www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18682-18693

Various audio Steganography techniques for audio signals

Rubby Garg[1], Dr.Vijay Laxmi[2]
[1]A research scholar M-Tech, Computer Science and Engineering,Guru Kashi University,India
[2]Dean, UCCA, Guru Kashi University, India
[1]rubbygarg@yahoo.com, [2]vijay2003@yahoo.co.in

Abstract

The rapid development of multimedia and internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information. Besides that, digital documents are also easy to copy and distribute, therefore it will be faced by many threats. It is a big security and privacy issue, it become necessary to find appropriate rotation because of the significance, accuracy and sensitivity of the information. Steganography and Cryptography are considered as one of the techniques which are used to protect the important information, but both techniques have their pro's and con's. In this paper we have proposed a novel approach to hide the data in audio signals based on LSB technique. Performance of the proposed system is evaluated on various parameters and is compared with the existing systems.

Keywords : Audio Steganography, LSB, Data Hiding, E-LSB.

Introduction

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

Thus the main purpose of this seminar is to explain Audio Steganography and algorithms commonly employed for Audio Steganography and its applications.

DOI: 10.18535/ijecs/v5i10.58

People use cryptography to send secret messages to one another without a third party overseeing the message. Steganography is a type of cryptography in which the secret message is hidden in a digital picture. While cryptography is preoccupied with the protection of the contents of a message or information, Steganography concentrates on concealing the very existence of such messages from detection.

The term Steganography is adapted from the Greek word steganographia, 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.

With the invention of digital audio and images files this has taken on a whole new meaning; creating new methods for performing “reversible data hiding” as it is often dubbed. This has many possible applications including the copyright watermarking of audio, video and still image data. In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another. In order for a data hiding technique to be successful it must adhere to two rules:

- The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.

- The embedded data must maintain its integrity within the carrier and should be easily

removable, under the right circumstances, by the receiving party.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is

generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone

1 Private Key Steganography

Private key steganography is also called as secret key steganography [Brainos II 2003]. This secret key steganography is defined as a steganographic system that requires the exchange of a secret key prior to communication. Secret key steganography takes a cover message and embeds the secret message inside of it by using a secret key. This secret key is also called the stego key. Only the parties who know the secret key can reverse the process and read the secret message.

Unlike pure steganography where a perceived invisible communication channel is present, secret key steganography exchanges a stego key, which makes it more susceptible to interception [Anderson, Petitcolas 1998]. The benefit to secret key steganography is even if it is intercepted; only parties who know the secret key can extract the secret message. This private key steganography method uses a mutual key for encrypting then hiding the secret message within the cover data. As in traditional encryption, the private key system is only as robust as the knowledge of the key. Since the private key system requires both parties to know the key, once it is compromised the entire stego message is non-secure.

2 Public Key Steganography

Public key steganography can be defined as a steganography system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly [Brainos II 2003]. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message.

Public key steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in public key cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

This public key encrypted steganography uses the key pair system to add a layer of robustness to the process. As in public key encryption, the public key of the recipient is used to encrypt the secret message and only that user’s private key may decrypt it after extracting it from the cover data. This method is the most secure type of steganography

Literature Survey

Fatiha Djebbar[1], Steganography has been proposed as a new alternative technique to enforce data security. Lately, novel and versatile audio steganographic methods have been proposed. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. In this paper, we present a current state of art literature in digital audio steganographic techniques. We explore their potentials and limitations to ensure secure communication. A comparison and an evaluation for the reviewed techniques is also presented in this paper.

Kaliappan Gopalan[2],A method of embedding a covert audio message in a cover utterance for secure communication is presented. The covert message is represented in a compressed form with possibly encryption and/or encoding for added security. One bit in each of the samples of a given cover utterance is altered in accordance with the data bits and a key. The same key is used to retrieve the embedded bits at the receiver. The results, based on cover signals from a clean TIMIT utterance and a noisy aircraft cockpit utterance, show that the technique meets several major criteria for successful covert communication.

