Data Hiding using Audio Steganography Considering Less Distortion of Cover Data for Nuclear Data

Md. Shamimul Islam[*], Nayan Kumar Datta, Md. Mahbub Alam, Dr. Md. Dulal Hossain, Dr. Md. Shakil Ahmed

Institute of Computer Science, Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, Ganakbari, Savar, Dhaka-1349, Bangladesh

[*]***shamimul32@gmail.com***

Abstract

In the modern era, we cannot imagine a single day without the internet and vast use of the internet of things (IoT). Due to the rapid growth of the internet and millions of smart devices, secure data communication becomes a challenging task for data sending and receiving sites in the wireless data communication field. So, when we consider a secured Digital Information exchange especially Nuclear related data exchange, it may require private, secure, invisible, and avoiding malicious communication. Audio Steganography is a mechanism in which a secret nuclear data message is being concealed audio cover file on the sender end and it is retrieved on the receiver end. In the proposed work, we focus on the implementation of audio steganography using the Least Significant Bit (LSB) algorithm technique. Then we evaluate the performance considering the file distortion, impairment, capacity. Our experimental study proved that how the LSB technique improves the robustness of the embedded audio stream. It also provides high-level security to the universal cyber data wherein the intruder is unable to distinguish between the original audio and the embedded audio streams.

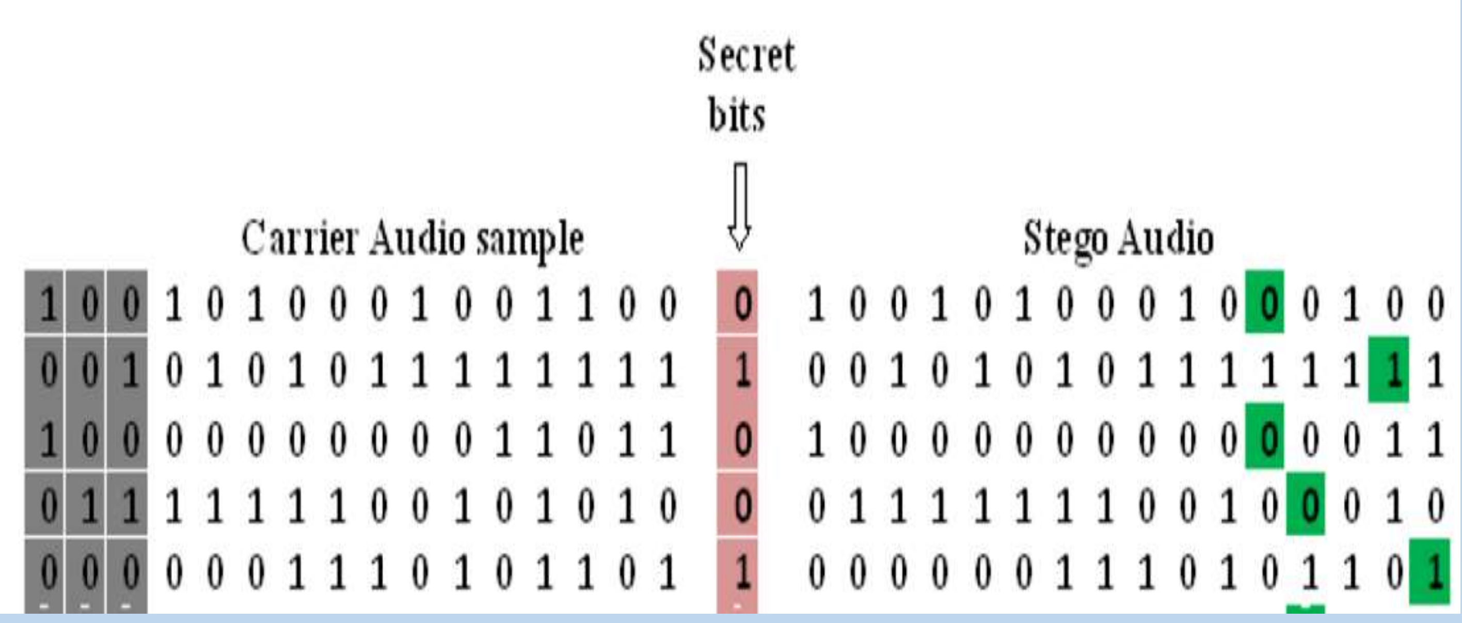
Keywords: Nuclear Data, Data security, Audio steganography, Data Communication, Least significant bit (LSB)

