ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 6, June 2019

Data Hiding in Audio Signals with Steganography

[1] Linu Babu P, [2] Bency Varghese A, [3]Ashly George, [4]Anjali Rajan
[1][2][3][4] Assistant Professor
[1] linubabup@gmail.com, [2] bencyvarghesea@gmail.com, [3]ashly523@gmail.com, [4]anjuraj222@gmail.com

***Abstract*—In this paper, a robust substitution technique has used to implement proposed work of audio steganography. Steganography is an art of science methodology of writing hidden messages such a way that no one apart from the intended reciever knows the presence of the secret message data. This technique resolves the various inherent issues ,after that it increases the data hiding capacity while being also achieve robustness from various intentional as well as unintentional hacking attacks like this it provides privacy to data. The main strength of our algorithm is depend on the segment size and its used to achieve very high embedding capacity for different data type that can reach up to 50% from the input audio file size. Here developing two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio which for embeds additional data The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information.The proposed methods offers high quality of steganography process in terms of Peak Signal–to-Noise Ratio (PSNR). Only minor changes in the contents of the audio file occur, which is indiscernible to human ears. In addition, several attacks on the sound wave were performed; the results showed that the hidden secret data can be retrieved with minimal distortion. An implementation of both these methods and their performance analysis has been done in this paper.**

***Index Terms*—LSB, PSNR, Steganography, robustness**

1. INTRODUCTION

The usage of the internet terminologies are increases rapidly and the huge revolution in digitization of data are happened. For this overall scenario of modern communication is changed. Because of this revolution in software industry the hardware as well as the software are becomes more user-friendly it and flexible.and enables consumer to communicate multimedia data.and able to transmit large multimedia files through broadband connection of internet. Data hiding is a technique of providing data security.Using audio file as a cover medium instead of image is more tedious,as Human auditory System(HAS) is more sensitive than Human Visual system (HVS).audio files are available anywhere.thats why it becomes very easier to hide data by using audio and therefore requires to develop many techniques which provide security to data which are in audio files.By using steganography we can able to provide security to provide data.Steganography is an art of secret communication.Sender hides the secret information such that its presence can not be detected.sender hides the secret information in some carrier file and then transmitted on reciever side ,the carrier file can be image, audio file,text file,video file. At the reciever‟s end,the secret data can be recovered from the stego signal using different algorithmic technique. We can able to speak that given data is secured only when it follows the following requrements.The first requirement is perceptual transperancy, i.e:cover object(object not containing any additional data) and stego object(object containing secret message) must be perceptually indiscernible.The second constraint is high data rate of the embedded data. robustness:it measures the ability of the embedded data to withstand against intentional and unintentional attacks. Unintentional attacks:attacks generally include common data manipulation such as re-sampling ,re-quantization etc. Intentional attacks include addition of noise,resizing,rescalling etc. Data rate(capacity):It refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion. In other words the bits rate of message is the no of the embedded bits within a unit of time and is usually given in bits per second(bps).Here presenignt 2novel approaches of LSB coding that increase capacity of cover audio so as embed large data and section II:describes the proposed methods,which uses DCT methods .Steganography has wide range of applications such as covert communication,digital watermarking,access control,digital rights managements etc. Through this method,the audio steganographic problems are studied and creating a powerful secure solution for it,and therefore the security issue in modern communication is successfully resolved.

1.1 Fundamental Concepts:

In the data hiding the secret message can be need to transfer on receiver side by using audio file. For the data hiding purpose we used steganography technique which is nothing but a cover writing and also uses a cryptogrphy concept for encryption send decryption purpose.sender has a public key and receiver has a private key.and through lsb algorithm we are embedding the audio secret message bits into the audio file.and through substitution technique we are provide security to the secret message whch is transfer through the carrier over the network.but at the receiver side by using the decryption key it decodes the message and get the secret message from the audio but that time original file of audio remains same.

1.2 Contributions:

Audio steganography is a data hdding technique.Now a days there are many techniques are available to provide security for hiding data in audio by using Steganography .But there are many drawbacks are in that techniques,so there is need to provide solution on that all.

We are making the improvement in that techniques, which are hiding data in audio by using steganography. In our technique we are handling the many issues related to that techniques like in previous techniques after hiding data because of quantization and compression, the noise was created in the original audio file.And due to this the size of audio file was increases.

