

[Kaur\* *et al.*, 5(12): December, 2016] IC<sup>TM</sup> Value: 3.00

# **IJESRT**

# INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# STEGANOGRAPHY SYSTEM FOR HIDING TEXT INTO AUDIO SIGNAL USING I-LSB TECHNIQUE & COMPRESSION ALGORITHM (LZW & ADAPTIVE

HUFFMAN)

Sukhdeep kaur\*, Karandeep singh

\*M. Tech, Research Scholar, Department of E.C.E, Baba Farid College of Engineering, Bathinda,

India

Assistant Professor, Department of E.C.E, Baba Farid College of Engineering, Bathinda, India

**DOI**: 10.5281/zenodo.221013

# ABSTRACT

Steganography is technique to hide the secret data within a cover media such as digital images, sound files, video files in such a way that the existence of the message remains same. Audio stenography technique hides the secret data such as text or images in the audio signals. In this paper we proposed a technique for hiding the text message into audio signals using Improved LSB technique. In the proposed system the combination of Adaptive Huffman and LZW algorithm is used to compress the text message. Various test cases are performed on various inputs and results of the proposed system are evaluated on the basis of SNR and Compression Ratio, Time and MSE. Experiment results shows that the proposed system give better performance than that of existing systems.

**KEYWORDS:** Audio steganography, Improved LSB, Adaptive Huffman and LZW Compression Algorithm.

#### **INTRODUCTION**

The term Steganography is adapted from the Greek word steganography, meaning "covered writing" and is taken in its modern form to mean the hiding of information Inside other information. Naturally these techniques date back throughout history, the main applications being in couriering information during times of war.

Steganography is the technique of concealing the messages in such a manner that nobody, aside from the sender and Expected receiver, identifies the presence of the message. Steganography works by supplanting bits of futile or unused information in standard PC records like sound, content, HTML, text with bits of various, undetectable data. This Shrouded data can be plain content, figure message, or even pictures.

In a PC based sound Steganography framework, mystery messages are implanted in sound. The hidden message is fitted by marginally adjusting the paired arrangement of a sound document. The sound Steganography software can install messages in WAV, AU, and even MP3 sound records. These strategies run from rather straightforward calculations that embed data as flag clamor to all the more effective strategies that endeavor modern flag handling procedures to conceal data.

In this manner the fundamental motivation behind this class is to clarify Audio Steganography and calculations usually utilized for Audio Steganography and its applications.

#### **ADVANTAGES**

#### Storage capacity:

Audio files are generally larger in size than images. So by using improved LSB audio steganography technique large amount of data can be stored.

#### Flexibility:

Another aspect of audio Steganography that makes it so attractive is its ability to combine with existing cryptography technologies.



[Kaur\* et al., 5(12): December, 2016]

#### IC<sup>TM</sup> Value: 3.00 Less degradation:

Greater measures of data can be inserted without capable of being heard debasement.

#### Security:

Data hiding in proposed system is more secure. Without the message extraction key nobody can recover the hidden data.

#### DISADVANTAGES

#### **Robustness:**

Copyright marks covered up in sound examples utilizing substitution could be effortlessly controlled or devastated if a knave comes to realize that data is concealed along these lines.

#### **Commercial issues:**

Commercialized sound Steganography have drawbacks that the presence of shrouded messages can be effortlessly perceived outwardly and just certain measured information can be covered up.

#### **Proposed Methodology:**

Proposed System use Improved Least Significant Bit (LSB) to hide the text message into audio signal. Improved least significant bit (I-LSB) coding technique is one of the easy and simplest ways to hide information in a digital audio file. LSB coding is used to hide the large amount of information in the audio file.

Proposed system has two parts one is used at transmitter and second is used at the receiver to embed the message into an audio signal and to recover back from the emended signal at receiver. Before hiding the text message into an audio signal we have to compress the text message. In proposed methodology we used the following algorithms.

#### LZW (Lempel Zev Welch):

As we know to store a large amount of data or files we need a large data storage capacity. so to utilize the same capacity Compression is the way minimize the data size. Lossless compression method is that data compression method in which no information or data is lost during the compression. LZW algorithm is one of the examples of lossless compression technique.

