An Improved Capacity Encrypted Secret Message Embedding LSB based Steganography with AES Implementation

Mr.Sk.John[1], Dr.Venugopal Reddy.CH[2]
[1]Assistant Professor, RISE Krishna Sai Prakasam Group of Institutions,Ongole, A.P, INDIA.
[2]Professor, RISE Krishna Sai Prakasam Group of Institutions,Ongole, , A.P, INDIA.

Abstract: Steganography is the art of conveying secret messages or hidden data through a public channel so that a third party is unable to detect them. In contrast to classical encryption, which aims to obscure the contents of hidden communications, steganography first converts the message character to its binary counterpart. The final four bits of this binary are taken into account, and redundancy in the binary code is applied using the prefix either 0 or 1. Control symbols in binary form are used to distinguish upper- and lowercase letters, spaces, and numbers. The ability of the stego system to disguise the text rises when utilizing the proposed LSB-based method. According to the MOS, 35 samples are taken and compared to the SNR values of a recognized and proposed algorithm.

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

I. INTRODUCTION

To transfer hidden data or secret communications across a public channel, steganography is the practice of using steganography techniques. Traditional encryption is to hide the content of secret messages; steganography's goal is to conceal the fact that secret messages exist in the first place. Electronic media is the primary focus of modern steganography, and tangible artifacts are rarely used in this type of work. Even typeset text [1, 3] has been used to disguise data in channels with images [1, 2], video [3, 4], and even audio [1, 3]. There are several reasons why this is a good idea. The first reason electronic media is easier to manipulate for hiding data and extracting messages is because information is typically less than the data in which it must be buried (the cover text). As a second benefit of electronic data, extraction may be automated, as computers are capable of effectively manipulating and executing the algorithms required to locate the messages. Messages can also be hidden in electronic data by manipulating superfluous, unneeded, and unobserved data spaces..

It was the primary objective of this study to identify a solution to hide text in an audio file without changing the file structure or content. A decrease in the cover object's perceptual quality may result in a perceptible alteration that could compromise the goal of steganography.

In general, a steganography system should meet three main requirements: imperceptibility of embedding, accuracy in recovering embedded information, and a big payload [1]. Message embedding techniques are not known to anyone but the sender and receiver in a steganography system. A successful steganographic method should have the following characteristics: A person should be unable to extract the secret data from the host medium unless they have access to the secret key that was used during the extraction process. It should be impossible to tell if the medium has been altered in any way after it has been embedded with the secret data. The concealed data in the medium should not be a cause for concern. Longest possible length: a high carrying capacity.

The hidden message should be as long as feasible in order to avoid detection [30]. When the host media is altered, for example by some lossy compression algorithm [12], the covert data should be able to persist. Extracting the secret information from the medium should be done with precision and accuracy.

Existing system

In cryptography, information is encoded in a way that makes it impossible for anybody but the person who knows how to decipher it. Cryptographic processes have become a major priority for a growing number of businesses because of the sheer volume of sensitive Internet activity. snags are discovered Documents encrypted with a public key have a much longer transmission time. In reality, the cost of transmitting massive amounts of data is prohibitive.The key sizes must be significantly larger to achieve the high level of protection.

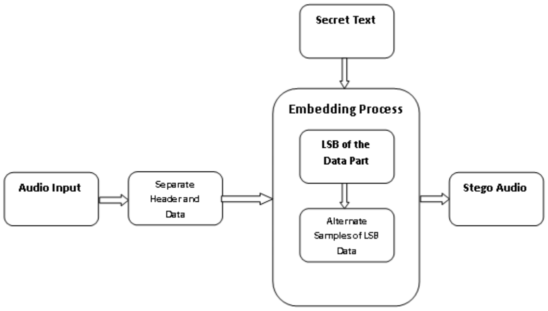
- Public key cryptography is susceptible to impersonation attacks.

II. PROPOSED SYSTEM

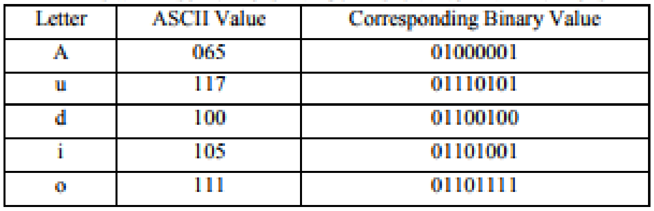
Design Methodology

".wav" files have been chosen as the host files for this experiment. Because of this, it is anticipated that only the most insignificant sections of the audio file will be altered[34]. To do so, one must first understand the file structure of the audio file in order to accomplish this. WAV files, like most other files, have a header and a data section. First 44 bytes of a wav file are reserved for the header. It's everything about the data except for the first 44 byte chunk.

