INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Hiding secured text data in audio signals using 3-LSB technique

Kuldeep Singh
kuldeep.ddeep1@gmail.com
Adesh College of Engineering and Technology, Faridkot, Punjab

Puneet Jain
jainsboy.2008@gmail.com
Adesh College of Engineering and Technology, Faridkot, Punjab

ABSTRACT

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. A lot of work has been developed for audio steganography. But there are various problems in the existing techniques. Existing frameworks utilize just word reference-based pressure method which can be supplanted by the mixture pressure systems to accomplish progressively precise outcomes. Existing frameworks has low SNR values which must be improved to utilize the framework in reality circumstances. In the proposed work we have used the I-LSB Technique and Adaptive Huffman Compression Technique on audio signals to obtain secure stego-signal. I-LSB uses three bytes of the audio signal to hide the text data. 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.

Keywords— *Audio stegnography, LSB, I-LSB, RLE, Huffman compression*

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 a ton of exhausting framework than showing messages in elective media, for instance, motorized photographs. These systems stretch out from rather basic figuring's 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.

The present strategy of Audio Steganography addresses extra camouflages on the picking of sound reports. customer will pick just wav records to figure. more embeddings information into sound records is for the most part thought to be more covering than pictures; as appeared by the human ear is to a remarkable degree unbalanced to disturbs in sound and may in sureness see such aggravation as low in show parcel in ten million. The four frameworks referenced more outfit clients with a wonderful game-plan of affirmation and makes the occasion progressively open to everyone.

2. LITERATURE SURVEY

Fatiha Djebbar [1], Steganography has been anticipated as another elective structure to complete data security. Starting late, novel and versatile sound steganographic strategies are anticipated. a perfect sound Steganographic structure select embeddings information in collaborator degree blurred, amazing and secure system and a compact range later cleansing it by got a handle on people. In this manner, vital the fundamental check in coordinated sound steganography is to draw in solid high most remote point steganographic structures. Improvement towards dealing with a framework that guarantees high cut-off or quality and security of pervaded data has provoked stunning explicit decision inside the stream steganographic strategy. during this paper, we will with everything considered present a gift condition of aptitude writing in managed sound steganographic techniques. We will administer in uncertainty analyse their potential outcomes and repressions to ensure secure correspondence. A relationship partner degreed an examination for the kept an eye on ways is in addition appeared during this paper.

Kaliappan Gopalan [2], a strategy for embeddings sweetening degree documented sound message in associate passing detached diction for secure correspondence is appeared. The confirmed message is cared-for in associate passing compacted structure with maybe cryptography to boot as coding for

sheathed security. One piece within the larger a part of the instances of a given detached clarification is adjusted by the information bits and a key. a like key's utilised to recover the showed bits at the beneficiary. The outcomes, see able of detached sign from a clean TIMIT diction assistant degreed associate uproarious flying machine cockpit clarification, demonstrate that the procedure meets specific sincere criteria for relentless unfold and-sharp edge correspondence.

Gunjan Nehru [3], this paper is that the examination of varied structures of sound steganography utilizing totally different figurings like non inheritable estimation approach and LSB approach. we've tried totally different systems that associates in sound steganography. As we tend to be careful about no lack of protection am cautious it's the exploit and nature of creating checked messages therefore nobody, by the sender and picked up beneficiary, associates the closeness with the message, a form of security through nonattendance of clearness. In steganography, the message adjusted unfold issue message is known as host message or detached message. exactly once the substance of the host message or detached message are modified, the resultant message is assumed as stego message. At the tip of the day, stego message is mixture of host message and befuddle message. Sound steganography wants a substance or sound puzzle message to be set in within a repercussion sound message. in context on straightforwardness of material resource, the detached sound message before steganography, stego message once steganography stays same. for info stowage away.

2.1 Research Gap

Existing frameworks utilize just word reference-based pressure method which can be supplanted by the mixture pressure systems to accomplish progressively precise outcomes. Existing frameworks has low SNR values which must be improved to utilize the framework circumstances. Messages covered up in the sound flag in the current frameworks are not verify as existing frameworks utilize basic LSB encoding to shroud the messages which must be supplanted by improved LSB encoding calculation to build the security.

3. PROPOSED METHODOLOGY

Proposed System utilize Improved Least Significant Bit (LSB) to shroud the instant message into sound sign. Improved least noteworthy piece (I-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.

3.1 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 3 bits into .wav document in an exchanging position.
Stage 8: Re-join 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 LSB positions from the .wav tests.'
Stage 4: Combine the message separated from LSBs.
Stage 5: Display output.

3.2 Huffman Coding for Compression

Huffman compression algorithm is an optimal compression or prefix algorithm where the frequencies of the letters are used for lossless compression of data. This method uses a special technique for representing symbols for each word, resulting in bit strings representation. Suppose for a given text, we need to count the frequency of characters and compute a tree so that the length of the encoding text is minimum, each character is a node in the tree. The root is always zero and level numbers are represented using number of bits to encode a character. If f is the frequency, then fk is the frequency of the k th character. Here, l is the level and lk is the level of the node of k th character. Therefore, we need to find a tree which minimizes ∑k fk lk which is known as the total external weighted path length of a tree.

We consider each node having weight equal to the frequency of the characters. If there are n number of weights, the frequencies are represented as f1, f2, f3,..., fn. For these frequencies, we can build a tree whose external weighted path length is minimum.