LZW (Lempel Zev Welch) algorithm is discovered by Ziv and Lempel in 1977. This algorithm carries out the lossless compression by using dictionary.

The whole LZW compression algorithm is as follow:

1) Dictionary is initialized by all basic existing characters {'A'..'Z','a'..'z','0'..'9'}.

2) C defined the current or first character in character stream.

- 3) N defined the next character.
- 4) Next is output which is same as current column.
- 5) Add to dictionary (C+N).

#### **Adaptive Huffman Compression:**

Adaptive Huffman coding is also called Dynamic Huffman coding is based on Huffman compression. In these techniques the user has no knowledge about the length of the incoming text message. This technique is used to hide the text data into audio signal in live audio, video systems. Steps of Adaptive Huffman coding.

- (1) Increment the count,
- (2) Update the Huffman tree.

During the updates, the Huffman tree will be maintained its sibling property that mean the nodes are arranged in order of increasing weights. When swapping is necessary, the farthest node with weight W is swapped with the node whose weight has just been increased to W+1.

#### **I-LSB insertion technique:**

Step1: Select the text information which is to be hide.

Step 2: Compress the text information using LZW and Adaptive Huffman Coding algorithm.

Step 3: selected the .wave file and extract the header from the .wave file.

Step 4: Insert the message bits into selected .wav file by using I-LSB technique.

Step5: join the .wav samples with the header to create the output file.



[Kaur\* *et al.*, 5(12): December, 2016] IC<sup>TM</sup> Value: 3.00 Step6: Store the results on particular location and display the file.

#### Message extraction process:

Step 1: select the .wav file in which information is shielded.

- Step 2: Extract the bits from LSB in alternate positions from the .wav samples.'
- Step 3: Combine the message extracted from LSBs.
- Step 4: Decompress the message using Inverse of LZW and Adaptive Huffman coding.

Step 5: display the results.

The proposed system shields the text information into audio samples using I-LSB technique. These are the evaluated parameters:

**Time:** This parameter is defined that how much time is taken to hide the text information into the audio signal. **MSE (Mean Square Error):** Defined as a signal fidelity measure, the purpose of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of fidelity or the level of error.

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

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

#### RESULTS

FILE NAME	TIME	MSE	COMPRESS ION RATIO	SNR
Steganography	0.084	0.01066	0.4976	88.89
Audio steganography	0.107	0.01064	0.5524	88.93
Secured data transmission	0.047	0.01138	0.5233	87.45
hybrid encryption	0.12	0.01075	0.5243	88.70
novel video steganography	0.1	0.01133	0.5635	87.54

Table3. Comparison of compression ratio

File name	Huffman + BWT	Dictionary compression	Adaptive Huffman
bibliography	0.457	0.278	0.479
Technical paper	0.452	0.282	0.488
Source code in"c"	0.438	0.286	0.469
Source code in "pascal"	0.335	0.237	0.538
Text:English text	0.345	0.174	0.466

[Fig.1 Comparison of Compression ratio]

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



[Kaur\* *et al.*, 5(12): December, 2016] IC<sup>TM</sup> Value: 3.00



#### Table4.Comparison of SNR

Cover File Name	Dictionary based compression	Adaptive Huffman+ LZW
News2	64.19	88.79
Notify	75.14	87.67
Tada	64.96	87.84
Windows XP windows	68.57	88.03

[Fig.2 Comparison of SNR]



Conclusion and Future Scope

# CONCLUSION

Steganography is an effective way to hide sensitive information. In the proposed work we have used the E-LSB Technique and Adaptive 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. Compression ratio is higher than existing system, and SNR also higher than SNR of Existing techniques. Our results indicate that the I-LSB insertion using Adaptive Huffman & LZW Compression is better than simple LSB insertion in case of lossless compression. The audio signal samples don't change much and is negligible when we embed the message into the audio signal.



[Kaur\* *et al.*, 5(12): December, 2016] IC<sup>TM</sup> Value: 3.00

Proposed system can be used to hide the text messages into audio signals. Proposed system can only hide the text data into an audio signal. As we know that a large data on various public resources is present in the form digital images that includes location maps, paintings, and architects. This type of data also require some secret way for transmission. In future a more robust system can be developed that can hide text messages as well as images into audio signals.

