International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 25th Mar 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-3

Title: **A NEW ENCRYPTED SECRET MESSAGE EMBEDDING IN BY USING LSB BASED STENOGRAPHY WITH AES**

Volume 07, Issue 03, Pages: 118– 122.
Paper Authors

M.LATHA KUMARI, G.SANDHYA, P.KANAKADURGA, M.GOPI,B.PRIYANKA, DR.P.CHENNARAO
Sri Sarathi Institute Of Engg &Technology.
.
.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NEW ENCRYPTED SECRET MESSAGE EMBEDDING IN BY USING LSB BASED STENOGRAPHY WITH AES

[1]M.LATHA KUMARI, [2]G.SANDHYA, [3]P.KANAKADURGA, [4]M.GOPI,[5]B.PRIYANKA
DR.P.CHENNARAO, PROFESSOR
Sri Sarathi Institute Of Engg &Technology
Mail id: haichenna@rediffmail.com

Abstract: A Steganography method of embedding textual information in an audio file is presented in this paper.In the proposed method each audio sample is converted into bits and then the textual information is embedded in it. In embedding process , first the message character is converted into its equivalent binary. The last 4 bits of this binary is taken into consideration and applying redundancy of the binary code the prefix either 0 or 1 is used. To identify the uppercase, lower case, space ,and number the control symbols in the form of binary is used. By using proposed LSB based algorithm, the capacity of stego system to hide the text increases. The performance evaluation is done on the basis of MOS by taking 20 samples and comparison of SNR values with some known and proposed algorithm.

Keywords: Steganography, Human Auditory System (HAS), Cover audio, Stego-object, Embed, Extraction.

Introduction

Steganography is an art of sending hidden data or secret Messages over a public channel so that a third party cannot detect the presence of the secret messages. The goal of steganography is different from classical encryption, which Seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages. Modern steganography is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures [1, 2, 3], video [3, 4], audio [1, 3] and even typeset text [1, 3]. This makes sense for a number of reasons. First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and extract messages. Secondly, extraction itself can be automated when the data is electronic, since computers can efficiently manipulate the data and execute the algorithms necessary to retrieve the messages. Electronic data also often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages. The main goal of this paper was to find a way so that an audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file. Because degradation in the perceptual quality of the cover object may

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

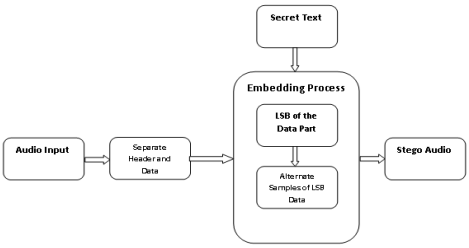
leads to a noticeable change in the cover object which may leads to the failure of objective of steganography.

Desired Characteristics of Stegnography:

A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end user at the destination) [1]. In a pure steganography framework, the technique for embedding the message is unknown to anyone other than the sender and the receiver. An effective steganographic scheme should posses the following desired characteristics [10- 11]: Secrecy: a person should not be able to extract the covert data from the host medium without the knowledge of the proper secret key used in the extracting procedure. Imperceptibility: the medium after being embedded with the covert data should be indiscernible from the original medium. One should not become suspicious of the existence of the covert data within the medium. High capacity: the maximum length of the covert message that can be embedded should be as long as possible [30] Resistance: the covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme [12]. Accurate extraction: the extraction of the covert data from the medium should be accurate and reliable.

Design Methodology

In the current endeavor, an audio file with ".wav" extension has been selected as host file. It is assumed that the least significant bits of that file should be modified without degrading the sound quality[34]. To do that, first one needs to know the file structure of the audio file. Like most files, WAV files have two basic parts, the header and the data. In normal wav files, the header is situated in the first 44 bytes of the file. Except the first 44 bytes, the rest of the bytes of the file are all about the data. The data is just one giant chunk of samples that represents the whole audio. While embedding data, one can't deal with the header section. That is because a minimal change in the header section leads to a corrupted audio file.



A program has been developed which can read the audio file bit by bit and stores them in a different file. The first 44 bytes should be left without any change in them because these are the data of the header section. Then start with the remaining data field to modify them to embed textual information. For example, if the word "Audio" has to be embedded into an audio file one has to embed the binary values of the word "Audio" into the audio data field.

