# International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Kaur *et al.*, 9(8): August, 2020]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# HIDING TEXT DATA IN AUDIO SIGNALS USING 3BIT LSB TECHNIQUE AND DCT APPROACH

**Ramandeep Kaur (Mtech) & Sarbjeet Kaur**
Adesh College of Engineering and Technology, Faridkot

**DOI**: https://doi.org/10.29121/ijesrt.v9.i8.2020.11

## ABSTRACT

Steganography is that the limit and examination of encompassing lined messages during aperspective that no one, nearby the sender and foreseen beneficiary, interfaces the part withthe message, a kind of security through nonattendance of clearness. The present strategy ofAudio Steganography addresses extra camouflages on the picking of sound reports. The proposed system use 3 Bit LSB Stegnography to hide the text data into an audio signal. Proposed system is evaluated on various input data containing from various sources. The performance of the proposed system is also compared with the performance of existing system.

**KEYWORDS**: audio stagnography, text data hiding, data security, secure transmission, stegnpgraphy.

## 1. INTRODUCTION

Steganography is that the limit and examination of encompassing lined messages during a perspective that no one, nearby the sender and foreseen beneficiary, interfaces the part with the message, a kind of security through nonattendance of clearness. Steganography works by powerful bits of immaterial or unused learning in unavoidable PC records, (for example, plot, sound, substance, HTML, or perhaps floppy circles) with bits of different, unnoticeable information. This verified information will be plain substance, figure message, or potentially film.

In a PC essentially based sound Steganography structure, bewilder messages are showed up in extraordinary sound. the key message is appeared by likely dependably changing the twofold virtuoso of a sound record. Existing sound Steganography programming will present messages in WAV, AU, and even MP3 sound records. Showing issue messages in innovative sound is a significant bit of the time an a ton of exhausting framework than showing messages in elective media, for instance, motorized photographs. These systems stretch out from rather basic figurings that supplement data as sign cry to even an enormous extent of veritable strategies for thinking that have pushed sign guiding approaches to manage administer spread data.

## 2. METHODS OF AUDIO STEGANOGRAPHY

### LSB Coding

Coding is that the most quick appreciation to manage present information in a dynamic sound record. By subbing the base pivotal smidgen of each reviewing reason with a twofold message, LSB creating contemplates a sensational course of action of figuring out how to be encoded. The going with diagram depicts at any rate the message "Hi" is encoded in a very 16-bit CD quality model maltreatment the LSB structure.

### Phase Coding

Stage mystery composing watches out for the drawbacks of the tumult causation strategies for sound Steganography. Stage mystery composing relies on the route during which that the stage areas of sound aren't as noticeable to the human ear as tumult might be. as opposed to showing burdens, the strategy encodes the message bits as stage advancements inside the stage extent of an automated sign, accomplishing Associate in Nursing confused cryptography similarly as sign to-saw energy degree.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

**Spread Spectrum**

Spread vary frameworks encipher data as a paired grouping that looks like clam or nonetheless which may be perceived by a recipient with the proper key. the strategy has been utilized by the military since the Nineteen Forties in light-weight of the very fact that the signs are burdensome to remain or close as they're uncomprehensible such a great amount out racket. unfurl fluctuate systems is utilized for watermarking by sorting out the tight transmission point of confinement of the acquainted data with the various trade speed of the medium. 2 translations of SS is utilized as a touch of sound Steganography: the brief movement and continue skipping plans. In direct-plan SS, the puzzle message is unfurled by a sure alluded to as the chip rate and after that decent with a pseudorandom signal. it's at that point interleaved with the unfoldsign. In continue ricocheting SS, the sound record's rehash change is balanced with the objective that it bobs now between frequencies. unfurl Spectrum Steganography has enormous potential in secure correspondences – business and military. Sound Steganography related with unfurl Spectrum may give encased layers of security.

## 3. LITERATURE SURVEY

Manisha Verma[1], In today's digital world one is concerned with the secrecy of data and focused on copyright-dependent individuals and organizations, specifically in the domain of the entertainment industry. The variations in the human voice lead to the difficulties to generate the watermark to the audio signals in order to preserve them from unauthenticated access. The major objective of the steganography process is to enhance the security of the transmitted data. The unauthorized user can not access or misuse the steganographic file. Audio steganography is also applicable to the non-technical fields in order to keep the privacy and security of the data. This paper presents a review of recent research on audio steganography. The major focus of the study is to address various types of audio steganographic techniques along with their pros and cons. There is a need to find technique so that the data hiding is done more securely and it is not possible for the third parties to detect the data in bits.

