A New Encrypted Secret Message Embedding In Audio using LSB Based Stenography with AES

C. P. Bhargavi[1], G. Mahitha[2], D. Sai Divya[2], G. Abhishiktha Shiny[2], D. Akhila[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Electronics and Communication Engineering
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Hyderabad, Telangana, India

Abstract: Steganography is used in this work to encode text into an audio file. It is recommended that the textual information being incorporated through every bit of audio data once it has been converted as bits. The message character was initially transformed towards its binary counterpart during the embedding procedure. The last four bits of this binary code are taken into account, as well as the prefix 0 or 1 is utilised to implement binary code redundancy. Control symbols that binary form are used to distinguish upper- and lowercase letters, spaces, and numbers. The ability of the stego system to disguise the text is increased by applying the suggested LSB-based method. The assessment of evaluation is based on MOS, having 20 samples being taken as well as the SNR values being compared to those of certain well-known and suggested algorithms.

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

1. INTRODUCTION

Using the technique of steganography, data or secret messages may be sent via an open channel without a third party being able to decipher its contents. Traditional encryption is to hide the content underlying secret communications; steganography's purpose is to conceal the fact that secret messages occur in the first place. Electronic media seems to be the primary focus of modern steganography, and tangible artefacts are seldom used in this kind of work. Numerous techniques to disguise data in channels comprising images [1, 2, 3], video [3, 4], audio [1, 3], and sometimes even typeset text [1, 3] have been proposed. There are several reasons why this is a good idea. First and foremost, electronic media are so much simpler to alter in order to conceal data and extract messages since the quantity of the information is often very tiny considering the size of something like the data in which it must always be buried (the cover text). A second advantage of using electronic data would be that computers are capable of effectively manipulating it and running the algorithms required to recover the messages. Messages may be hidden by manipulating superfluous, unneeded, and unobserved data gaps in electronic data. Finding a means to utilise audio files for host media for hiding textual messages while without altering the files' structure or content was central to this paper's mission. Whereas a change there in cover object's perceived quality might lead to a failure for steganography's intended goal, deterioration of both the cover object's quality should be avoided.

Desired Characteristics of Stenography:

There are three main criteria for such a steganography system: imperceptibility when embedding, accuracy of recovering embedded information, and substantial payload (the bits sent to the end user at the destination) [1]. Only the sender and recipient are aware of the message's steganographic encoding method while using pure steganography. [10, 11] These are desirable elements of a successful steganographic scheme: A person are now unable to retrieve the secret data from either the host media unless they have access towards the secret key that was used during the extraction process. The hidden data should not be detectable from either the original media after it has been inserted. The concealed data in the medium should never be a cause for concern. Hidden messages should be as lengthy as feasible [30] to maximise their capacity. That example, a lossy compression strategy may alter host media, but the hidden data should still be capable of surviving. To ensure the integrity of the information extracted first from medium, effective extraction must be precise and dependable.

2.EXISTING SYSTEM

2.1 Audio cryptography

Is there any benefit to having more security if you're already paranoid? Is it possible that we are naive enough to assume that we don't require fundamental security measures? As even the Internet has become a vital means of communication and commerce among tens of millions of people, security has become more crucial for everything from business transactions and payments through private messages and the safeguarding of passwords.

2.2 Public-Key Cryptography

In the previous 300-400 years, public-key cryptography has indeed been hailed as the greatest important advancement in cryptography. The first public description of modern PKC were published in a scientific journal. Two-key cryptography, as outlined in their article, allows two parties to communicate securely across an insecure channel without sharing a secret key.

PKC relies on the presence of so-called one-way functions, which seem to be mathematical functions that really are cheap to calculate, but whose inverse function was difficult to compute. Messages may be sent using this method with ease. Let's say Alice wishes to communicate with Bob. Bob decrypts this encrypted text with the help of Alice's private key, which she uses to encrypt some data. The sender of a communication might be identified using this technique.

2.3Disadvantages of Cryptography:

- Transmission time with documents encrypted utilizing public key cryptography For transmission of extremely big documents was prohibitive.
- This key sizes would have to be much bigger to ensure the high degree of security.
- Public key cryptography was prone to impersonation attempts.

3.PROPOSED METHOD

The technique of cover creation encrypts data in the same manner as a cover enabling secret communication was formed. Phase Coding embeds data by modifying the phase in such a preset way while trying to hide information into a digital sound. Your human hearing system is limited in its ability to detect phase changes in such a signal (HAS).

3.1Design Methodology

".wav" files have been chosen as even the host files for this experiment. To avoid diminishing its sound quality, it really is generally accepted to alter only the most insignificant bits[34] of something like the file. To begin, one must be familiar with the audio file's file structure. Both header plus data are the two primary components of WAV files, as is the case with the majority of other types of files. Initial 44 bytes of such a wav file are reserved for the header. All but 44 bytes of something like the file were dedicated to storing data. This data consists of a single, massive collection of audio samples. When embedding data, every header section is out of the question. As a result of such audio file being corrupted due to a little change inside the header section.