By using our latest substitution technique, without performing any compression and quantization we are hiding the data in audio file. For that various latest LSB and DCT steganographic algorithms we are using. And therefore the size of audio get not changed,and quality of original audio is maintained.Because of modern steganography techniques we are able to provide security to data from vulnerable attacks and able to hide data very securely in audio without any modification in original audio

2. LITERATURE SURVEY

2.1 Existing System:

The literature survey paper gives an overview about data hiding which is compressed in the audio signals.and the source for compression is a AAC format file. In the AAC MPEG4 data hiding scheme is performed based on the human auditory system.In this data hiding is performed mainly in the quantization process of MDCT phase method of the AACcoding.and hidden data capacity can be easily achieved without any modification into the original audio file. but the implementation is very complicated because of the quantization and compression process. This scheme alters the quantization and coding process by modifying the scale factors to produce more bits,in which redundant bits of audio file xan be replaced with the hidden data.The basic structure of the system includes all the relevant parts of the AAC MPEG-4 perceptual encoding.in this it performs various steps like domain conversion RS and SPA detection frequency and perceptual domain measurement.

This scheme enables optimal coordination between the quantization process of the encoder and the data hiding.The scheme vary the data hiding capacity by adjusting no of coefficients for the quantization.and thus,this scheme provides data hiding.When the embedded data bit rate needs to be changed, that time this scheme can change the quantization parameters also.hence it affects on the original quality of the original audio file signals. The coefficients which are carry the hidden data are picked as per the pseudo random mechanism which is unlikely to be intercepted by a third party.in this sender can able to embed only one bit at a time.hence,very poor performance it has and because of quantization orginal audio size also changes which creates the noise and create bad impact for data hiding.

2.2 Solution

2.2.1 Conflict:

When the data hiding performed into the AAC audio file, at that time need to compressed audio signals.and also all secret data hiding purpose low bit rating was performed.which is very time consuming and complicated task because of compression the noise is generated into the audio file.for the embedding low bit rating technique is used.therefore the size of audio file is increases. .hence, the receiver can not get the original audio. hence,project seeks to grow.and its community needs to manage all this major conflict. And need to generate the solusion for that.

2.2.2 Substitution:

XU shexhung finds a method for data hiding in AAC audio file,in that it performed quantization and the compression of audio.because of that the size of audio file was increases and receiver can’t get the original contents .Hence, the dr A.R Kekre and Uttara athwale studies this problem and they develop the LSB algorithm technique for the bit embedding purpose because of that doesn’t need to compressed audio file.hence, the size of algorithm is does not varies as per the secret msg.

But this is not the fine solution ,need to do more improvement into the sender can send the message over the network securely for that purpose we are adding steganographic technic and also performs some security purpose substitution steps at a time of bit embedding. Because of that substitution algorithm sender can able to send message through carrier over the network very securely.and when the receiver get the message it can able to get original audio and secret message as it is.because of substitution algorithm hacker can not able to perform any modification into the audio file.

