A New Steganographic Method for Embedded Image In Audio File

Dalal N. Hmood *dal_scin81@yahoo.com*
Computer Department/College of Science
University AL-Nahrain
Baghdad, 10001, Iraq

Khamael A. Khudhiar *khamail_abbas@yahoo.com*
Computer Department/College of Science
University AL-Nahrain
Baghdad, 10001, Iraq

Mohammed S. Altaei *mohammedaltaie@yahoo.com*
Computer Department/College of Science
University AL-Nahrain
Baghdad, 10001, Iraq

Abstract

Because secure transaction of information is increasing day by day therefore Steganography has become very important and used modern strategies. Steganography is a strategy in which required information is concealment in any other information such that the second information does not change significantly and it appears the same as original. This work presents a new approach of concealment encrypted mobile image in a audio file.The proposed work is replacing two LSB of each byte in audio file and these bytes are choices as randomly location. It becomes very difficult for intruder to guess that an image is hidden in the audio.

Keywords: Steganography,Encrypted, Wavelet,Quantization,LSB;

1. INTRODUCTION

In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file[1]. Steganographic systems, can be divided into two categories, one is in which the very existence of the message is kept secret, and non steganographic systems, in which the existence of the message need not be secret[3].

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed [2].

This paper is an attempt uses an audio file as a cover media to hide an mobile image without making noticeable changes to the file structure and contents of the audio file based on two Least Significant Bit insertion method of the low part of the audio file, as it has been already proved that modification of LSB creates a minimal change in the audio file format. Section 2 describes some of the related work, Section 3 describes hiding Methodology, section 4 describes experiments and results. Conclusions are explain in Section 5.

2. RELATED WORK AND CONTRIBUTION

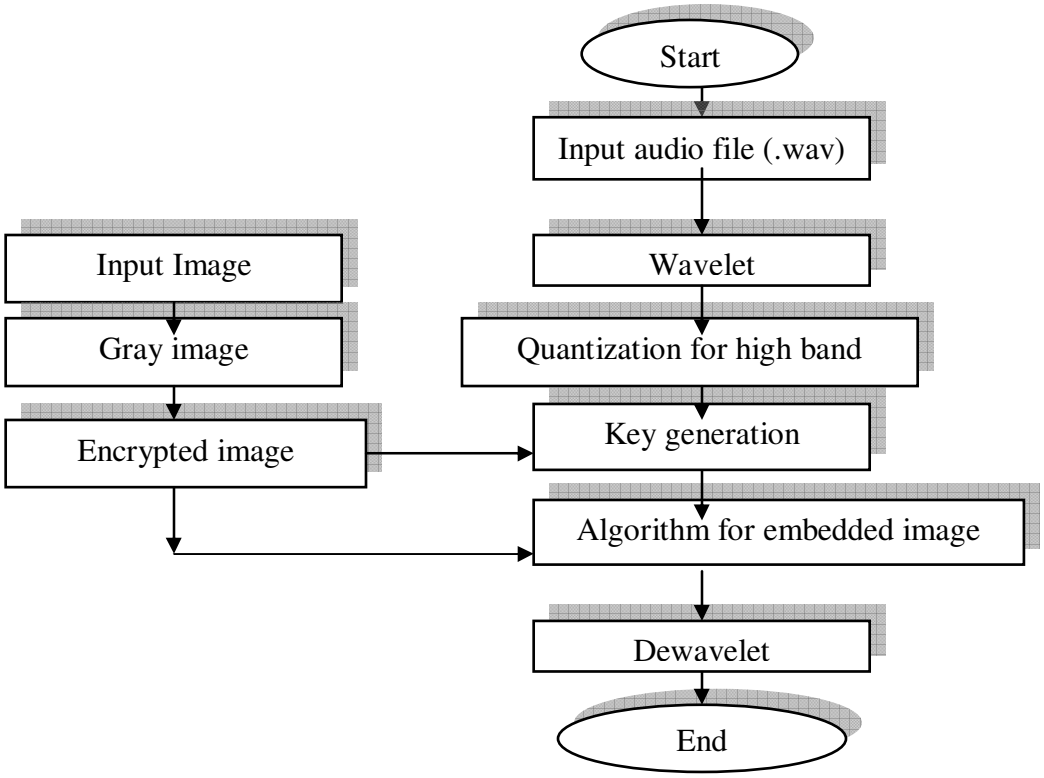
Information hiding is the technology to embed the secret information into a cover data in a way that keeps the secret information invisible. This paper presents a new steganographic method for embedding an image in an Audio file. Emphasis will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method of data hiding in voiced audio.