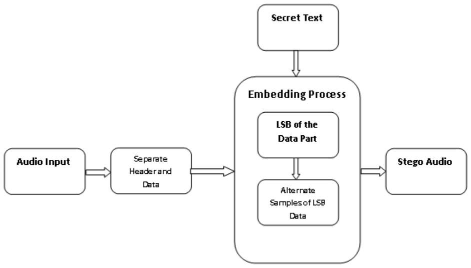
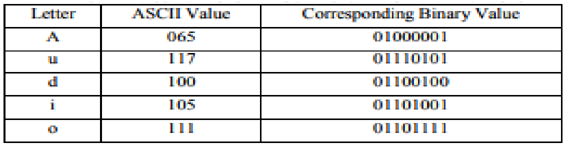


Fig: embedding process

Bit by bit, an audio file may be read then stored in a new file using a tool that was built specifically for this purpose. Those were the first 44 bytes of something like the header section and should not be altered. Begin by making changes to the additional data fields so that text may be embedded. For instance, if the word "Audio" is to be included in an audio file, all binary values from "Audio" should be included in the audio data.



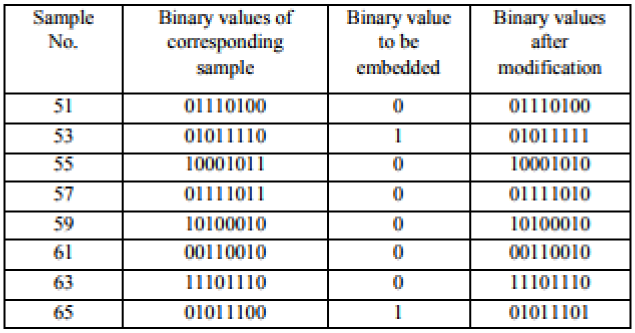
Letter	ASCII Value	Corresponding Binary Value
A	065	01000001
u	117	01110101
d	100	01100100
i	105	01101001
o	111	01101111

Table:text for corrsponding binary values

Several bits of every sample file were edited or changed to incorporate text data as part of the development of this programme. This host audio file suffers once the bits are changed, as has already been documented. One, two, three, and four bits were all altered in different ways. However, upon the completion of all revisions, an observation was made.

3.2 Algorithm (For Embedding of Data):

- ➢ Keep the audio file's header portion as it is...
- ➢ Begin at a logical starting point in the data. This 51st byte was used as a starting point again for experiment. Remove or alter the tiniest portion of the data that must be encoded.
- ➢ The least important part of each alternative sample should be changed in order to embed 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

Table: Embedding of Data with help of audio samples

On the receiver's end, the very same reasoning is used to the data retrieval procedure.

Algorithm (For Extracting of Data):

Leave first 50 bytes.

- Keeping track of the least significant bit begins with byte number 51.
- A left shift of both the preceding bit is performed on every alternative sample to save its least significant bit.

- This secret message's ASCII values may be derived by converting the binary numbers to decimal.
- • Decipher the secret message hidden inside the ASCII code.

3.3EXTRACTION PROCESS

This audio file "audio.wav" changes very little when the planned binary values are replaced with the current binary values, and this change is nearly undetectable to anybody except the sender. To retrieve data somewhere at receiver's end, it is necessary to adhere to the retrieval algorithm: A stego-object is a binary representation of an audio message which has been encoded by the source. Do not alter the very first 50 bytes.

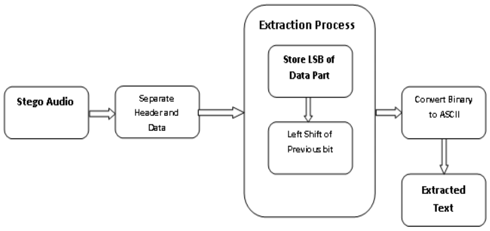


Fig 3.1: retrieval process of secret text

Set a queue of bits beginning with 51 and then verify the least significant bit. Use each example to get a complete picture of what's going on. 53rd, 55th, 57th, and so on. Save the samples' least significant bits in such a queue and then move the preceding bit left. This text may be recovered by converting the binary values into decimal and then back into ASCII.

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: retival process coreesponding audio sample

This following table depicts the entire retrieval procedure in further detail.

Advantages:

- Secrecy
- Imperceptibility
- High capacity

Applications:

- Military Applications
- Secured Data Transmission

4. RESULTS

This section gives the detailed analysis of simulation results implemented using MatlabR2016a. Further, performance of proposed approach is compared with state of art approaches using same dataset.

