International Journal of Pure and Applied Mathematics
Volume 116 No. 21 2017, 619-628
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

Secured Data Hiding in Audio Files Using Audio Steganography Algorithm

[1]M. Parthasarathi and [2]T. Shreekala

[1]Department of Computer Applications,
School of Computing Sciences,
Vels University, Chennai, Tamil Nadu, India.
triplicanegod@gmail.com

[2]Department of Computer Applications,
School of Computing Sciences,
Vels University, Chennai, Tamil Nadu, India
sreekalatm@gmail.com

Abstract

The easiest way to keep something from prying eyes is to place it right in front of the person looking for it and make it look as innocuous as possible. Everyone has a taste for a certain kind of music. Hence, it is more than likely that the person will have that kind of music on the storage device of his computer. Also, it is quite common case where people share and transfer different music files to one another. If one were able to hide the message can be. Also, transfer of this message can be done quite conveniently without raising any eyebrows. This paper comes up with a technique of hiding the message in the audio file in such a way, that there would be no perceivable changes in audio file after the message insertion. At the same time, if the message that is to be hidden were encrypted, the level of security would be raised to quite a satisfactory level. Now, even if the hidden message were to be discovered the person trying to get the message would only be able to lay his hands on the encrypted message with no way of being able to decrypt it.

1. Introduction

Steganography is the technique of encrypting a file, message, image or video to another file, message, image, or video. The word steganography derived from the Greek word steganos, means for "covered, concealed, or protected", and graphene means for "writing" [2]. Steganography is the method of covering and hiding messages in a medium called a cipher text. Steganography is related with cryptography but it differ from watermarking[6]. The basic idea behind cryptography is, a secret message can be kept by encoding it so that no one can view it. If a good cipher is used, it is likely that no one, not even a government entity, will be able to read it. Here is where steganography comes in. The purpose of steganography is to embed the data or a message. All steganography requires is a cipher text, where the data has to be hidden, a message that is made up of data, an algorithm that decides steps to hide the data, and a key that will be used to encrypt that file. First the data that is being passed from one person to another is encrypted. And the information is embedded into a cipher text. This is done according to the embedding algorithm and a secret key that performs the actions of the embedding process. This process outputs a steganogram which has the information hidden inside.

Audio Steganography

Hiding the messages into digital sound is called as audio Steganography. Data hiding in audio signals is especially challenging, because Auditory system (HAS) is more extensive than human visual system (HVS), [3,5]. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than thousand to one. Sensitivity to additive random noise is also acute. The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However there are some ‘holes’ available. While they has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out the quieter sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally there are some environmental distortions so common as to be ignored by the listener in most cases [1].

2. Literature Survey

Data hiding and watermarking in digital images and raw video have wide literature. Data hiding in motion vectors at the encoder replaces the regular pair, due to tampering the motion vectors, to become, where the superscript denotes hiding. The message should survive the video lossy compression and can be identically extracted. This robustness constrain should have low distortion effect on the reconstructed video as well as low effect on the data size (bit rate). A novel video watermark technique in motion vectors, the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. In Data hiding for digital video with phase of motion vector and A novel steganographic algorithm based on the motion vector phase embed the data in video using the phase angle between two consecutive CMV. These CMV are selected based on the magnitude of the motion vectors as in Video watermark technique in motion vector. The message bitstream is encoded as phase angle difference in sectors between CMV. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold. For hiding the data secretly in an audio file, there are few techniques introduced earlier. These are:

- Low-bit Encoding
- Phase Coding
- Spread Spectrum

Low-bit Encoding

Low-bit encoding is the one of the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, large amount of data can be encoded in an audio signal [4]. Ideally, the channel capacity is 1 kb per second (kbps) per 1 kilohertz(kHz), e.g., in a noiseless channel, the bit rate will be 8 kbps in an 8 kHz sampled sequence and 44 kbps in a 44kHz sampled sequence. In return for this large channel capacity, audible noise is introduced. The impact of this noise is a direct function of the content of the host signal, e.g., crowd noise during a live sports event would mask low-bit encoding noise that would be audible in a string quartet performance.