Introduction

Audio Steganography is a technology that is used to hide secret information in digital media, thus hiding the fact that secret communication is taking place. By hiding secret information in less suspicious digital media, well-known channels, for example e-mail and social networking sites, are avoided, thereby reducing the risk of information being Leaked in transit. Should an attacker attempt to intercept the communication through a man-in-the-middle attack, he would have no reason to suspect that he has intercepted anything more that an innocent audio. Steganography can be used to enhance the security of various applications, including secure communication. Implementing LSB algorithm, audio steganography ensures data security especially nuclear data transmission in terms of payload capacity, robustness against manipulation attack, statistical un detectability and invisibility.

Methodology

For audio steganography, LSB (Least Significant Bit) algorithm replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. In our proposed work, the secrete message has to encrypted with some standard encryption algorithm with a key supplied by the sender and shared with the receiver. Then the position for insertion inside the sample of the carrier audio file has to be selected based on the decimal value of first 3 MSB bits. Then one bit of the secrete message has to be inserted at the 4th position of the corresponding sample of carrier audio file. After the decimal value for 3 MSB bits are considered for the next sample and similarly the next secrete bit has to be put at the decimal valued position and the process will be repeated for each bit in the secrete message till the full secrete message is hidden.



1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 | 0 | 1 0 0 1 0 1 0 0 0 1 0 0 0 1 0 0

0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 | 1 | 0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1

1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1 | 0 | 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1

0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0 | 0 | 0 1 1 1 1 1 1 1 0 0 1 0 0 0 1 0

0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 | 1 | 0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1