4.1 Dataset

The dataset contains the voice samples from five different persons. From each person 9 samples are collected with multiple phrases. Totally, 45 phrases are collected in entire dataset. Further, 80% of dataset is used for training, 20% of dataset is used for testing the Audio stego systems.

4.2 Objective evaluation

In this section, several quality metrics are utilized in order to verify the quality of the encrypted and decrypted speech signals and to determine the cryptosystem's immunity against a variety of cryptanalysis attacks [9]. In addition, the quality of the encrypted and decrypted speech signals is used to determine the cryptosystem's immunity. The results of the simulation are implemented using Matlab on a personal laptop of the type HP (Intel CORE i3) with Windows 7 operating system. The TIMIT database is searched at random for five speech signals to use as testing materials. These five speech signals have lengths of 1.4150, 2.8550, 3.3150, 4.7350, and 5.3950 seconds, respectively, and a sampling frequency of 16 KHz.

Figure displays the waveforms of the original speech signal, the ciphered speech signal, and the decoded speech signal for the final test speech signal. 4. Through examination of Figs. 4a and 4b, it is possible to see that the ciphered speech signal that is created by the provided scheme is completely different from the speech signal that is fed into the system. It is incomprehensible, comparable to white noise, and exceedingly uniform, which indicates that there is no residual intelligibility in the ciphered speech signal. This is because it is akin to white noise. On the other hand, when analyzing the data shown in Figs. 4a and 4c, it can be seen that the original signal and the decoded speech signal that was produced through the process of decryption are exactly the same. This suggests that the signal that was recovered is of a high quality and precise to a great degree.

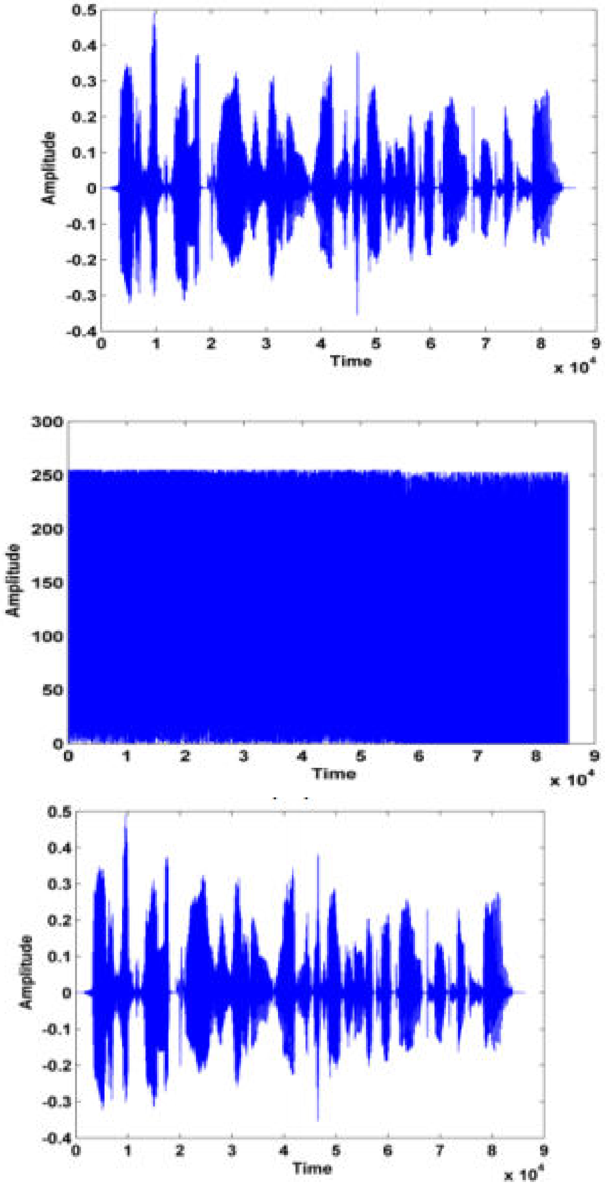


Fig. 4: (a) Original Speech Signal, (b) Ciphered Speech Signal, (c) Deciphered Speech Signal

Differential analysis: A modified speech signal is created by inverting the bit that is considered to be the least important in each sample. The input and changed speech signals are both ciphered using the same key, which results in the production of two encrypted speech signals.