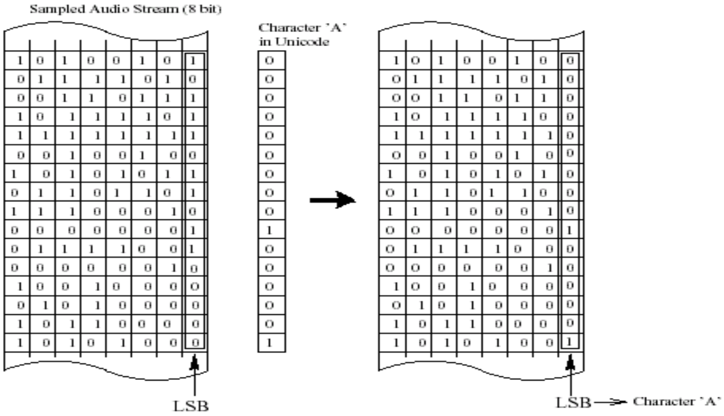
Adaptive data attenuation has been used to compensate this variation. In this algorithm, Least significant bit of every pixel of frames is used to hide the secret information bit[9],[10],[11]. The major advantage of this method is its poor immunity to manipulation. Encoded information can be destroyed by channel noise, re-sampling, etc., unless it is encoded using redundancy techniques. In order to be robust, these techniques reduce the data rate which could result in the requirement of a host of higher magnitude, often by one to two orders of magnitude. In practice, this method is useful only in closed, digital-to-digital environments.

Phase Coding

The source sound signal (C) is segmented to get the header. The remaining part is to be broken up into smaller segments which have lengths equal to the size of the message to be encoded. A (DFT) Discrete Fourier Transform is used for each segment to create a matrix of the phases. The embedded message is inserted in the phase vector of the initial signal segment as follows:

$$phase\_new = \begin{cases} \pi/2 & if \quad message \quad bit = 0 \\ -\pi/2 & if \quad message \quad bit = 1 \end{cases}$$

Cons with this phase coding are a low data transmission rate because of which the secret message is encoded in the first signal segment only and to get the secret message from the sound file, the receiver must know the segment length.



Spread Spectrum

The formal (SS) spread spectrum is a technique to spread secret message across the frequency spectrum of the audio signal. The (SS) Spread Spectrum technique expands the secret message over the frequency spectrum of the audio file. As the outcome, the final signal takes a bandwidth which is more than what is actually required for transmission. Anyhow, the (SS) Spread Spectrum technique has one main con that it can introduce noise into a audio file. In (SS) spread spectrum technique secret message is expand over the audio signal's frequency spectrum as much as possible. However, the Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file [7, 8]. Without this, a variety of signal locking algorithms may be used, but these are computationally expensive.

Disadvantages

1. The Data size increase when extracting and embedding process takes place.
2. Robustness constrain should have low distortion effect on the reconstructed video as well as low effect on the data size (bit rate).
3. If extracting process takes place there may be lose of hidden data.

3. Proposed System

In this paper, a different approach directed towards achieving a minimum distortion to the prediction error and the data size overhead. This approach is based on the associated prediction error and the difficulty of dealing with the nonlinear quantization process. Lossy video compression is overviewed to define our notation and evaluation metrics. At the encoder, the intrapredicted (I)-frame is encoded using regular image compression techniques similar to JPEG but with different quantization table and step; hence the decoder can reconstruct it independently. The video is ordered into groups of pictures (GOPs) whose frames can be encoded in the sequence. The temporal redundancy between frames is exploited using block-based motion estimation that is applied on macroblocks of size in or and searched in target frames.

Advantages

1. A single bit is hidden in the least significant bit of the larger component of each candidate motion vectors (CMV).
2. The video encoding/ decoding which makes it hard to be detected by image steganalysis methods and is lossless coded.
3. This method is found to have lower distortion to the quality of the video and lower data size increase.

A. Algorithm for Embedding Text File Content Into Audio File At The Sender Side. [12]

```
Step1: Select the audio file for embedding the secret message.
Step2: Play the audio file so that it sounds clear to the end user.
Step3: Select the text file containing the secret message.
Step4: Encrypt the text file contents.
Step5: Compare text file and audio file size.
        If text file size > audio file contents
    Error message displayed indicating cannot embed secret message.
     Else
Embed secret message in the audio file in the 4th and 5th LSB bit of every sample.
Step6: Display message to user of the new audio file created after embedding secret message.
```

B. Algorithm for Extracting The Embedded Text From Audio File at the Receiver Side. [13]

```
Step 1: Select the new audio file for extracting the secret message.
Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.
Step3: If secret message present in audio file
     Then
     Display message to end user after extracting message.
         Else
     Display that no hidden data is present in the text.
Step4: Decrypt the secret message.
Step5: Display message to end user after decrypting the message.
```