Abdullah M Basahel[2],The great developments in the world of communications and the advancement of the associated technologies, such as the Internet of Things (IoT) with web-based and mobile applications, have changed our way of life. This has created a kind of linkage between virtual and real worlds, rendering applications and services to be ubiquitous. We are also witnessing a phenomenon in which the electronic devices that connect to the Internet and are widespread making use of technology and providing a better level of service to users. However, sending and receiving information over the Internet generates many issues and problems. The most serious of them is the security and protection of transmitted information. This issue has become one of the most important things which is a matter of concern to researchers as well as the users themselves. Ensuring privacy and security of the transmitted data is a matter of urgency and cannot be neglected while dealing with the transmission of data using the services and tools in the IoT. In this article, we provide an improved algorithm to increase the protection level of transmitted information by means of cryptographic encryption so that this information cannot be seen by others or disclosed to anybody. This algorithm has been evolved as an application that works on mobile phones so that any user can benefit from it when exchanging sensitive and confidential information such as account numbers and passwords with other users.

Siddalingesh Bandi[3], Recently, security has become the prime concern for any organization and other civil and military applications. In this field of security, the data security during communication over an insecure wireless channel is the most important task which can be done by performing cryptography, watermarking and steganography. However, cryptography and watermarking schemes can be identified easily because of change in the data structure hence attackers can focus on that particular part to hack the secret information whereas steganography is a hiding mechanism in which secret message can be concealed into the cover and it can be retrieved at the receiver end. Several techniques have been introduced during last decade which are focused on image-image steganography and audio steganography. In the proposed work, we concentrate on audio steganography and develop a novel approach where secret message can be in the form of plain text or image, whereas cover message is in the form of audio. In order to provide additional security to this model we incorporate AES encryption scheme where secret message is encrypted and hidden in the cover audio. The proposed approach uses DCT coefficient computation and AES encryption scheme. An extensive experimental study is carried based on different test cases and evaluated against state-of-art techniques. The experimental study shows that the proposed approach achieves better performance for audio steganography.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

## 4. PROPOSED METHODOLOGY

Proposed System utilize 3 BIT Least Significant Bit (LSB) to shroud the instant message into sound sign. # Bit least noteworthy piece (3-LSB) coding is the most straightforward approach to install data in a computerized sound document. By substituting the least noteworthy piece of each testing point with a parallel message, LSB coding considers a lot of information to be encoded.

**Bit Least-Significant Bit (LSB) Technique**

The least enormous piece (toward the day's end, the eighth piece) of a couple or most of the bytes inside an image is changed to a pinch of the puzzle message. Electronic pictures are generally of two sorts (I) 24 bit pictures and (ii) 8 bit pictures. In 24 bit pictures we can embed three bits of information in each pixel, one in each LSB position of the three eight piece regards. Extending or decreasing the motivating force by changing the LSB does not change the nearness of the image; much so the resultant stego picture looks essentially same as the spread picture. In 8 bit pictures, one bit of information can be concealed.

**Algorithm to hide the text message into an audio signal:**

**Phase 1 (Data Hiding Phase)**

Stage 1: Input the .wav sound document in which information is to be covered up.
Stage 2: Input the instant message.
Stage 3: Encrypt the document utilizing the encryption method.
Stage 4: Compress the instant message utilizing Adaptive Huffman Coding.
Stage 5: Extract the header from the .wav document.
Stage 6: Store the quantity of bits to be covered up into header of .wav document.
Stage 7: Using 3-LSB method cover the message bits into .wav document in an exchanging positions.
Stage 8: Rejoin the .wav tests to make the yield document.
Stage 9: Compress stego sound utilizing DCT pressure alongside run length encoding.
Stage 10: Store and show the document to client.

**Phase 2 (Data Extraction Phase)**

Stage 1: Input the .wav record in which information is covered up
Stage 2: Extract the header and afterward complete number of shrouded bits.
Stage 3: Extract the bits from exchanging 3-LSB positions from the .wav tests.'
Stage 4: Combine the message separated from 3-LSBs.
Stage 5: Display

## 5. RESULTS AND DISCUSSION

The proposed system hides the text data into audio samples using LSB technique. Proposed system is evaluated on the basis of various parameters which are as follows:

**SNR (Signal to Noise Ratio):** is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB).

**Compression Ratio (CR):** Compression ratio can be defined as the ratio between output bits generated and total number of input bits.