Gunjan Nehru[3],This paper is the study of various techniques of audio steganography using different algorithmic like genetic algorithm approach and LSB approach. We have tried some approaches that helps in audio steganography. As we know it is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. In steganography, the message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography, stego message after steganography remains same. for information hiding.

Jayaram[4], Today’s large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. In this paper we mainly discuss different types of audio steganographic methods, advantages and disadvantages.

Kamal Pradhan[5], Abstract—Data transmission in public communication system is prone to the interception and improper manipulation by eavesdropper. Audio Steganography is the procedure of hiding the existence of secret information by zipping it into another medium such as audio file. This paper explores the innovative audio Steganography technique in a practical way in order to conceal the preferred information. The proposed system uses LSB (least significant bit) technique for embedding text into an audio file. The text is encrypted using AES (Advanced encryption standard) encryption function and md5 hash function which is used for verifying data integrity of the audio file. The performance of this system is evaluated through a more secure process based on robustness, security and data hiding capacity

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 is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

Proposed system works in two phase, in which one phase is used to hide the data into an audio signal and another phase is used to recover the data from audio file.

Algorithm to hide the text message into an audio signal:

Phase 1 (Data Hiding Phase)

Step1: Input the text message.

Step 2: Compress the text message using Adaptive Huffman Coding.

Step 3: Input the .wav sound file in which data is to be hidden.

Step 4 : Extract the header from the .wav file.

Step 5: Store the number of bits to be hide into header of .wav file.

Step 6: using LSB technique overlap the message bits into .wav file in an alternating positions.

Step 7: Rejoin the .wav samples to create the output file.

Step 8: Store and display the file to user.

Phase 2 (Data Extraction Phase)

Step 1: input the .wav file in which data is hidden

Step 2: Extract the header and then total number of hidden bits.

Step 3 : Extract the bits from alternating LSB positions from the .wav samples.’

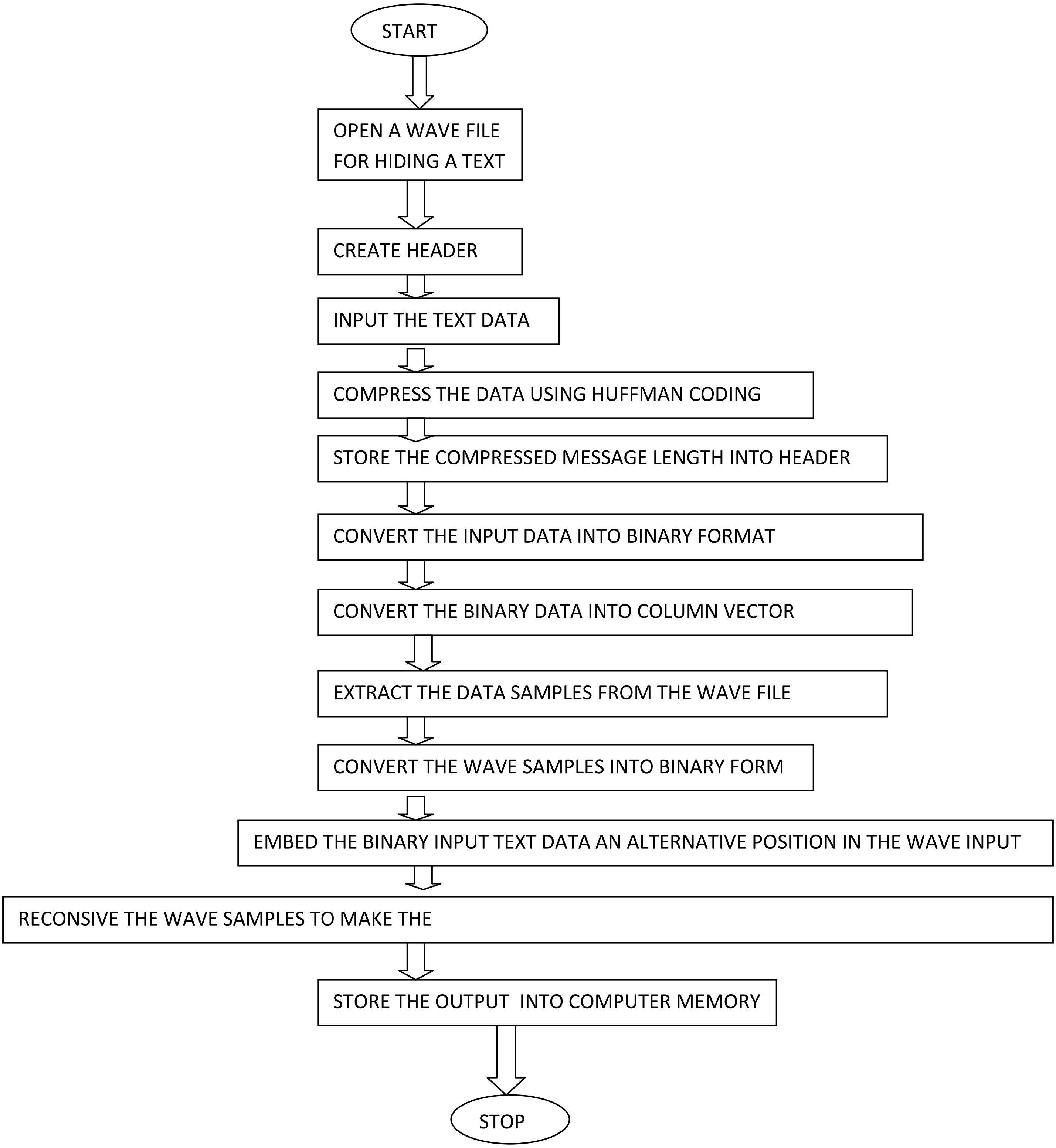
Step 4: Combine the message extracted from LSBs.