The data consists of a single large collection of audio samples, which represents the entire recording. The header section cannot be dealt with while embedding data. The reason for this is because even the tiniest modification in the header portion of the audio file can cause it to be corrupted.



The audio file can be read bit by bit by a program that has been written, and the data is then stored in a separate file. The first 44 bytes of the header section should remain unchanged, as these comprise the data. Then, work with the remaining data fields to add textual content. The binary values of the word "Audio" must be included in the audio data field, for example, if the term "Audio" must be included in an audio file.



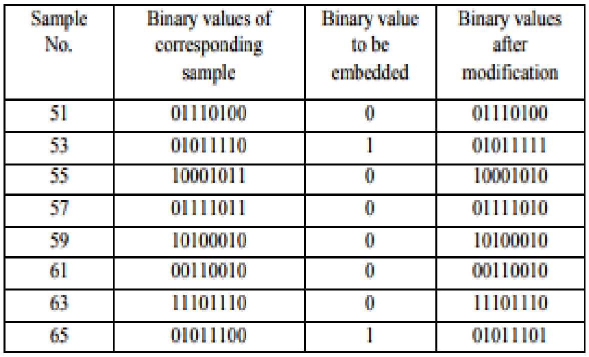
Letter	ASCII Value	Corresponding Binary Value
A	065	01000001
u	117	01110101
d	100	01100100
i	105	01101001
o	111	01101111

Table: serect text corresponding binary code

Text data has been inserted into this algorithm by altering several bits of each sample of the file. The host audio file suffers after the bits are changed, as has been documented. As an example, bits 1, 2, 3, and 4 were all altered at the same time. However, after undergoing all the changes, it has been discovered.

Algorithm (For Embedding of Data):

- ➢ Do not alter the audio file's header section...
- ➢ A good place to start is at the beginning of the data. The 51st byte was used as a starting point for the experiment. Data that must be embedded should be edited into the least significant piece of the file.
- ➢ Change the most insignificant part of each alternate sample to encode the entire 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

"

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

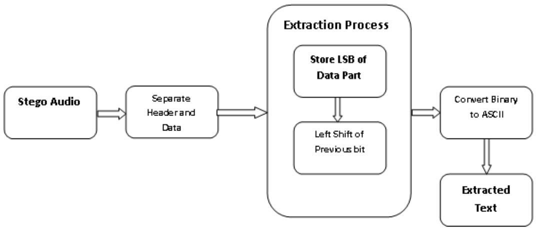
Algorithm (For Extracting of Data):

Leave first 50 bytes.

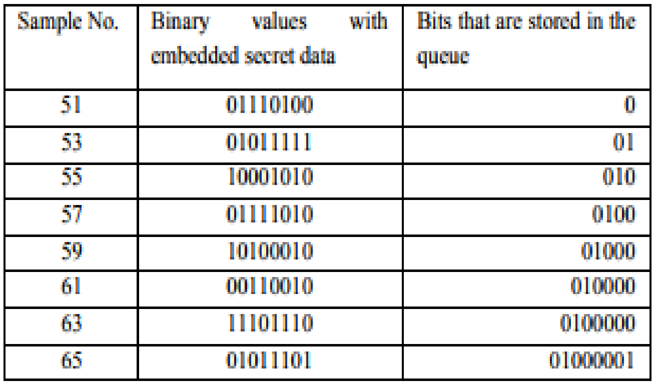
• Start from the 51st byte and store the least significant bit in a queue.

• 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 . A little, almost undetectable modification is made to the audio file "audio.wav" when the intended binary values are substituted for the current binary values. the receiving end must follow the retrieving procedure in order to retrieve data



To begin, convert the audio file to binary format using the stego-object that was provided by the original source. Leave the first 50 bytes alone.

