An Efficient technique for data hiding in audio signals

Randa A. Al-Dallah,[a] Aseel M. Al-Anani,[b]
Rola I. Al-Khalid,[c] Samah A. Massadeh[d]
[a] Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan
randa.dallah@fet.edu.jo
[b] Department of Computer Information Systems, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
a.anani@ju.edu.jo
[c] Department of Computer Information Systems, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
r.khaild@ju.edu.jo
[d] Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan
samah.massadeh@fet.edu.jo

Abstract. Data hiding, a form of steganography, is one of the emerging techniques that embeds secret data into a digital media and thus ensures secured data transfer. In this paper, the steganographic method used, is based on audio steganography which is concerned with embedding secret data in an audio file. The basic idea of our proposed method is that the host signal (the sound wave cover media) undergoes preprocessing, and then the results takes the shape of an image in which the data can be securely hidden in the image layers. The secret data is then hidden in a preprocessed sound wave using a traditional steganographic technique. The proposed method 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 are 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.

Keywords: data hiding, audio steganography, scaling, sample, PSNR, attacks.

1 INTRODUCTION

Audio steganography is one of the popular data hiding techniques that embeds secret data in audio signals. The secret data is hidden in a way that unauthorized persons are not aware of the existence of the embedded data and without altering the quality of the cover audio. Data hiding in audio signals has numerous applications such as protection of copyrighted audio signals, covert communication, hiding data that may influence the security and safety of governments and personnel [1,2].

An effective audio steganography should have the following characteristics for successful embedding and extracting data: perceptual transparency (i.e. the cover and the stego objects must be imperceptible), high data rate and robustness of the embedded data [3,4].

Least Significant Bit (LSB) coding is one of the simplest techniques used by many researchers to hide data in digital audio file [5,6]. LSB allows large amount of data to be embedded by substituting the least significant bits with the embedded secret message bits. On the other hand, using LSB, increases the noise in the audio file which can be detected by the sensitive human ears.

Recent researches have been presented which concentrate on hiding secret data in audio. Kriti and Pradeep[7] proposed a scheme where a secret gray scale image file is to be embedded in an audio cover file. In their scheme, a comparison is made between

secret image bits and the audio samples (1st MSB -Most Significant Bit- to the 7th MSB positions). If a match is found the three LSB of the audio sample is replaced with the binary equivalent of the MSB position. As a result, the image is hidden without affecting the size of the cover audio file. The SNR is calculated, which shows less noise in the audio file compared with other novel techniques. Debnath, Poulami and Tai-hoon [8] used a method called the zigzag LSB method where the binary value of the of the secret message is inserted into the last bit of the audio in a zigzag fashion. On the average, only half of the bits are altered in the audio file. So there are no noticeable sound variations of the audio file before and after hiding the data. Ajay [9,10] also presented a new 4th bit rate LSB audio steganography method where the message is embedded in 4th LSB layer . This gives an increased robustness against noise addition. Nedeljko and Seppanen [3] developed a reduced distortion bit-modified algorithm for LSB audio stegonagrapgy where the algorithm increases the depth of the embedding layer form 4th t o 6th LSB layer.

In this paper, we proposed a data hiding method where the host signal (the sound wave cover media) undergoes preprocessing and mapping, then the results takes the shape of a colored image in which the data can be securely hidden in the image layers. The secret data is then embedded in the colored image using the LSB coding steganographic technique. The colored image, in which the secret data embedded, will be converted back to sound wave before transmission.

This paper is organized as follows: Section 2 the proposed methods, Section 3 experimental results, section 4 conclusions.

2 THE PROPOSED METHOD

2.1 The Proposed Hiding Technique

Since 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.

Our technique consists of three stages (see Fig. 1). In the first stage the cover audio file is preprocessed by scaling the wave samples and mapping it into a colored cover image, in the second stage, the secret gray image is embedded in the colored cover image and finally, the colored cover image is converted back into sound wave. The three stages are explained as follows:

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 (2^{24}-1) using eqs (1) and (2) :

   New_samples = sample_values + abs(min(sample_values)). (1)

Scaled_Samples = round(New_samples .*((2^{24}-1) / max(New_samples))). (2)

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)

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

1. Input the secret gray image that is to be embedded and convert it into binary form.
2. Determine the size of the image to embed it in the cover image.
3. 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.

