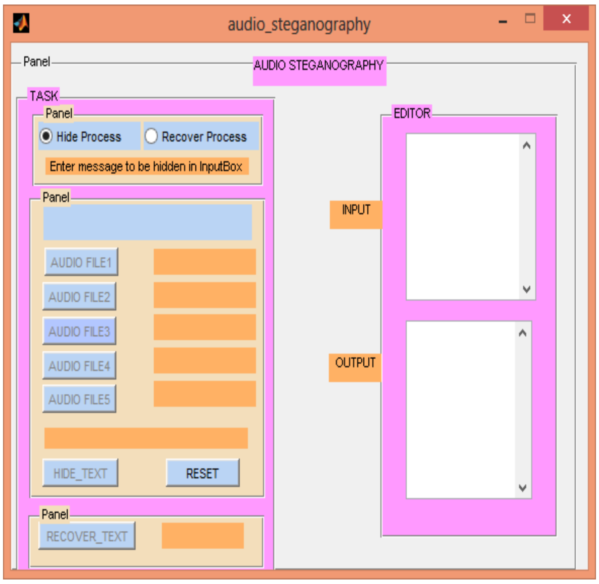
2.1 Basic Working of Steganography

The basic working principle of steganography is very simple. Steganography works by selecting a cover medium which can be either of audio, video, image or text. In case of audio steganography, an audio file is taken as cover to hide the user's message using some algorithms and key. Key is an optional parameter. These parameters are used together to hide the message inside an audio file. An audio file containing hidden message is generally termed as "Stego file". A stego file once ready can be sent to anyone freely.

3. IMPLEMENTATION

LSB coding approach suffersa very deterministic way.An attacker can easily identify and uncover the message by just removing the complete LSB plane [1]. Based on these demerits this application is implemented for the purpose of increasing security by shuffling the input message before hiding it in the audio file. Even if any attacker gets to know theentire message then also correct message will not be decoded. This is so because message is shuffled as per dynamic generation of random sequence. The generation of random sequence depends on the number of files selected for hiding the secret message. This application is written in Matlab.

Figure 1 below illustrates the GUI interface of this application.



Enter message to be hidden in InputBox

Fig 1: Application Interface

Figure2 illustrates the flow diagram that represents the workflow activities for proposed application. The application starts when the user select either hide process or recover process from GUI interface.

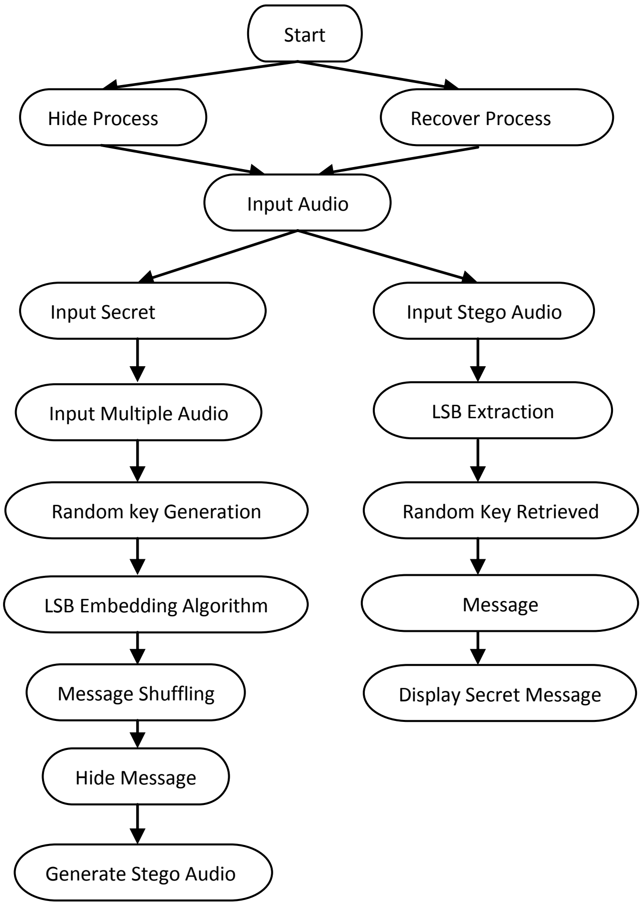
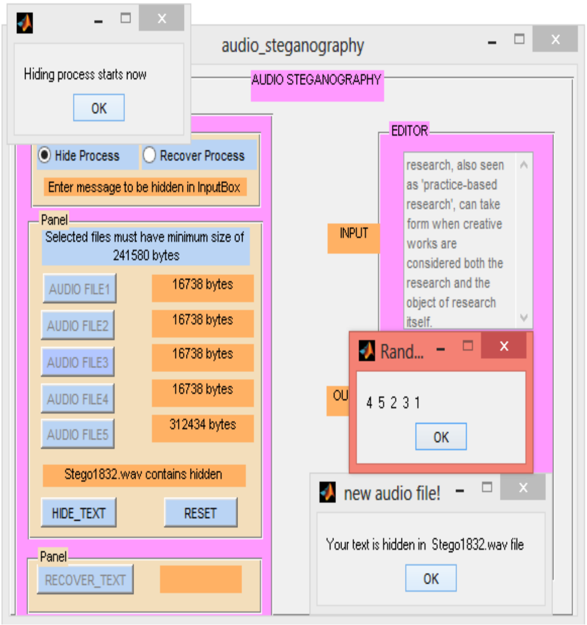