Table 2: Quality Metrics Values for Encrypted Signal

Signal name	SNR (dB)	PSNR (dB)	NPCR	UACI	CC
Signal 1	-61.4085	6.0671	99.96	37.2940	3.1683 × 10−4
Signal 2	-62.7880	6.0823	99.96	37.2066	−1.6828 × 10−4
Signal 3	-62.5135	6.1119	99.96	37.0317	4.8035 × 10−4
Signal 4	-64.8471	6.0914	99.98	37.1593	−7.2535 × 10−4
Signal 5	-65.4124	6.1153	99.97	36.9895	−6.2950 × 10−4

After that, the two encrypted speech signals are compared using two criteria that are standard: the Number of Pixels Change Rate (NPCR), the Unified Average Changing Intensity (UACI), the Signal to Noise Ratio (SNR), the Peak Signal to Noise Ratio (PSNR), and the Correlation Coefficient (CC) analysis. Both the NPCR and UACI should be at their ideal levels of 100% and 33.3%, respectively. Table 2 contains a listing of the NPCR and UACI values that were acquired from the work that was recommended for various voice files. The data shown in this table demonstrates that all of the NPCR and UACI values are quite close to those considered to be optimal. As a result, the differential analysis will not break the voice cryptosystem that has been presented.

Spectrogram analysis

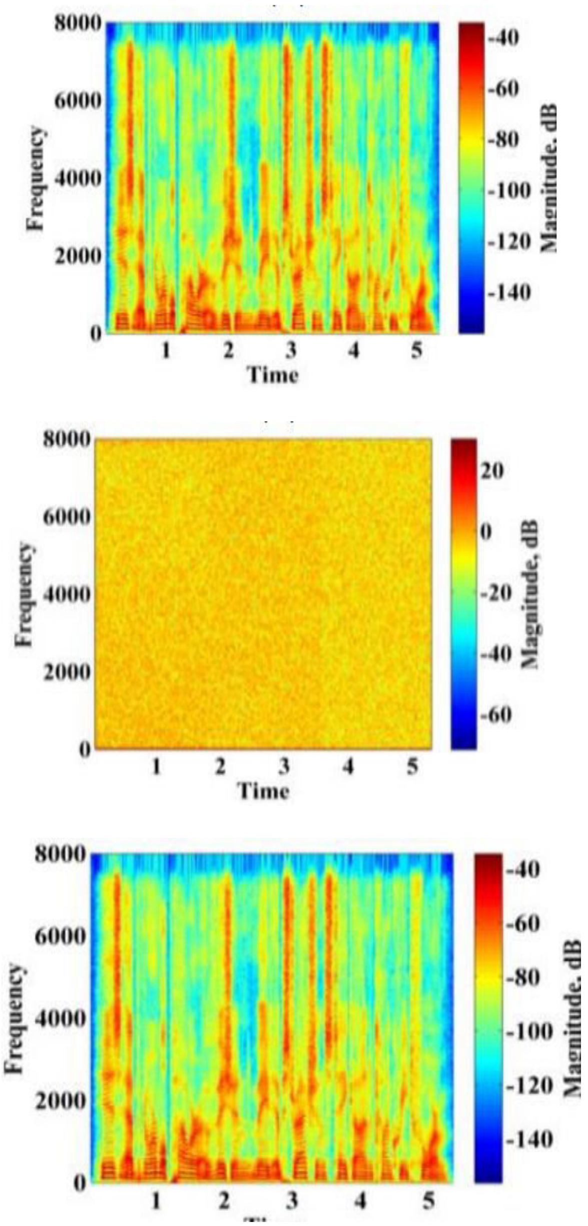


Fig. 6: Spectrograms of (a) Original Speech Signal, (b) Ciphered Speech Signal, (c) Deciphered Speech Signal

A spectrogram is a graphical depiction of the frequency spectrum, showing how the frequencies change over the course of a spoken stream over time. Figure displays the spectrograms of the original, ciphered, and decrypted voice signals that were generated by the cryptosystem that has just been described. 6. When compared side by side, this is quite obvious. 6a and 6b that the ciphered signal spectrogram is completely different from the original signal spectrogram, which indicates that the encryption process is of good quality; this is shown by the fact that the original signal spectrogram has been altered. In addition to this, it may be seen clearly by contrasting Figs. 6a and 6c show that the spectrograms of the decrypted signals and the original signals are identical, which is evidence that the process of decryption is of a high quality.

5.Conclusion and future work

Because of its low processing requirements and ease of use, LSB modification is indeed a straightforward and effective operation. However, this method is simply concerned with replacing the least important bit in order to disguise the hidden information. Concerns about the safety of LSB must be addressed. Secret information may be accessed easily if the intruder can identify which part of both the cover message has been altered to include secret information. Two methods for inserting bits at random locations are proposed as an improvement to the LSB approach in order to avoid this issue. As a consequence, the intruder must be able to determine the exact location of each bit inside the cover message, which necessitates a greater amount of time and processing resources. As an additional layer of protection, the Advanced Encryption Standard (AES) has already been used. Our project's ultimate purpose would be to implement and evaluate the findings of both the simulation on point-to-point Link Communication. Eventually, the initiative might be developed into a finished product for use against security agencies and anyone concerned with safe communication. Like cryptographers, stereophonics may be created to insert any secret message into real-time even when you are talking to another person and can be used in the same way.

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.