Letter	ASCII Value	Corresponding Binary Value
A	065	01000001
u	117	01110101
d	100	01100100
i	105	01101001
o	111	01101111

Table:

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

To develop this algorithm multiple bits of each sample of the file have been changed or modified to insert text data in it. It has also been observed the degradation of the host audio file after modification of the bits. The bit modification was done by various ways, like 1, 2, 3, 4 bits were changed in turn. But after going through all the modification it has been observed.

Algorithm (For Embedding of Data):

- Leave the header section of the audio file untouched...
- Start from a suitable position of the data bytes. (For the experiment purpose the present start byte was the 51st byte). Edit the least significant bit with the data that have to be embedded.
- Take every alternate sample and change the least significant bit to embed the whole message

Sample No.	Binary values of corresponding sample	Binary value to be embedded	Binary values after modification
51	01110100	0	01110100
53	01011110	1	01011111
55	10001011	0	10001010
57	01111011	0	01111010
59	10100010	0	10100010
61	00110010	0	00110010
63	11101110	0	11101110
65	01011100	1	01011101

Table:

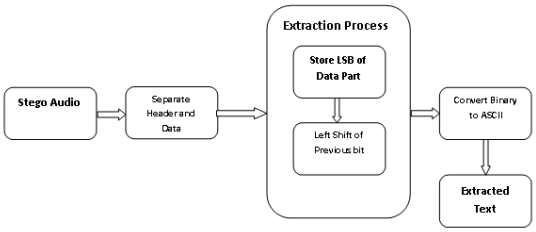
The data retrieving algorithm at the receiver's end follows the same logic as the embedding algorithm.

Algorithm (For Extracting of Data):
Leave first 50 bytes.

• Start from the 51st byte and store the least significant bit in a queue.

• Check every alternate sample and store the least significant bit in the previous queue with a left shift of the previous bit.

• Convert the binary values to decimal to get the ASCII values of the secret message. • From the ASCII find the secret message



.Editing of the existing binary values with the intended binary values causes a minimal change in the audio file "audio.wav" that remains almost imperceptible to anyone other than the sender. When it comes to the point of data retrieving at the receiver's end, the retrieving algorithm has to be followed: First, change the audio message into binary format that has come from the source as stego-object. Leave first 50 bytes with no change in them.

Sample No.	Binary values with embedded secret data	Bits that are stored in the queue
51	01110100	0
53	01011111	01
55	10001010	010
57	01111010	0100
59	10100010	01000
61	00110010	010000
63	11101110	0100000
65	01011101	01000001

Table:

Start from 51st bit, check the least significant bit, and store it in a queue. Check every alternate sample to collect the whole messages. Like 53rd, 55th and 57th and so on. Store the least significant bits of the alternate samples in the queue with left shift of previous bit. Convert the binary values to decimal to get back the ASCII from which the text can be retrieved. The whole retrieval process can be depicted with the following table more thoroughly

Advantages:

- Secrecy
- Imperceptibility
- High capacity

Applications:

- Military Applications
- Secured Data Transmission

Conclusion:

REFERENCES

W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336. [2] Kharrazi, M., Sencar, Husrev T., and Memon, N., "Image Steganography: Concepts and Practice", WSPC, April 22, 2004.

[3] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking". Boston, Artech House, pp. 43 – 82. 2000.

[4] K. Matsui and K. Tanaka. Video-steganography. In: IMA Intellectual Property Project Proceedings, volume 1, pp 187-206, 1994.

[5] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, pp. 26-34, IEEE, Feb. 1998.

[6] Matsuoka, H., "Spread Spectrum Audio Steganography using Sub – band Phase Shifting", Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'06), IEEE, 2006.

[7] S.S. Agaian, D. Akopian, O. Caglayan, S. A. D'Souza, "Lossless Adaptive Digital Audio Steganography," In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903-906, November 2005.

[8] K. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421- 424, April 2003.

[9] Mohammad Pooyan, Ahmed Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", International Symposium on Signal Processing and Information Technology, IEEE, 2007.

[10] C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern- Based Modification", IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[11] Chen and G.W. Womell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443, May 2001.

[12] B. Chen, "Design and analysis of digital watermarking, information embedding, and data hiding systems," Ph.D. dissertation, MIT, Cambridge, MA, June 2000.

[13] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography", 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, IEEE, 2003. [14] J. Zollner, H. Federrath, H. Klimant, et al., "Modelling the Security of Steganographic Systems", in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.

[15] Johnson, Neil F. and Stefan Katzenbeisser. "A Survey of Steganographic Techniques", In Information Hiding: Techniques for Steganography and Digital Watermarking. Boston, Artech House. 43-78. 2000.