Steganography has become great area of interest for researchers as need for secure transaction of information is increasing day by day. Information may be text, image, audio or video. Steganography is a technique in which required information is hided in any other information such that the second information does not change significantly and it appears the same as original. This paper presents a novel approach of hiding image in a video. The proposed algorithm is replacing one LSB of each pixel in video frames. It becomes very difficult for intruder to guess that an image is hidden in the video as individual frames are very difficult to analyze in a video running at 30 frames per second. The process of analysis has been made more difficult by hiding each row of image pixels in multiple frames of the video, so intruder cannot even try to unhide image until he get full video.

In other paper taken an in-depth look on steganography by proposing a new method of Audio Steganography. Emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method for data hiding in audio. The contribution of present paper is segmenting audio file in two bands (low band and high band) and used high band(unvoiced) for hidden encrypted image,and used a new approach for generate key from encrypted image .In most paper use 1LSB but we used in this paper 2LSB.

3- PROPOSED METHODOLOGY

This proposed method to hide encrypted image in audio file (.wav) as shown in FIGURE 1



3.1 Encrypted Image

Message is the data that the sender wishes to remain it confidential. It can be plain text, other image, or anything that can be embedded in a hit stream such as a copyright mark, a covert communication, or AUDIO file.

After convert color image to gray image each byte in the image is converted into binary representation. for an example if we are taking the first byte in the image equal 97 then "first byte=" 01100001 is stored in byte array. Because binary equivalent for 97 is 01100001, and then used the rotate bits of image and randomly key that we choose between (0-255) such as 128 BY using XOR operation to encrypted image, as shown in the **FIGURE 2.**

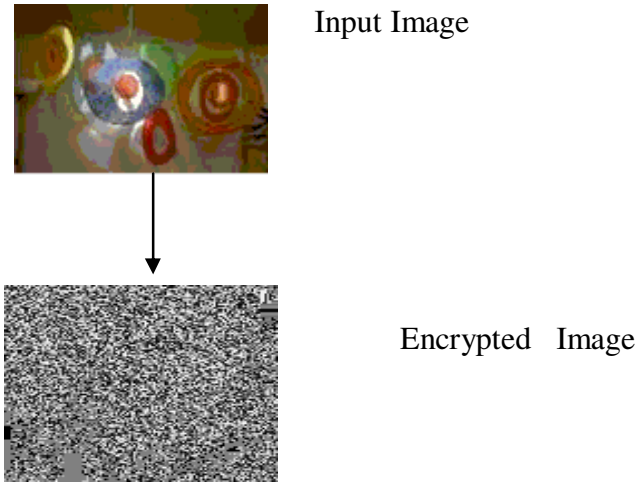


FIGURE 2 Encrypted Image

3.2 Generated Random Key From Encrypted Image

The best means of obtaining unpredictable random numbers is by measuring physical phenomena such as radioactive decay, thermal noise in semiconductors, sound samples taken in a noisy environment, and even digitized images of a lava lamp. However few computers (or users) have access to the kind of specialized hardware required for these sources, and must rely on other means of obtaining random data.

The term "practically strong randomness" is used here to represent randomness which isn't cryptographically strong by the usual definitions but which is as close to it as is practically possible.Due to size constraints, a discussion of the nature of randomness, especially cryptographically strong randomness, is beyond the scope of this work. A good general overview of what constitutes randomness, what sort of sources is useful (and not useful), and how to process the data from them, For example: - pixel value of image was 99

0	1	2	3	4	5	6	7
0	0	1	0	0	1	1	0

Rotate the bit

0	1	2	3	4	5	6	7
0	1	1	0	0	1	0	0

Implemented XOR between bits of pixel and bits after rotate

0	1	2	3	4	5	6	7
0	1	0	0	0	0	1	0

2 0 0 1

The last stage finds the summation of two bits

The key= 2+0+0+1=3

$$Key=\sum_{i=0}^{3}\sum_{j=i*2}^{i*2+1} byte(j)*2^{k} \qquad k=\begin{cases}0\\ \\ 1\end{cases} \qquad \text{---------- (1)}$$

The last stage using ***equ.1*** to calculate key

3.3 Wavelet Transform:

The original sound signal is broken up into two parts low frequency and high frequency using Wavelet Transform then used high frequency part to embedded encoded image.