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.

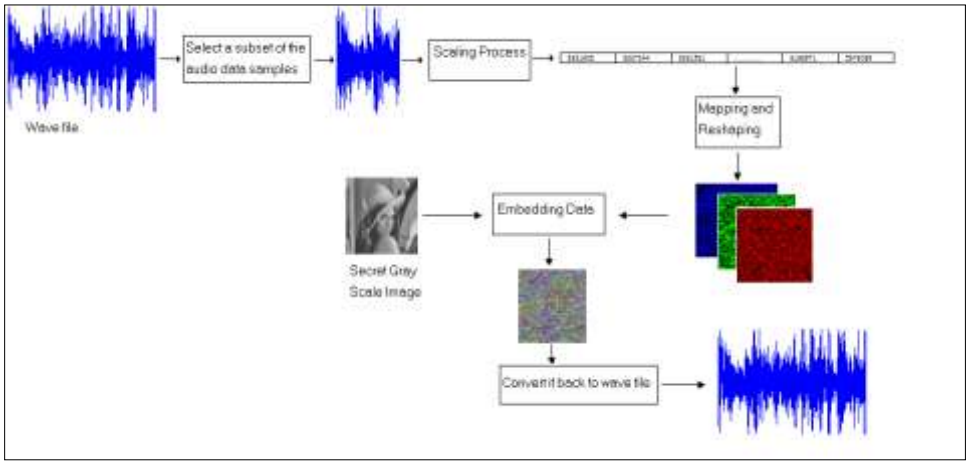


Fig. 1. The Hiding Technique

2.2 The Proposed 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 (2^{24} -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 secret

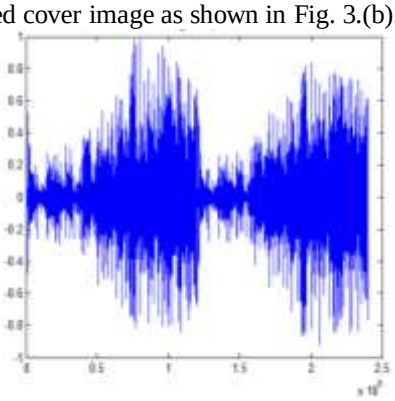
image pixel and the first two bits from the Blue Layer to be the seventh and eighth bits in the secret image pixel.

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

3 EXPERIMENTAL RESULT

Several experiments have been conducted using different audio wave signals. We used a 24 bit wave audio as the host cover media. In the hiding phase, the cover wave audio file and the secret gray image represent the inputs of our technique as shown in Fig. 2.

Fig. 3.(a) shows the selected wave samples that are enough to embed the secret gray image. To convert the wave samples into a colored image, a scaling process is applied to the selected samples. The scaled samples are then mapped and reshaped to obtain the colored cover image as shown in Fig. 3.(b).

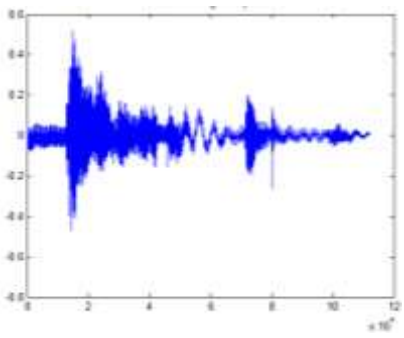


(a)

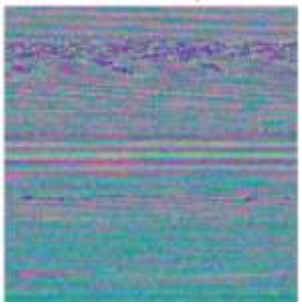
(b)

Fig. 2: Wave and Gray image. (a) 30s 24 bit CD quality wave audio file at 48 kHz. (b) 256x256 Gray image

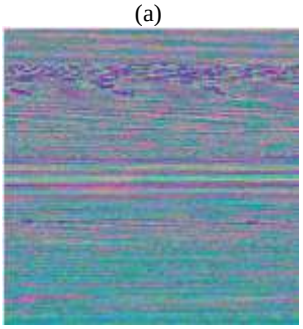
Fig. 3.(c) shows the result of using LSB technique to embed the secret image. Before data transmission, the colored cover image is converted back into audio (stego wave) as shown in Fig. 3.(d)