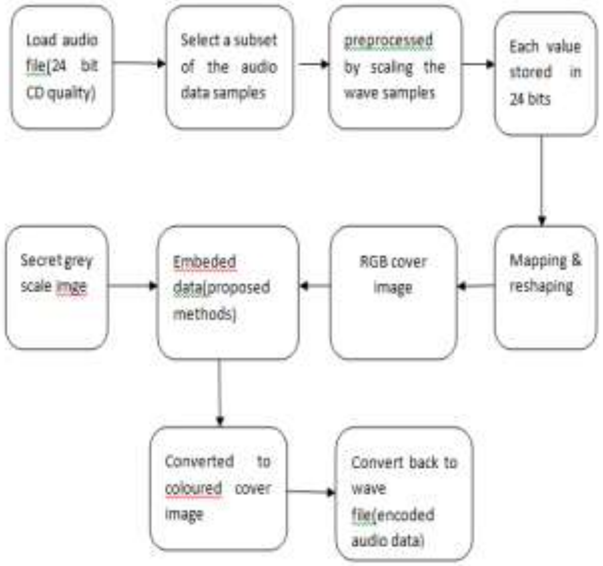
3. PROPOSED SYSTEM

The human auditory system is sensitive to small amplitude variations in audio files, we developed a hiding technique where it is possible to hide secret data in an audio file and ends up with a sound that is indistinguishable from the original.
Sound samples are stored as 8, 16 or 24 bit values. In order to hide secret data, we used 24 bit CD quality wave audio file at 48 kHz as a cover file to hide a secret gray scale image. Our technique can be applied on samples of 8 or 16 values by scaling the sample values into 24 bit.
In the proposed technique, the sound is divided into samples where each sample is 24 bit, 8 bits are to be hidden in each sample by distributing the bit pattern that corresponds to the secret gray scale image across the LSBs of the preprocessed sound samples (i.e. the preprocessed sound waves take the shape of a RGB colored image). So the embedding capacity is 8 bits per audio sample which results in large embedding capacity. Additionally, hiding the secret bit pattern by distributing it in the layers of the colored image, add more secrecy to the hidden data.
Spatial domain technique Spatial steganography mainly includes LSB(Least Significant Bit) steganography Least significant bit (LSB) insertion is a common,simple approach to embedding information in a cover image . The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Stage 1: Scaling the wave samples and mapping it into a colored cover image

1. Read the audio data samples in the cover audio file.
2. The values of the audio data samples will be in the range [+8,388,607, -8,388,608]
3. To make the technique more secure and to decrease the possibility of distortion in the retrieved secret data select a subset of the data samples that are enough to embed the secret data either by taking a set of sequential samples of numbers equivalent to the number of pixels in the secret data, or taking the odd or even samples of numbers equivalent to the number of pixels in the secret data.
4.Scale the selected sample values to values from 0 to 16777215 (224-1)

Due to the scaling process, the scaled values are similar to the image values (each value is stored in 24 bits)
5. Map and reshape these values to produce a colored cover image (the colored image is consisted of three layers Red, Green and Blue). This image will be used to hide the secret data.
The mapping process can be achieved by using the following two ways:
-Color mapping: Map each scaled value to a specific color (Red, Green or Blue) using a color table.
-Split each scaled value (24 bits) into three groups of 8 bits (i.e. the RGB color components)


Load audio file(24 bit CD quality)
Select a subset of the audio data samples
preprocessed by scaling the wave samples
Each value stored in 24 bits
Mapping & reshaping
RGB cover image
Embeded data(proposed methods)
Secret grey scale imge
Converted to coloured cover image
Convert back to wave file(encoded audio data)

General block diagram of proposed method

Stage 2: Embedding the secret gray image in the colored cover image:

a) LSB technique

Using the LSB technique, embed each pixel (8 bits) of the secret gray image in the corresponding pixel of the colored cover image (24 bits) by doing the following:
a) Divide the pixel in the secret gray image into 2 groups of 3 bits and 1 group of 2 bits.
b)Embed the resulted groups of bits in the corresponding pixel in the colored cover image (embed the first group of 3 bits in the Red layer, the second group of 3 bits in the Green layer and the last group of 2 bits in the Blue layer)
Repeat the steps a) and b) until you embed all the pixels of the secret image in the colored cover image.

b) LSB extracting technique

The data extraction at the receiver's side follows the same logic as the embedding technique. The first step is to read the wave data samples in the cover audio file then scale the sample values to values from 0 to 16777215 (224 -1) as discussed before. After that, map and reshape these values to produce a colored cover image, finally, retrieve the secret image by:

a) Each pixel in the secret image will be constructed by retrieving the first three bits from the Red Layer to be the least three bits in the secret image pixel, the first three bits from the Green Layer to be the fourth, fifth and sixth bits in the secre image pixel and the first two bits from the Blue Layer to be the seventh and eighth bits in the secret image pixel.

b)Retrieve the image size from the cover image to reconstruct the secret image.

c) DCT based steganography

The audio data samples are converted to gray image is same as that of LSB techniqueData embedded in the cover image will be different from lsb.

DCT coefficients are used for compression technique. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

In dct domain technique first Read audio data select a portion of wave samples and convert it into corresponding RGB cover image by proper scaling mapping & reshaping.Read secret message then convert it in binary. The cover image is broken into 8×8 block of pixels. Working from left to right, top to bottom subtract 128 in each block of pixels. DCT is applied to each block. Each block is compressed through quantization table. Then Calculate LSB of each DC coefficient and replace with each bit of secret message. hence obtained the stego image.The image of size M×N is divided into 8×8 blocks and two dimensional (2-D) DCT is performed on each block. The DCT is calculated using equation 1:

$$F(u,v)=\frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \qquad (1)$$

for x=0,..., 7 and y=0,..,7

$$\text{where } C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases}$$

Here, C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT and high frequency coefficients are lower right positions.Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion

d) DCT extracting technique

The extracting method for dct is the reversal of the hiding method. first read the stego wave file,then by preprocessed scaling convert the audio file into stego cover image of RGB color. This Stego image is broken into 8×8 block of pixels. Working from left to right, top to bottom subtract 128 in each block of pixels. DCT is applied to each block. Each block is compressed through quantization table.Calculate LSB of each DC coefficient. : Retrieve and convert each 8 bit into character