The results statistics of the proposed system is shown as below:

***Table 5.1 Statistics of the proposed system:***

| FILE NAME | AUDIO FILE | ENTR-OPY | AVERAGE LENGTH | REDUN-DANCY | TOTAL BITS | COMPRE-SSED LEzNGTH | COMPRE-SSION RATIO | SNR |
|---|---|---|---|---|---|---|---|---|
| Sample 1 | inp1.wav | 18501 | 1.3 | 1.2147 | 94 | 22 | 0.23 | 86.221 |

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Sample 2 | inp2.wav | 1.1219 | 1.82 | 2.3863 | 70 | 18 | 0.25 | 85.218 |
| Sample 3 | Inp3.wav | 1.6464 | 2.2 | 1.3449 | 74 | 21 | 0.28 | 89.239 |
| Sample 4 | Inp4.wav | 2.6402 | 2.45 | 0.6234 | 110 | 52 | 0.47 | 86.624 |
| Sample 5 | Inp5.wav | 1.4321 | 3.12 | 0.5234 | 92 | 38 | 0.41 | 87.219 |

***Table 5.2 Comparison of the proposed system with the existing system on the basis of the SNR values:***

| FILE NAME | AUDIO FILE | SNR value in existing system | SNR value in proposed system | Improvement |
|---|---|---|---|---|
| Sample 1 | inp1.wav | 79.94 | 86.221 | 6.06 |
| Sample 2 | inp2.wav | 80.89 | 85.218 | 4.32 |
| Sample 3 | Inp3.wav | 84.17 | 89.239 | 5.06 |
| Sample 4 | Inp4.wav | 79.73 | 86.624 | 6.89 |
| Sample 5 | Inp5.wav | 81.22 | 87.219 | 5.99 |

***Table 5.3 Comparison of the compression of file with and without RLE:***

| FILE NAME | AUDIO FILE | Original Size | Compression existing | Compression with Modified Huffman | % Compression |
|---|---|---|---|---|---|
| Sample 1 | inp1.wav | 312500 | 164473 | 71875 | 23 |
| Sample 2 | inp2.wav | 453000 | 251666 | 113250 | 25 |
| Sample 3 | Inp3.wav | 233315 | 101441 | 65328 | 28 |
| Sample 4 | Inp4.wav | 415212 | 278202 | 195149 | 47 |
| Sample 5 | Inp5.wav | 325653 | 154337 | 133517 | 41 |

The above table represents the comparison of the existing and proposed system on the basis of compression ratio parameter. It is shown that the compression ratio of the proposed system gives better results than that of the existing system on the same type of the data given. The above table represents the compression ratio of the existing and proposed system and their corresponding difference is given.

Graph representing the comparison of existing and proposed system on the basis of SNR:

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

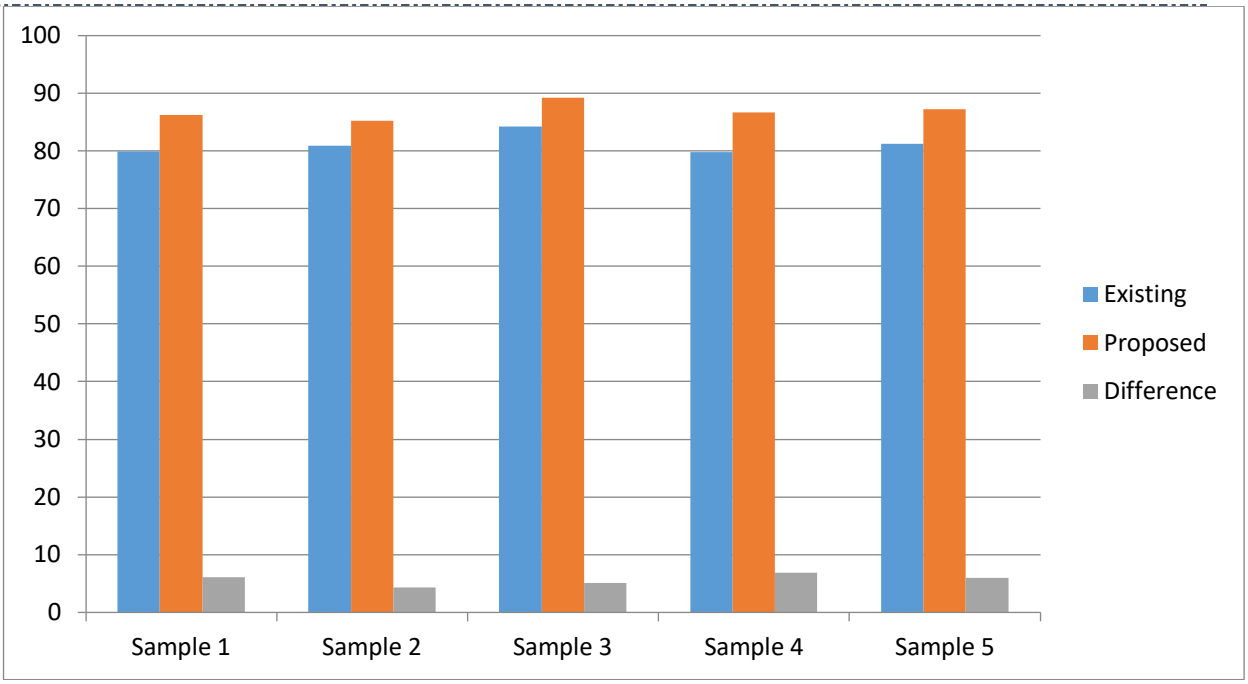


***Figure 5.1: Comparison of SNR***

## 6. CONCLUSION AND FUTURE SCOPE

**Conclusion**

Steganography is an effective way to hide sensitive information. In the proposed work we have used the 3-LSB Technique and Modified Huffman Compression Technique on audio signals to obtain secure stego-signal. The compression algorithm is used to compress the text data that is to be hidden in the audio signal. With the help of the proposed compression algorithm large text messages can be hidden into the smaller audio signals. The results are improved as compared to the existing approach which reflects that the new approach is better in terms of security and speed in data transmission. Table 5.2 shows comparison of SNR in existing and the proposed system, which is better than that of the existing system. Our results indicate that the 3- LSB insertion using Modified Huffman Compression is better than simple LSB insertion in case of lossless compression. The audio signal samples doesn't change much and is negligible when we embed the message into the audio signal. The algorithm use 24 bit data samples, therefore a negligible change will be in the audio signal that results in better SNR values.

**Future Scope**

Proposed system can be used to hide the secret messages written in text format into audio signals. Proposed system can only hide the text data into an audio signal. Further improvements can be made by using random encoding along with different media types for secret messages.

## REFERENCES

[1] Manisha Verma, Hardeep Singh Saini,"Analysis of Various Techniques for Audio Steganography in Data Security",IJSRNSC, Volume-7, Issue-2, Apr 2019
[2] Abdullah M Basahel,MohammadYamin,Adnan Ahmed Abi Sen,"Enhancing Security of Transmitted Data by Improved Steganography Method", IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.4, April 2019
[3] SiddalingeshBandi, Manjunatha Reddy H S,"Combined Audio Steganography and AES Encryption to Hide the Text and Image into Audio using DCT",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019
[4] YoussefBassil,"Audio Steganography Method for Building the Deep Web", American Journal of Engineering Research (AJER),2019,Volume-8, Issue-5, pp-45-51

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[5] Dingwei Tan, Yuliang Lu, Xuehu Yan and Xiaoping Wang"A Simple Review of Audio Steganography",2019 IEEE 3rd Information Technology,Networking,Electronic and Automation Control Conference (ITNEC 2019) [6] M.BarithaBeguma ,Y.Venkataramanib, LSB Based Audio Steganography Based On Text Compression, International Conference on Communication Technology and System Design 2011, 1877-7058 © 2011 Published by Elsevier Ltd. doi:10.1016/j.proeng.2012.01.917.

[6] Swati Malviya1, Manish Saxena2, Dr.Anubhuti Khare3, Audio Steganography by Different Methods, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012).

[7] Ali M. Meligy,Mohammed M. Nasef and Fatma T. Eid,An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys, I. J. Computer Network and Information Security, 2015, 7, 24-29. Published Online June 2015 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2015.07.03, Copyright © 2015 MECS,

[8] Harleen Kaur1, Meena Aggarwal2, Amrinder Kaur3, Data Concealing Using Audio Steganography, Kaur et al., International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-4, Issue-6), © 2015, IJERMT All Rights Reserved.

[9] HilalAlmara'beh, Steganography Techniques - Data Security Using Audio and Video, Almara'beh International Journal of Advanced Research in Computer Science and Software Engineering 6(2), February - 2016, pp. 45-50, © 2016, IJARCSSE All Rights Reserved.

[10] Ifra Bilal and Rajiv Kumar, Audio Steganography using QR Decomposition and Fast Fourier Transform, Indian Journal of Science and Technology, VOL 8(34),DOI: 10.17485/ijst/2015/v8i34/69604, December 2015.

[11] Ali M. Meligy,Mohammed M. Nasef and Fatma T. Eid, An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys,I. J. Computer Network and Information Security, 2015, 7, 24-29. Published Online June 2015 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2015.07.03, Copyright © 2015 MECS.

[12] Jasleen KourDeepankarVerma,Steganography Techniques –A Review Paper, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5).

[13] Navneet Kaur, Sunny Behal, Audio Steganography Techniques-A Survey, Navneet Kaur Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 6( Version 5), June 2014, pp.94-100.

[14] Ajay.B.Gadicha, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5, November 2011.