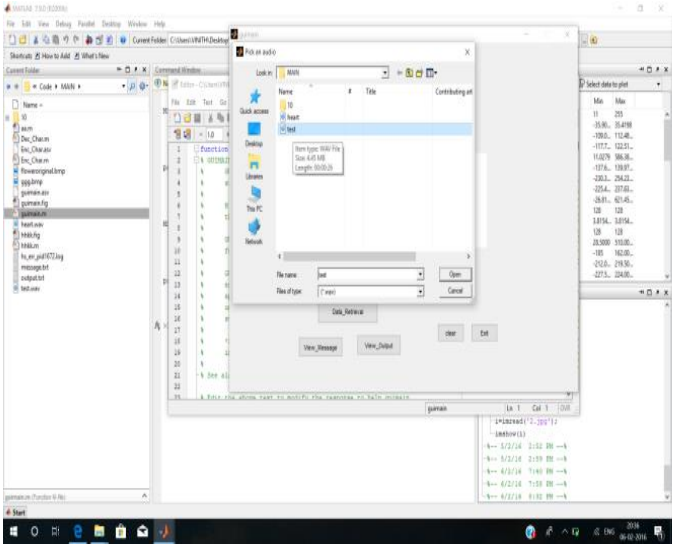


Sample No.	Binary values with embedded secret data	Bits that are stored in the queue
51	01110100	0
53	01011111	01
55	10001010	010
57	01111010	0100
59	10100010	01000
61	00110010	010000
63	11101110	0100000
65	01011101	01000001

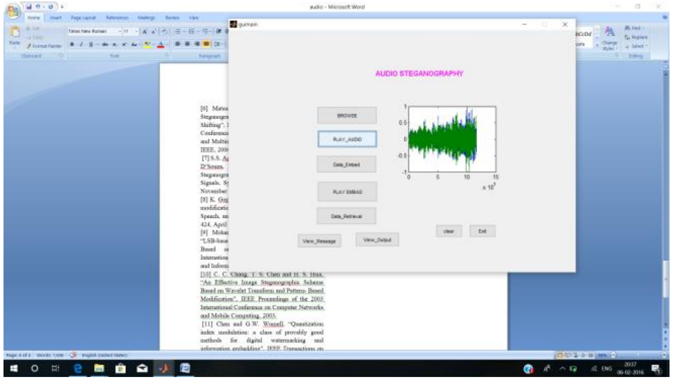
Table: audio sample corresponding binary code

Set a queue of bits beginning with 51 and then check the least significant bit. To get a complete picture of what's going on, go through each and every example. 53rd, 55th, 57th, and so forth. Keep in queue the least significant bits of alternate samples with a shift of the previous bit's value left. The text can be recovered by converting the binary values to decimal and then back to ASCII. Following table depicts the entire retrieval procedure in further detail.

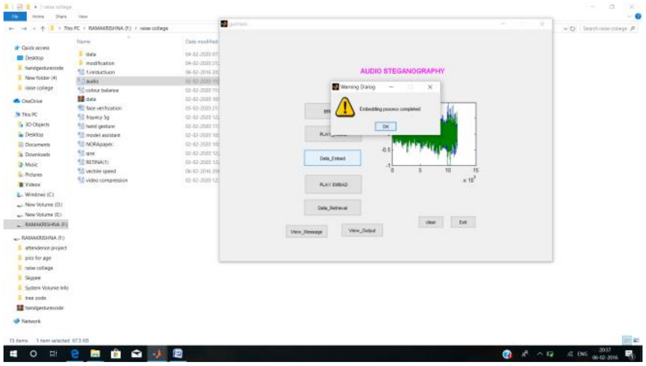
III. RESULTS



Browse audio signal

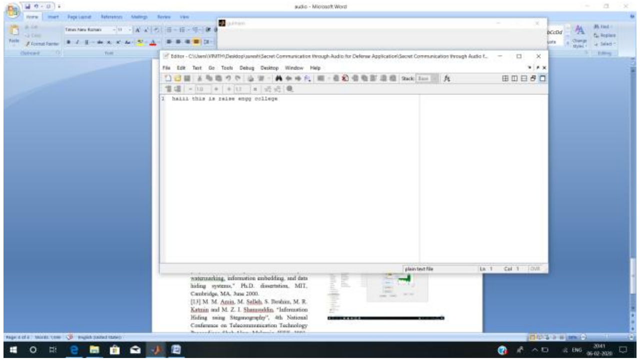


Input audio signal



Embedding process completed

Data embedding


audio - Microsoft Word
Editor - C:\Users\VINITH\Desktop\suresh\Secret Communication through Audio for Defense Application\Secret Communication through Audio f...
File Edit Text Go Tools Debug Desktop Window Help

```
haiii this is raise engg college
```

Retrieval screct message

Advantages:

- Secrecy
- Imperceptibility
- High capacity

Applications:

- Military Applications
- Secured Data Transmission

III. REFERENCES

[1] 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.