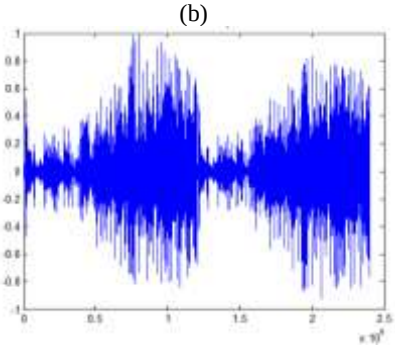
(a)



(b)



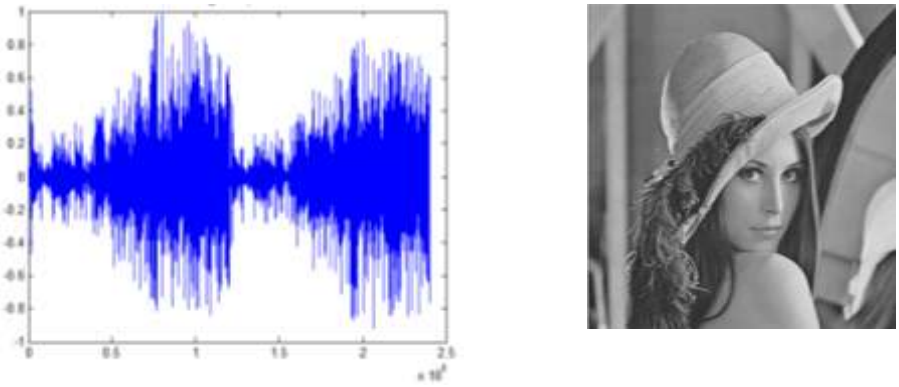
(c)



(d)

Fig. 3: (a) Subset of samples. (b) Colored Cover Image. (c) Cover Image after embedding the secret image. (d) Wave audio (stego wave) after hiding.

In the extracting phase, the input to our technique is the wave audio file (stego wave) as shown in Fig. 4.(a). The reverse process is applied to the stego wave to recover the secret image as shown in Fig. 4.(b).



(a) (b)

Fig.4: (a) 24 bit stego wave audio. (b) 256 x 256 Reconstructed Secret Gray image

The technique we use is secure and offers a high quality of steganography process in terms of PSNR. The stego wave produces a PSNR value that is equal to 157.0246 while the reconstructed secret image gives a PSNR value equals to 47.4907. The results show that the value of PSNR is acceptable and there is slight quality degradation.

We applied several attacks on our technique such that salt and pepper, Gaussian, DCT, histogram, brightness, and darkness. The results showed that the embedded secret gray image is not fragile and can be retrieved with minimal distortion.

4 CONCLUSION

In this research, we presented an efficient technique for hiding data in audio signals. In the proposed technique data can be hidden in audio samples of different sizes (8, 16 or 24). The basic idea of our technique is that the cover 24 bit audio samples are being scaled and mapped into a colored cover image in which the secret data is distributed across the LSBs of the image layers. Distribution of the secret data in the image layers makes our technique highly secure and increases the capacity of the data hidden. From the experimental results, it is found that the hidden secret data creates minimal changes in the cover audio and without altering its quality. Moreover, the secret data itself is successfully hidden and extracted with minimal distortion.

References

Poulami Dutta, Debnath Bhattacharyya and Tai-hoon Kim (2009). Data Hiding in Audio Signal: A Review. *International Journal of Database Theory and Application 2*(2): pp.1-8.

K. Gopal Gopalan, Daniel S. Benincasa and Stanley J. Wenndt (2001). Data Embedding In Audio Signals. *Aerospace Conference 6*(10-17): pp.2713-2720.

Nedeljko Cvejic, Tapio Seppanen (2004). Reduced distortion bit – modification for LSB audio steganography. *Proc. IEEE International Conference on Signal Processing, Beijing*, China 204-207.

H.B. Kekre, Archana Athawale, Swarnalata Rao and Uttara Athawale (2010). Information Hiding in Audio Signals. *International Journal of Computer Application(0975-8887) 7*(9).

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.

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.

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.

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

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

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