Low frequency of Wavelets of audio file | LOW | HIGH | igh frequency of Wavelet of audio file

3.4 Least Significant Bit replacement (or coding)

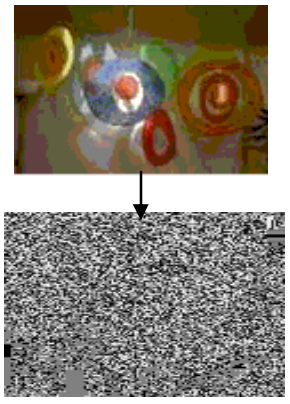
Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the two least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.LSB is the most simple and a straight forward approach to embed or hide a message into a cover-audio [3]. The message is embedded with sequence-mapping technique in the bit of a cover-audio. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the audio if they are suspicious that there exists secret information that was embedded in the audio.

3.5-Getting Encrypted Image From Audio File

In this system using the reverse steps for the proposed Method for getting encrypted image and then decrypted for getting the original image in which hiding in the audio file.

4. EXPERMINAT AND RESULT

Encrypted low resolution image with size(m×n) and hiding in audio file after processing illustrated sequence above and shown result in Figures(2,3,4,5,6,7).



Input Image

Decrypted Image

FIGURE 2: Encrypted Image

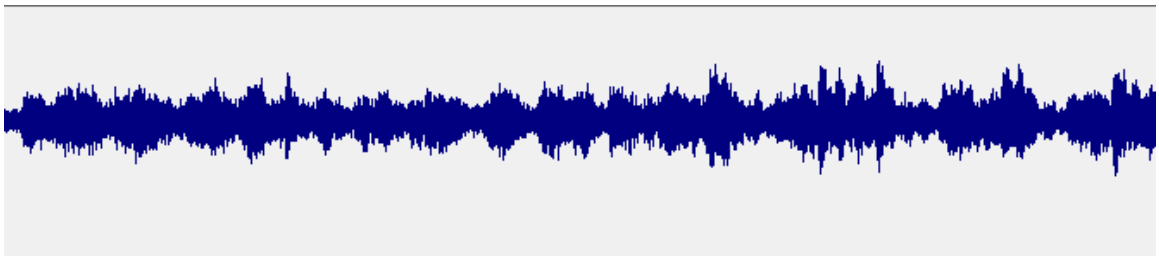


FIGURE 3:Original wave

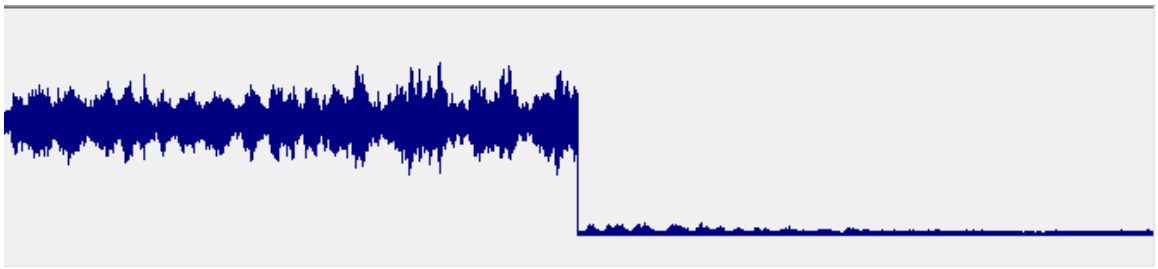


FIGURE 4:Wavelet of audio file

128	128	128	127	128	128	128	128	128	2	0	8	3	4	6	5	2	0	2	0	4

Low frequency **high frequency**

TABLE 1: Data of Wavelet of audio file before embedded encrypted image

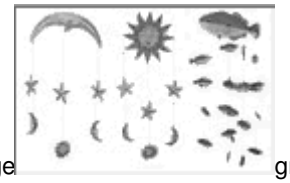
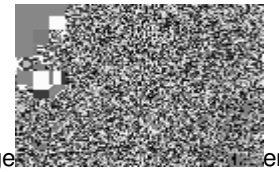