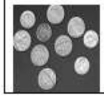
Stage 3: Converting the colored cover image back into sound wave

Convert the colored cover image back to a wave file by rescaling the values to be in the range [+8,388,607, -8,388,608] and sending the cover wave to the receiver side.

4. EXPERIMENTAL SETUP AND DISCUSSION

The proposed perceptual video encryption is implemented with MATLAB 7.10.0 operating system. The experiments are carried out on 3 images hiding in an audio signal. Performance evaluation factors like PSNR and MSE values for encoded audio for proposed methods with and without AWGN and comparison method, is tabularized in table4.1

Table 4.1: simulation results for LSB & DCT Method

	LSB METHOD			DCT METHOD			SIZE OF THE COVER IMAGE
	PSNR(without AWGN)	PSNR(with AWGN)	MSE	PSNR(without AWGN)	PSNR with AWGN)	MSE	
	48.045	47.183	0.498	41.213	39.213	4.64	256*256
	50.36	49.632	0.4235	40.463	38.745	6.162	256*256
	51.635	50.523	0.3807	38.325	36.126	7.453	256*256

The comparison table depicting the differences between both the methods is given below in Table 4.2. Here invisibility, robustness against attacks, payload capacity,PSNR,MSE are compared.

5. CONCLUSION

This paper Customization of audio steganography will help sender to send a secret information using an audio file to send to receiver effectively and efficiently. This software will troubleshoot the errors for secure data transmission which is used for writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. The algorithm will hide the message as per the proposed solution . Older methods for data hiding are discussed.This paper implements LSB based steganography, DCT based steganography and computes PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are better of quality. Comparison of LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of LSB based steganography scheme is high as compared to DCT based steganography scheme for all types of images-(Grayscale as well as Color). DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme. Even though the amount of secret data that can be hidden using DCT technique is very small as compared to LSB based steganography scheme still, DCT based steganography scheme is recommended because of the minimum distortion of image quality. As future work, data hiding in audio signal may be extended to other steganographic technique like wavelet transformation for more secure data transmission and the noise attack may be extended to some of salt & pepper noise instead of AWGN. It is used for secure data transmission. This is a serious and vital issue in some applications such as battlefield communications and banking transactions .

REFERENCES

1. Dalal N. Hmood, Khamael A. Khudhiar and Mohammad S. Altaei (2012). A New Steganographic Method for Embedded Image In Audio File. International Journal of Computer Science and Security(IJCSS) 6(2): pp.135-141.

2. Samir K. Bandyopadhyay and Biswajita Datta (2011). Higher LSB Layer Based Audio Steganography Technique. International Journal of Electronics and Communication Technology (IJECT) 2(4): pp.129-135.

3. Kirti Saroha , Pradeep Kumar Singh (2012). A Variant of LSB Steganography for Hiding Images in Audio. International Journal of Computer Applications(0975-8887) 11(6): pp.12-16.

4. Debnath Bhattacharyya, Poulami Dutta and Tai-hoon Kim (2009). Secure Data Transfer through Audio Signal. Journal of Security Engineering 6(3): pp.187-194.

5. Masoud Nosrati, Ronak Karimi and Mehdi Hariri (2012). Audio Steganography: A Survey on Recent Approaches. World Applied Programming 2(3): pp.202-205.

6. Ajay.B.Gadichal (2011). Audio Wave Steganography. International Journal of Soft Computing and Engineering (IJSCE) 1(5): pp.174-176.

7. Yincheng Qi, Jianwen Fu, and Jinsha Yuan, “Wavelet domain audio steganalysis based on statistical moments of histogram”, Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.

8. Yin-cheng qi, liang ye, chong liu “Wavelet domain audio steganalysis for multiplicative embedding model” Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009.

9. V. Vapnik, “Statistical Learning Theory”, John Wiley, 2008.

10. Mengyu Qiao, Andrew H. Sung , Qingzhong Liu “Feature Mining and Intelligent Computing for MP3 Steganalysis” International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009