C. Compare PSNR and SNR of the original and embedded audio files and display their values respectively

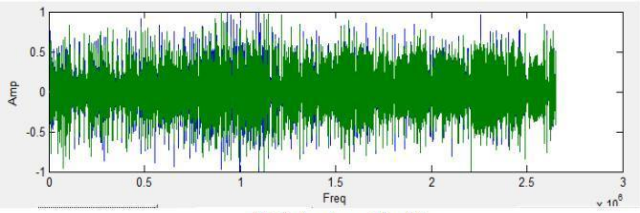
4. Results

Different experiments were conducted to prove that the proposed method of embedding audio file. [14] The following experiments were conducted by modifying the 4th and 5th bit LSB with same data and different data.

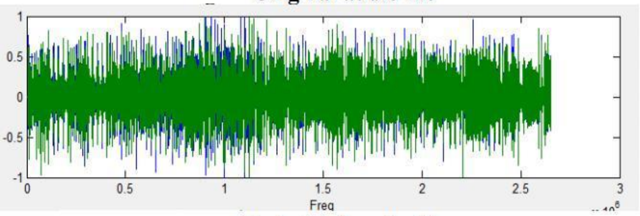
1. Same audio file is embedded with different text file with varying text content sizes.
2. Different audio files of different time durations are taken and embedded with same text content.

3. Different categories of audio file are considered and embedded with same text content.

In all the cases, SNR (Signal to Noise Ratio) and PSNR (Peak; Signal to Noise Ratio) area calculated. The first figure shows the original audio file before embedding the text content and the Figure 2 shows the audio file after embedding the text content. The results show that the size of the audio file remains same even after embedding the secret message.



Original audio file



Embedded audio file

The results of the experiment conducted by changing the 4th and 5th LSB bit with same data have been tabulated in Table I, Table II and Table III.

Table I: SNR/PSNR Values for Same Audio File With Varying Text Content Sizes

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
Text1	103	-2.22E-0 8	16.66214531
Text2	100	-2.19E-0 8	16.66214531
Text3	75	-2.17E-0 8	16.66214531
Text4	50	-2.17E-0 8	16.66214531
Text5	25	-2.24E-0 8	16.66214531

Table II: SNR/PSNR Values for Different Audio Files of Different Time Durations with Same Text Content

	Text File size :103 Bytes		
File Name	Duration (sec)	SNR	PSNR
Sample_15	15	-0.000000125	17.50264063
Sample_30	30	-4.83E-08	17.16767049
Sample_60	60	-2.19E-08	16.66214531
Sample_80	80	-1.65E-08	16.6129556
Sample_90	90	-1.47E-08	16.61077829
Sample_100	100	-0.000000013	16.63435136

Table III: SNR/PSNR Values for Different Categories of Audio File with Same Text Content

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
HARDCORE	103	0.00000258	11.2635686
HIPHOP	103	0.00000202	11.2635686
JAZZ	103	-9.66E-09	17.719165
METAL	103	-2.52E-08	10.6906624
POP	103	-3.38E-08	10.4659678
ROCK	103	-6.97E-08	13.5509855

The results of the experiment conducted by changing the 4th and 5th LSB bit with different data have been tabulated in Table IV, Table V and Table VI.

Table IV: SNR/PSNR Values for Same Audio File with Varying Text Content Sizes

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
Text1	103	-6.84E-09	16.66214532
Text2	100	-6.8E-09	16.66214532
Text3	75	-6.88E-09	16.66214532
Text4	50	-6.85E-09	16.66214532
Text5	25	-6.84E-09	16.66214532

Table V: SNR/PSNR Values for Different Audio Files of Different Time Durations with Same Text Content