Fig: Bits of a secret Message are embedded in a 16-bit sample

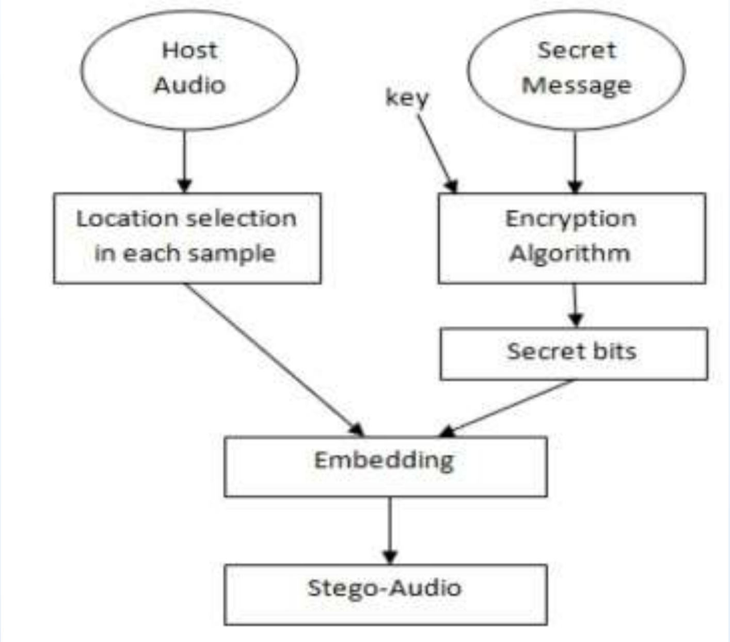


Fig: Encoding process

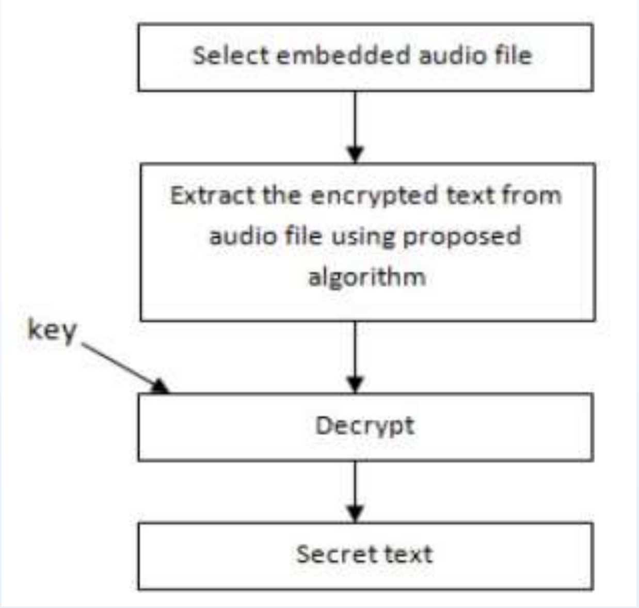
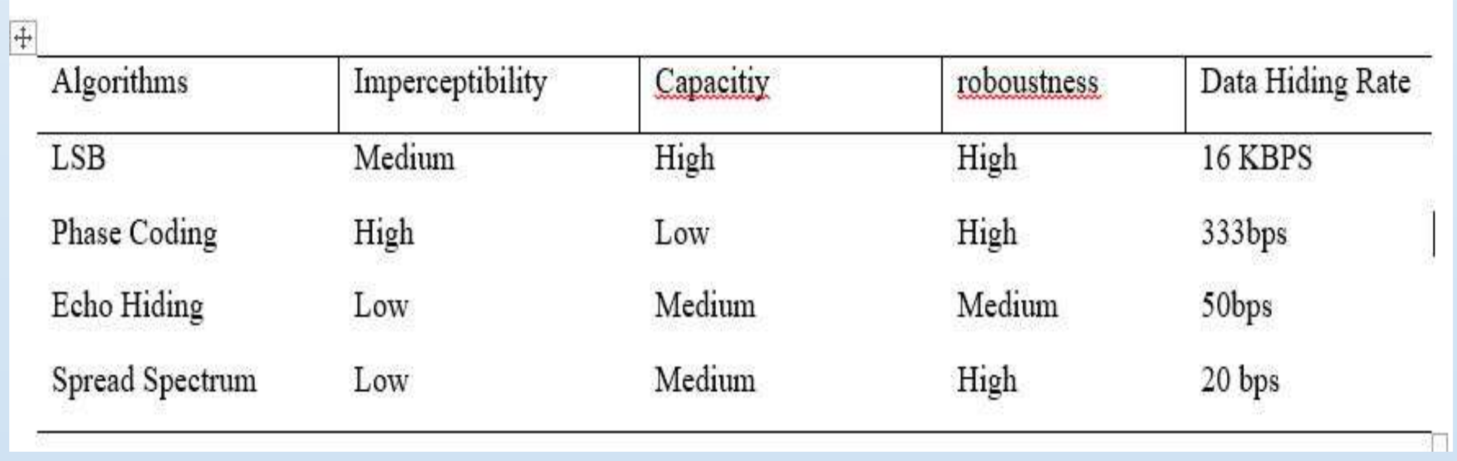

Select embedded audio file
Extract the encrypted text from audio file using proposed algorithm
key
Decrypt
Secret text

Fig: Decoding Process

Result and Discussion

In our research, we have compared our result with other algorithms which specifies more acceptability values of capacity, robustness and imperceptibility.



Algorithms	Imperceptibility	Capacitiy	roboustness	Data Hiding Rate
LSB	Medium	High	High	16 KBPS
Phase Coding	High	Low	High	333bps
Echo Hiding	Low	Medium	Medium	50bps
Spread Spectrum	Low	Medium	High	20 bps

Fig: Audio steganography comparison results.

In the above result we can make a decision that LSB algorithm is more reliable to secure communication nuclear related data over real world communication world. Our proposed algorithm and technique ensure more security in terms of data hiding which also reduces PSNR(peak signal ration) and chance of Human Auditory System(HAS).

Conclusion

In order to provide better protection for transfer nuclear digital data over insecure communication medium, our defined modified least significant bit Algorithm applied under audio file as cover media provides better performance. Audio steganography techniques address issues related to the need to secure and preserve the integrity of data hidden in voice communications in particular. Various quality measures (PSNR, MSE, and SSIM) achieved values up to satisfaction. The proposed methodology successfully achieves the research objectives in terms of capacity, invisibility and robustness.