3.3 DCT Algorithm

DCT Algorithm divides the audio signal files into various parts of having individual frequencies where the frequencies in the input audio signal are no more important are removed with the help of quantization technique and the frequencies that are very much important in the input audio signals used for decompression. As comparison to other compression techniques, DCT has various advantages that are firstly single integrated circuit can be used to implement the DCT. Secondly a lesser number of coefficients are required to combine all the information of an audio signal. It also minimizes the noise during compression and decompression and hence is being used widely.

3.4 RLE (Run Length Encoding) Algorithm

It is a very important and efficient multimedia compression technique that can be used anywhere to reduce the total number of bits in the data sequence. RLE techniques work very efficiently when there are duplicate bits of information. RLE techniques in the proposed system works in the way that is replaces the occurrences of same types of data with their total

count of the occurrences of that substring. For example, the sequence of input data is 2,2,2,3,3,3,3 then it can be replaced by (2,3) and (3,4) respectively. In the same way, operation of decompression works. It replaces the first occurrence of string with the total number of data represented by the second number.

4. RESULTS AND DISCUSSIONS

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:

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

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

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

Table 1: Statistics of the proposed system:

File Name	Audio File	Entropy	Average Length	Redundancy	Total Bits	Compressed Length	Compression Ratio	SNR
Text 1	inp1.wav	1.9501	2	2.5607	104	26	0.25	83.1163
Text 2	inp2.wav	2.1219	2.2	3.6793	80	22	0.275	83.1557
Text 3	new316.wav	2.6464	2.7	2.0239	80	27	0.3375	87.3399
Text 4	piano2.wav	3.6402	3.667	0.7264	120	55	0.4583	83.3484

Table 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
Text 1	inp1.wav	79.94	83.1163	3.1763
Text 2	inp2.wav	80.89	83.1557	2.2657
Text 3	new316.wav	85.67	87.3399	1.6699
Text 4	piano2.wav	79.73	83.3484	3.6184

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

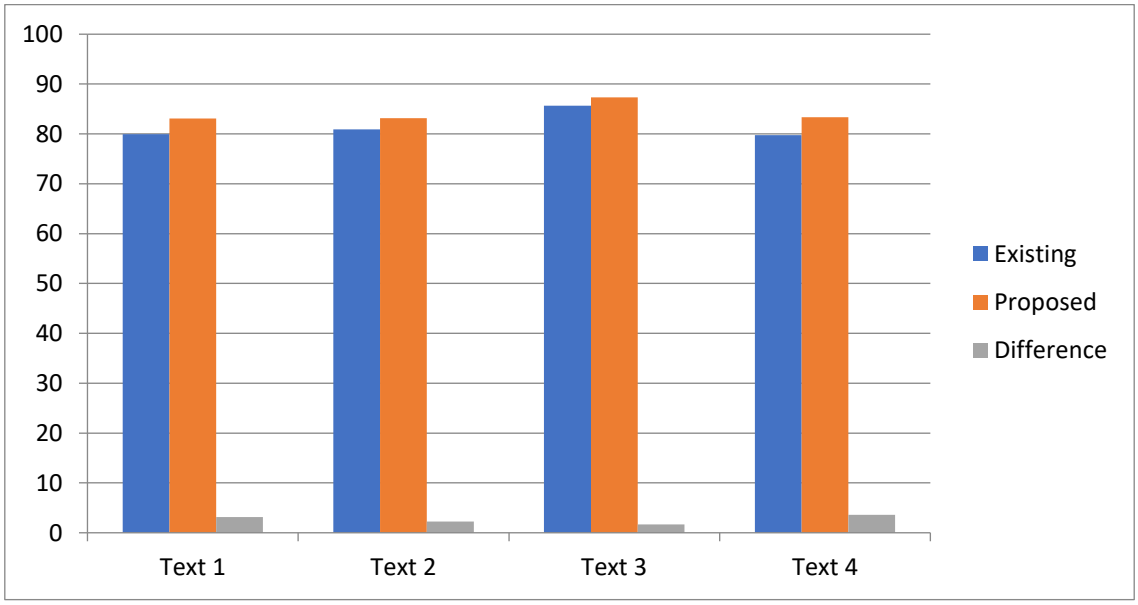

Fig. 1: Comparison of SNR

5. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

Steganography is an effective way to hide sensitive information. In the proposed work we have used the I-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. The resultant stegno audio is again compressed using the DCT along with Run Length Encoding. As the audio to be transmitted is again compressed, so the transmission process becomes fast and easy. 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. Result of comparison of SNR in existing and the proposed system, shows that proposed work is better than that of the existing system. Our results indicate that the E- LSB insertion using Adaptive Huffman Compression is better than simple LSB insertion in case of lossless compression. Result also shows the compression ratio using RLE and without using RLE. 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.

5.2 Future Scope

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 include location maps, paintings, architects. This type of data also

requires 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.

6. REFERENCES

[1] Fatiha Djebbar, Beghdad Ayady, 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.

[2] 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.

[3] 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.

[4] 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.

[5] Kamal Pradhan Chinmaya Bhoi, Robust Audio Steganography Technique using AES algorithm and MD5 hash. International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 10 (November 2014), © 2014, IJIRAE- All Rights Reserved.

[6] M.Baritha Beguma ,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.

[7] 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).

[8] 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,

[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] Hilal Almara'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] 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.

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

[14] 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.

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

[16] Ankit Chadha, Neha Satam, Rakshak Sood, 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.

[17] 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.

[18] 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.

[19] Hasna Parveen 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.

[20] 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.