Step 5: Decompress the message using Inverse Adaptive Huffman coding.

Step 6: Display the extracted message to the user.

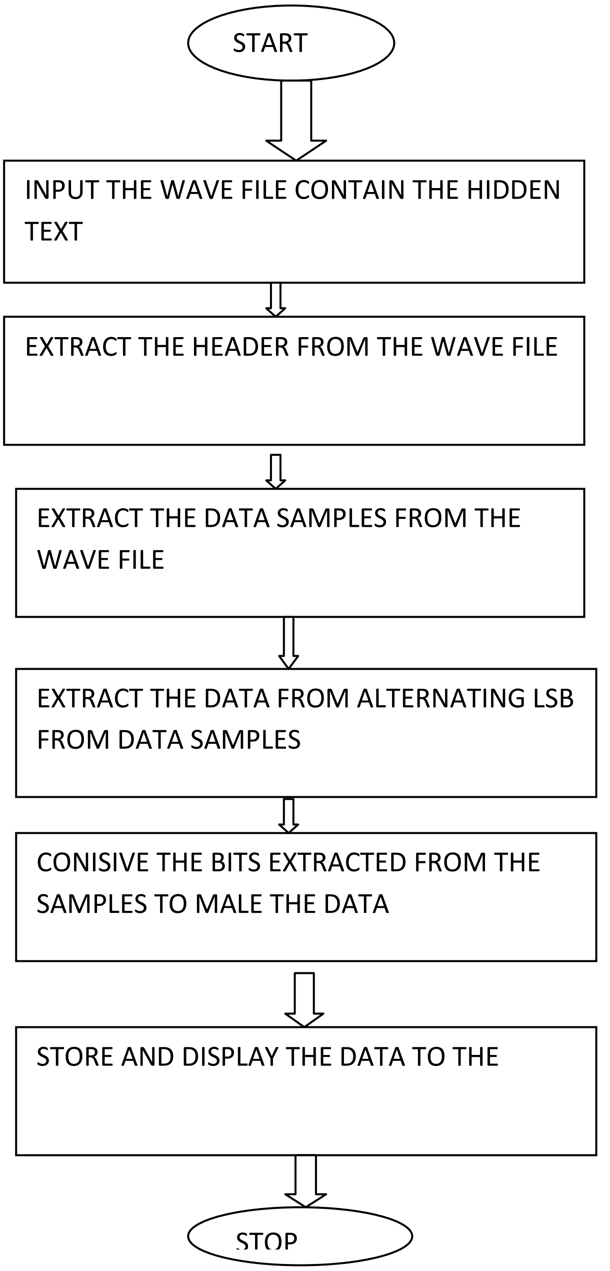
DOI: 10.18535/ijecs/v5i10.58

Flow chart for data hiding phase:


START
OPEN A WAVE FILE FOR HIDING A TEXT
CREATE HEADER
INPUT THE TEXT DATA
COMPRESS THE DATA USING HUFFMAN CODING
STORE THE COMPRESSED MESSAGE LENGTH INTO HEADER
CONVERT THE INPUT DATA INTO BINARY FORMAT
CONVERT THE BINARY DATA INTO COLUMN VECTOR
EXTRACT THE DATA SAMPLES FROM THE WAVE FILE
CONVERT THE WAVE SAMPLES INTO BINARY FORM
EMBED THE BINARY INPUT TEXT DATA AN ALTERNATIVE POSITION IN THE WAVE INPUT
RECONSIVE THE WAVE SAMPLES TO MAKE THE
STORE THE OUTPUT INTO COMPUTER MEMORY
STOP

DOI: 10.18535/ijecs/v5i10.58

Flowchart for Data Extraction


START
INPUT THE WAVE FILE CONTAIN THE HIDDEN TEXT
EXTRACT THE HEADER FROM THE WAVE FILE
EXTRACT THE DATA SAMPLES FROM THE WAVE FILE
EXTRACT THE DATA FROM ALTERNATING LSB FROM DATA SAMPLES
CONISIVE THE BITS EXTRACTED FROM THE SAMPLES TO MALE THE DATA
STORE AND DISPLAY THE DATA TO THE
STOP

DOI: 10.18535/ijecs/v5i10.58

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:

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

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

Table 5.1 Result statistics of the proposed system.

FILE NAME	ENTROPY	AVERAGE LENGTH	REDUN-DANCY	TOTAL BITS	CPMPRE-SSED LENGTH	COMPRE-SSION RATIO	SNR
My name is sukhdeep kaur sidhu	3.6444	3.6667	0.6106	240	110	0.4583	∞ db
Steganography	3.3927	3.4615	2.0276	104	45	0.4327	∞ db
Lily	1.5	1.5	0	32	6	0.1875	∞ db
Holly	1.9219	2	4.0622	40	10	0.2500	∞ db
Jasmine	2.8074	208571	1.7735	56	20	0.3571	∞ db
Daisy	2.3219	2.4	3.3624	40	12	0.3000	∞ db
Poppy	1.371	1.4	2.1189	40	7	0.1750	∞ db
Rose	2	2	0	32	8	0.2500	∞ db
Alyssum	2.5216	2.5714	1.9744	56	18	0.3214	∞ db
Iris	1.5	1.5	0	32	6	0.1875	∞ db
Violet	2.585	2.6667	3.1607	48	16	0.3333	∞ db
Lvy	1.585	1.6667	5.155	24	5	0.2083	∞ db
Paper	2.2571	2.3333	3.6287	48	14	0.29197	∞ db

Paper 1	2.5216	2.5714	1.9744	56	18	0.3214	∞ db
Paper 100	2.7255	2.7778	1.9188	72	25	0.3472	∞ db
Paper 1000	2.6464	2.7	2.0239	80	27	0.3375	∞ db
Paper 10000	2.5503	2.6364	3.373	88	29	0.3295	∞ db
Paper 100000	2.4508	2.5	2.0064	96	30	0.3125	∞ db
Paper 1000000	2.3535	2.3846	1.3206	104	31	0.2981	∞ db
Paper 10000000	2.2608	2.2857	1.1011	112	32	0.2857	∞ db