Fig 2: Workflow of Process

3.1 Hiding Process

The user enters a text message as input for hiding process. Application calculates the minimum file size required to hide the input text based on certain factors. Audio file1 button is enabled for the user to select a file to hide the user message. Based on users file selection this application intelligently enables the next select button in runtime, if the selected file size does not met minimum required capacity. This process continues till the user has selected the file(s) of minimum required size. Selected file size(s) are displayed in a static text area next to it along with total size in bottom. As soon as the selected file size becomes sufficient to hide the user message further select buttons remains disabled and user is prompted to start the hidingprocess. Hiding process starts when the user clicks on the hide text button on the application interface. Based on the number of files selected a permutation of number 1 to file count is generated each time. On the background the input user message is broken into pieces of equal length. Number of pieces depends on the number of files selected. Now the message pieces are shuffled as per the permutation generated above and are combined again. Shuffling the message before hiding enhances the security of application to greater level. At the same time all selectedaudio files are combined together as per their selected sequence to create a new stego audio file. In the next step the user message is written into above created stego file as per the LSB Algorithm. User message is converted into binary before being written to the stego file. When using the LSB algorithmthe binary bit is written to every least significant bit only thusreducing the Noise factor in the stego file. This stego file can be sent to the concerned person via email or any other medium with the secret user message which can be correctly decoded using this application only.



Hiding process starts now

Enter message to be hidden in InputBox

Selected files must have minimum size of 241580 bytes

AUDIO FILE1	16738 bytes
AUDIO FILE2	16738 bytes
AUDIO FILE3	16738 bytes
AUDIO FILE4	16738 bytes
AUDIO FILE5	312434 bytes

Stego1832.wav contains hidden

research, also seen as 'practice-based research', can take form when creative works are considered both the research and the object of research itself.

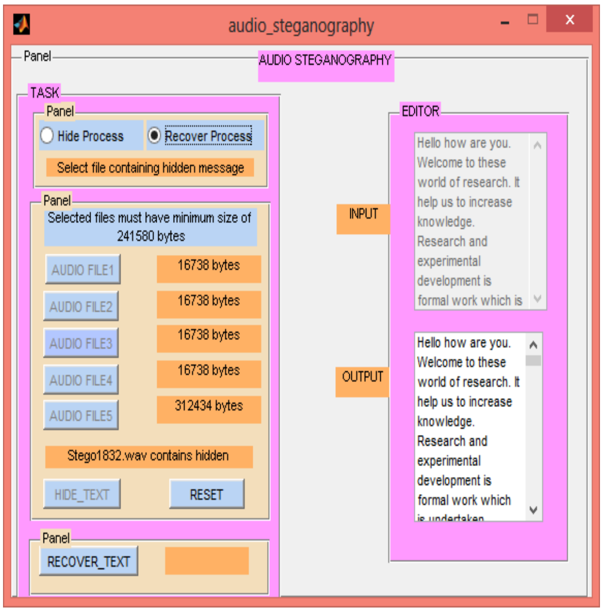
4 5 2 3 1

Your text is hidden in Stego1832.wav file

Fig 3: Random Sequence and Stego File Created

3.2 Recovering Process

The user needs to select recover hide radio button to carry recover process. User selects a stego file as input. Shuffled message is retrieved using LSB algorithm which is reshuffled and joined in a correct sequence captured during hiding process. Secret message gets displayed in the output.