original image 
gray image 
encrypted image

FIGURE 5: Encrypted Low Resolution image

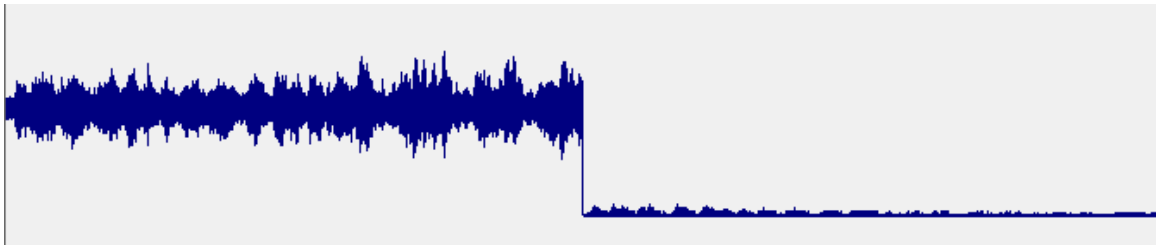


FIGURE 6: Hiding image in audio file

128	128	128	127	128	128	128	128	128	2	1	8	7	3	6	5	0	0	2	2	4

Low frequency **high frequency**

TABLE 2: Data of Wavelet of audio file after embedded encrypted image

FIGURE 7: stego audio file

To measure the difference between the original cover and stego-audio we use the Peak Signal to Noise Ration (PSNR), which expressed as the following ***equation [2,3]***

$$PSNR=10Log10\ \frac{255^2}{MSE} \quad \text{..... (2)}$$

and Mean-Square Error (MSE) is defined as:-

$$MSE=\frac{1}{M}\sum_{J=1}^{M}(X_J - X'_J)^2 \quad \text{..... (3)}$$

5. CONCLUSION

A new approach of embedding an image data into the audio file using LSB based Audio Steganography has been successfully developed and implemented as discussed in this paper. Proposed method is hiding encrypted image in random position based on encrypted byte of image in low frequency of audio file using 2LSB algorithm .Better results are analyzed by both the subjective listening testing i.e. Mean Opinion Score and Objective testing i.e. signal to noise ratio graphs. Moreover, how the performance is affected by changing different bit positions has also been reported in this work using (PSNR =61.863 and MSE=0.329). The main aim of this research work was embedding of image into audio as a case of audio steganography. In test cases, the image data has been successfully embedded and extracted from the audio file.

6. REFERENCES

[1] Jain Ankit, "Steganography : A solution for data hiding", Guru Nanak Dev Engineering College, Ludhiana

[2] Pradeep Kumar Singh, and R.K.Aggrawal, "Enhancement of LSB based Steganography for Hiding Image in Audio", *International Journal on Computer Science and Engineering*, Vol. 02, No. 05, 2010, P 1652-P1658.

[3] MAZLEENA S., MOHD R. K., MUHALIM M. A., and SUBARIAH I., " INFORMATION HIDING USING STEGANOGRAPHY", UNIVERSITI TEKNOLOGI MALAYSIA, 2003.

[4] Kriti Saroha and Pradeep Kumar Singh, "A Variant of LSB Steganography for Hiding Images in Audio*", International Journal of Computer Applications, Volume* 11– No.6, December 2010.

[5] Kriti Saroha SOIT CDAC U.P., INDIA Pradeep Kumar Singh Department of Computer Science ,KIETU.P., INDIA "A Variant of LSB Steganography for Hiding Images inAudio" *International Journal of Computer Applications (0975 – 8887)*Volume 11– No.6, December 2010

[6] Dr Osamah Abdulgader Al-rababah,"A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III*" College of Alkamel - Computer Department king Abdulaziz university- 110Alkamel 21931 Jedda, Saudia Arabia*, IJCSNS International Journal of Computer Science and Network S 202 ecurity,* VOL.10 No.7, July 2010

[7] Souvik Bhattacharyya and Gautam Sanyal, "Hiding Data in Images Using PCP", *International Journal of Computer and Information Engineering* 3:3 2009.