# REFERENCES

- 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
- [2] Pooja Jain , Anurag jain and Chetan Agrawal, IMPROVING DATA COMPRESSION RATIO BY THE USE OF OPTIMALITY OF LZW & ADAPTIVEHUFFMAN ALGORITHM (OLZWH)
- [3] 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 (<u>http://www.mecspress.org/</u>) DOI: 10.5815/ijcnis.2015.07.03, Copyright © 2015 MECS,
- [4] Fatiha Djebbar, BeghdadAyady, Habib Hamamzand Karim Abed-Meraim,"A view on latest audio steganography techniques", 2011 International Conference on Innovations in Information Technology, 978-1-4577-0314-0/11/\$26.00 ©2011 IEEE
- [5] Kaliappan Gopalan, "AUDIO STEGANOGRAPHY USING BIT MODIFICATION", This paper was originally published in the Proceedings of the 2003 IEEE International Conference on Acoustics, Speech, & Signal Processing, April 6-10, 2003, Hong Kong (cancelled). Reprinted with permission. 0-7803-7663-3/03/\$17.00 ©2003 IEEE,
- [6] Gunjan Nehru1, Puja Dhar2, A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814 ,www.IJCSI.org, Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.
- [7] Jayaram P1, Ranganatha H R2, Anupama H S3, INFORMATION HIDING USING AUDIO STEGANOGRAPHY A SURVEY, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011,
- [8] 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),
- [9] 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.
- [10] 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
- [11] 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.
- [12] JasleenKourDeepankarVerma, 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 <u>www.ijera.com</u> 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,
- [15] Ankit Chadha, Neha Satam, RakshakSood, Dattatray Bade, An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution, International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013,
- [16] BANKAR PRIYANKA R. KATARIYA VRUSHABH R. PATIL KOMAL K. SHASHIKANT M. PINGLE, AUDIO STEGANOGRAPHY USING LSB, 1st International Conference on Recent Trends in Engineering & Technology, Mar-2012, Special Issue of International Journal of electronics, Communication & Soft Computing Science & Engineering, ISSN: 2277-9477,



[Kaur\* et al., 5(12): December, 2016]

ICTM Value: 3.00

ISSN: 2277-9655 Impact Factor: 4.116 CODEN: IJESS7

- [17] Tanmaiy G. Verma, Zohaib Hasan, Dr. Girish Verma, SANGHAVI MAHESH R., A Unique Approach for Data Hiding Using Audio Steganography, International Journal of Modern Engineering Research (IJMER), www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101,
- [18] HasnaParveen O H, Audio Steganography Scheme to Advance the Security of Data in Hybrid Cloud, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), International Conference on Recent Trends in Computing and Communication (ICRTCC 2015), Cochin College of Engineering & Technology, Vol. 4, Special Issue 1, June 2015,
- [19] S.S. Divya, M. Ram Mohan Reddy, HIDING TEXT IN AUDIO USING MULTIPLE LSB STEGANOGRAPHY AND PROVIDE SECURITY USING CRYPTOGRAPHY, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 1, ISSUE 6, JULY 2012, ISSN 2277-8616.
- [20] Jithu Vimal1, Literature Review on Audio Steganographic, Techniques, International Journal of Engineering Trends and Technology (IJETT) Volume 11 Number 5 May 2014, ISSN: 2231-5381.
- [21] LatikaYogita Gulati, A Review of Steganography Research and Development, Latika et al., International Journal of Advanced Research in Computer Science and Software Engineering 5(4), April- 2015, pp. 871-874
- [22] Ms. Manisha1 Ms. Maneela2, A Survey on Various Methods of Audio Steganography, Volume 4, Issue 5, May 2014, Manisha et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(5), May 2014, pp. 236-242
- [23] R. Chandramoulia and N.D. Memonb, Steganography Capacity: A Steganalysis Perspective,
- [24] Nishu Gupta1, Mrs.Shailja2, A Practical Three Layered Approach of Data Hiding Using Audio Steganography, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014.