The above table represents the statistics of the proposed system. In the above

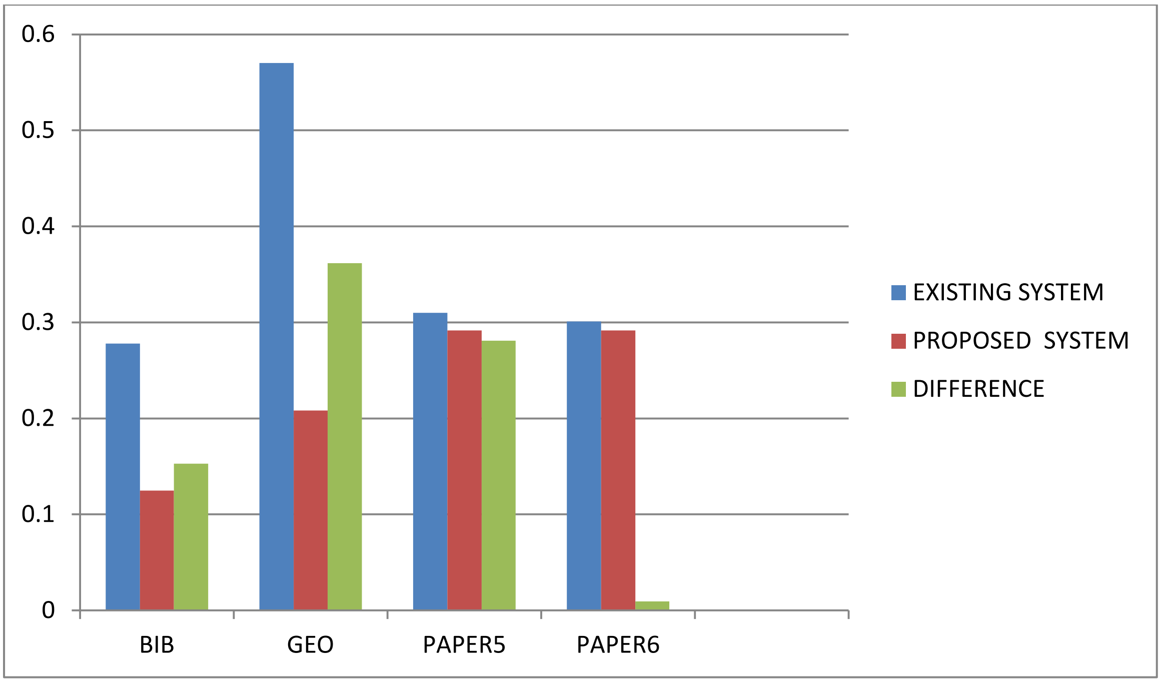
Table : Comparison of the proposed system with the existing system on the basis of the compression ratio

FILE NAME	COMPRESSION RATIO 1	COMPRESSION RATIO 2
BIB	0.278	0.1250
GEO	0.57	0.2083
OBJ1	0.232	0.2500
PAPER1	0.282	0.2917
PAPER2	0.282	0.2917
PAPER3	0.275	0.2917
PAPER4	0.2765	0.2917
PAPER5	0.31	0.2917
PAPER6	0.301	0.2917
PROGC	0.286	0.3000
PROGL	0.237	0.3000

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.

Comparison graph of the proposed system with the existing systems on the basis of compression ratio:

DOI: 10.18535/ijecs/v5i10.58



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. Table 4.2 and Table 4.3 shows that SNR higher than SNR of Existing techniques. Our results indicate that the E- LSB insertion using Adaptive 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 is use 24 bit data samples, therefore a negligible change will be in the audio signal that results in infinite SNR values.

Future Scope

Propsoed 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, 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.

DOI: 10.18535/ijecs/v5i10.58

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.