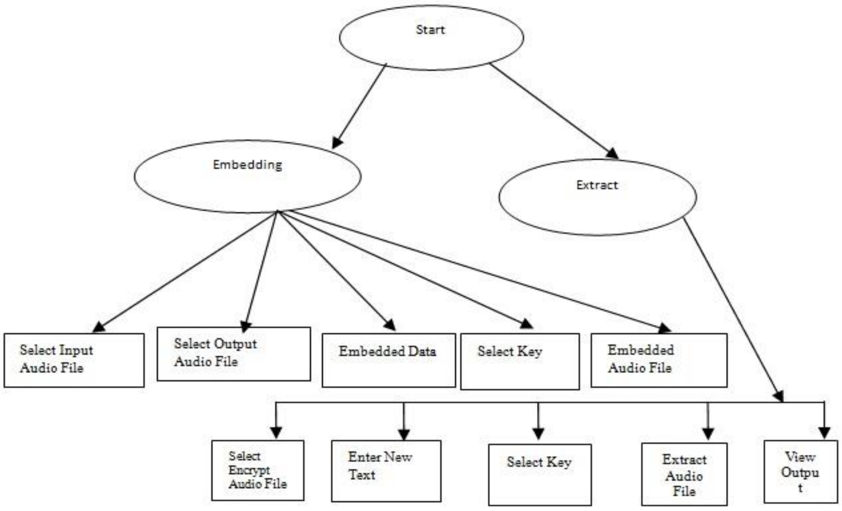
	Text File size :103 Bytes		
File Name	Duration (sec)	SNR	PSNR
Sample_15	15	-3.77E-08	17.50264072
Sample_30	30	-1.51E-08	17.16767052
Sample_60	60	-6.78E-09	16.66214532
Sample_80	80	-5.12E-09	16.61295561
Sample_90	90	-4.47E-09	16.6107783
Sample_100	100	-4.03E-09	16.6

Table VI: SNR/PSNR Values for Different Categories of Audio File with Same Text Content

	Audio File Duration : 60sec		
File Name	Size (Bytes)	SNR	PSNR
HARDCORE	103	0.00000152	11.26356751
HIPHOP	103	0.00000129	10.98350927
JAZZ	103	4.06E-09	17.71916498
METAL	103	-7.81E-0 9	10.69066241
POP	103	-1.01E-0 8	10.46596782
ROCK	103	2.15E-0 8	13.55098551

With these results, we can see that the SNR and PSNR values reduce as the file size increases, indicating that weak noise is not harmful to the changed bits at higher layers.

5. Data Flow Diagram



6. Conclusion

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Audio file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly.

Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic steganographic algorithms that do not use keys. By using this algorithm, two parties can be communicated with a fairly high level of confidence about the communication not being detected.

In designing the “Steganography” utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts. Also the principles maintained good quality in the developed system as per the user requirements.

References

[1] Bender W., Butera W., Gruhl D., Hwang R., Paiz F.J., Pogreb S., Techniques for data hiding, IBM Systems Journal 39(3-4) (2000), 547–568.

[2] Jayaram P., Ranganatha H.R., Anupama H.S., Information Hiding Using Audio Steganography–A Survey, The International Journal of Multimedia & Its Applications 3(3) (2011).

[3] Pal D., Ghashol N., A robust audio steganography scheme in time domain, International Journal of computer Applications 80(15) (2013).

[4] Cvejic N., Seppanen T., Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding, Journal of Universal Computer Science 11 (2005).

[5] Gopalan K., Audio Steganography Using BIT Modification, International Conference Multimedia and Expo (2003).

[6] Jain M.P., Trivedi P.V., Effective Audio Steganography by using Coefficient Comparison in DCT Domain, International Journal of Engineering Research & Technology 2(8) (2013).

[7] Santosa R.A., Bao P., Audio-to-Image Wavelet Transform based Audio Steganography, 47th International Symposium ELMAR-(2005), 209-212.

[8] Qi Y.C., Ye L., Liu C., Wavelet domain audio steganalysis for multiplicative embedding model, International Conference on Wavelet Analysis and Pattern Recognition (2009), 429-432.

[9] Lu C.S., Multimedia security: steganography and digital watermarking techniques for protection of intellectual property, Artech House, Inc (2003).

[10] Chae J.J., Manjunath B.S., Data hiding in Video, Proc. of the 6th IEEE International Conference on Image Processing (1999).

[11] Provos N., Honeyman P., Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy Magazine 1 (2003).

[12] Zamani M., Manaf A.A., Ahmad R.B., Zeki A.M., Abdullah S., A genetic-algorithm-based approach for audio steganography, World Academy of Science, Engineering and Technology 54 (2009).

[13] Geetha K., Vanitha Muthu P., Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy, International Journal on Computer Science and Engineering, 02(04) (2010), 1308-1313.

[14] Ajay B. Gadicha, Audio Wave Steganography, International Journal of Soft Computing and Engineering 1(5) (2011).