Select file containing hidden message

Selected files must have minimum size of 241580 bytes

AUDIO FILE1	16738 bytes
AUDIO FILE2	16738 bytes
AUDIO FILE3	16738 bytes
AUDIO FILE4	16738 bytes
AUDIO FILE5	312434 bytes

Stego1832.wav contains hidden

Hello how are you. Welcome to these world of research. It help us to increase knowledge. Research and experimental development is formal work which is

Hello how are you. Welcome to these world of research. It help us to increase knowledge. Research and experimental development is formal work which is undertaken

Fig 4: Application Interface after Recovering Process

4. RESULTS AND DISCUSSION

The functionality of this application is rigorously and successfully tested using different length messages and multiple wav audio files of various sizes. GUI is user friendly and interactive. Message of any length can be hidden easily with proper sized audio file. Intelligent interface guides the user throughout the process. Series of validation added in the application minimizes the chances of human error to zero thus making it a friendly experience for the user.

Table 1.Enhanced Security by Shuffling text content

Number of Files	Possible Order of ShuffledMessage	Security Level
1	Not Applicable	Normal
2	(1,2) (2,1)	Medium
3	(1,2,3) (2,1,3) (3,1,2) (1,3,2) (3,2,1) (2,3,1)	Medium-High
4	24 arrangements	High
5	120 arrangements	Highest

The possible arrangement of message shuffling and respective security level is shown in Table-1. Security enhancement is directly proportional to number of files selected for hiding the message. Even after removal of all LSB planes, it would be still difficult to guess the correct arrangement of message.

5. CONCLUSION

The application of steganographic algorithm has been built emphasizing enhancement in capacity and security of message transmission. This user friendly application maintains privacy, confidentiality and accuracy of the user's message upon hiding or recovering message. Message shuffling before hiding is an added advantage in terms of security. Using LSB algorithm gives an advantage of working with any audio file format. Audio quality does not deteriorate much even in case of using multiple audio file thus minimizing the suspicion of any secret transmission. Our future enhancement will be to incorporate support for various other audio formats and to minimize the noise content from the generated Stego file.

6. ACKNOWLEGEMENT

I would like to thank Prof. MinuChoudhary, for the guidance in research work of audio steganography. I would like to thank Prof. ChandrakantBadgaiyan for motivating this research work and for his constructive suggestions.

7. REFERENCES

[1] Fatiha Djebbar_1 and Beghdad Ayad2and Karim Abed Meraim3and Habib Hamam4 "Comparitive Study of Digital Audio Steganography Techniques" Survey paper2011.

[2] Jayaram P1, Ranganatha H R2, Anupama H S3 "Information Hiding Using Audio Steganography-A Survey"IJMA 2011 Vol.3, No.3,August.

[3] Abdulaleem Z. Al-Othmani1, Azizah Abdul Manaf2 and Akram M. Zeki3 *"A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation*"IJCSI,Vol.9,Issuse 1,No 1, January 2012.

[4] Dr.H.B.Kekre, ArchanaAthawale, B.SwarnalataRao, UttaraAthawale, *Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding,* IEEE Third International Conference on Emerging Trends in Engineering and Technology, 2010.

[5] Masahiro Wakiyama†, Yasunobu Hidaka†, Koichi Nozaki "An audio steganography by a low-bit coding method with wave files" IEEE 2010 Sixth International Conferene on Intelligent Information Hiding and Multimedia Signal Processing.

[6] Jisna Antony, Sobinc.c, Sherly A.P, "audio steganography in wavelet domain-a survey",International Journal of Computer Applications, Volume 52-No.13, August 2012.

[7] M.L.Mat Kiah1, B.B. Zaidan2,3,4, A. A. Zaidan2,3,4*, A. Mohammed Ahmed1 and Sameer Hasan Al-bakri1, "A review of audio based steganography and digital Watermarking", International Journal of the Physical Sciences Vol. 6(16), pp. 3837-3850, 18 August, 2011.

[8] Parul Shah, PranaliChoudhari and Suresh Sivaraman, "Adaptive Wavelet Packet Based Audio Steganography using Data History" 2008 IEEE Region 10 Colloquium and the Third ICIIS, Kharagpur, INDIA December 8-10.

[9] Muhammad Asad, JunaidGilani Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 978-1-61284-941-6/1112011 IEEE.

[10] Ashwini Mane, GajananGalshetwar, AmuthaJeyakumar, "Data Hiding Technique: Audio Steganography Using LSB Technique", International Journal of Engineering Research and Applications, Vol.2, Issue 3, May-Jun 2012, pp.1123-1125.

[11] Dalal, Khamael& Mohammed, "A New Steganographic Method for Embedded Image In Audio File", International Journal of Computer Science and Security(IJCSS), Volume(6) : Issue(2) : 2012.