International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 18 (2018) pp. 13697-13701

New Method for Hiding Secret Message and Book in Audio

Alhussain AKOUM[1]

[1] *CCNE Department, Faculty of Technology,*
Lebanese University, Liban

Abstract

Ensuring the security of information is a critical point when sending data over the internet. For this reason, steganography is used widely these days where the message is hidden totally in a cover data such as image or audio, so that no one can be able to detect the message other than the sender and the receiver. In our previous work, we proposed an algorithm for hiding secret message and book in an RGB image. In this paper, we propose a new method for hiding message and book in an audio file. This paper discusses two main parts. The first one is an algorithm for embedding the secret message or book in the audio file, and this subsystem will be at the sender side. The second part is the algorithm for recovering the message, and this subsystem will be at the receiver side. The recovered message which is formed of images retains exactly the same quality of the initial one (0% loss). The size of the audio file holding the secret message or book will be normal and not large.

Keywords: Steganography, Cover Audio, Security, Quality, Size.

INTRODUCTION

The term "steganography" is of Greek origin and it means hidden writing [1] [2], where Greeks in the past when they want to send secret messages, they bring a trusted slave and tattoo the message on his head after shaving it, and wait for the hair to grow up again before sending him to the specified place.

Nowadays, most information and messages are in digital form and exchanged between people using the internet. When all people can have access to the internet and there is probability that third parties can access the data exchanged between two destinations, the users of the internet were worrying about the secret information they transmit through this web. Consequently, the "Cryptography" science appeared for ensuring the security of the information exchanged between two stations by encrypting data in different techniques. But encryption still not the final solution for saving information from hackers or third parties, since encryption does not hide the data at all, but it makes the data meaningless to any third party, which means that someone can at least try to decrypt the message[3] [4]. For this reason, "Modern Steganography" is used today for saving data instead of encryption, since steganography is powerful than cryptography, where steganography hides the message or information at all in a cover data so that no one can even notice that there is a message embedded inside the used cover data knowing that steganography doesn't make any changes to the embedded secret message [5] [6] [7]. This technique for securing digital information is important for the intelligence services, states security. Also it is used for hiding secret personal information and for copy right proofing [8] [9].

The most famous steganography techniques use images as cover data, and our previous work uses RGB image as cover data. Audio files also can be used as message holder for any secret message. In this work, the cover data is an audio file holding the information of the message that can be made up of several pages (images) or it can be a book.

The proposed system is of two subsystems. The first one is for hiding the message in the audio file. The second one is for recovering the message from the audio file, where no one can recover this message without passing an authentication test for ensuring security. In addition, the technique of embedding and extracting the secret message is unknown to any third party. It is a private issue between the sender and the receiver.

We will discuss the encoding subsystem in the second section, the decoding subsystem in the third section, the experimental work in the fourth section, then a conclusion and future plans in the fifth and the sixth sections respectively.

ENCODING SUBSYSTEM

The message that we want to hide in the audio file may be made up of several pages which are in the format of image where these images can be of any extension (.jpg, .tif, etc) and of any type (binary, grayscale, RGB, etc). We will deal with bitmap images (.bmp) that will be converted to audio files.

Hiding Secret Message

The message pages or images will be selected at first. We have to know the characteristics of each page (image) of the message like the dimension, the type (RGB, grayscale...) and the number of images that form this message. It is preferred that all pages share the same type and dimension. The images we will use will be of dimension 800x600. Since audio files are represented in computer memories as column vectors and images as matrices, then we have to change the aspect of the images in order to have a pattern similar to the audio pattern. In other words, we have to convert the matrices we have into column vectors (matrices of single dimension). For each image or matrix we will move through the entire columns, which means from column 1 to column 800. When we stand on a column, we select the entire rows corresponding to this column. Every column we select will be concatenated vertically with the previous one using the "vertcat" function in Matlab. Then, we will obtain 800 columns each of 600 rows or elements, and these columns are arranged orderly over each

other's to form one long vector which is the shape of an audio file with one channel.

This long vector will be converted to real audio signals using the "audiowrite" function in matlab where we will deal with wav files (.wav). The function "audio write" excepts unsigned integers represented over 8 bits (uint8) as the input data type of the column vector to be a wav file and normalize the values of the vector to make them in the range -1.0≤0≤1.0 using the following formula: normalized_value=(initial_value-128)/128 where the usage of the value 128 is because the initial values in the pixels in each image are integers between 0 and 255 (8 bits), then (2^n)/2=2^7=128 [10]. So it can be written as wav file. There are sensitive parameters we have to take care of for avoiding long audio length and large file size such as the sampling frequency and the bit depth which is the number of bits per sample.

We use 44.1 KHz as the sampling frequency which is suitable for the resultant column vector we have so that the length of the wav file will not be long. We will choose 8 as the value of bit depth (bits per sample) where this is the minimum value that can be assigned to the bit depth which will make our wav file small in size without altering the samples of the audio.

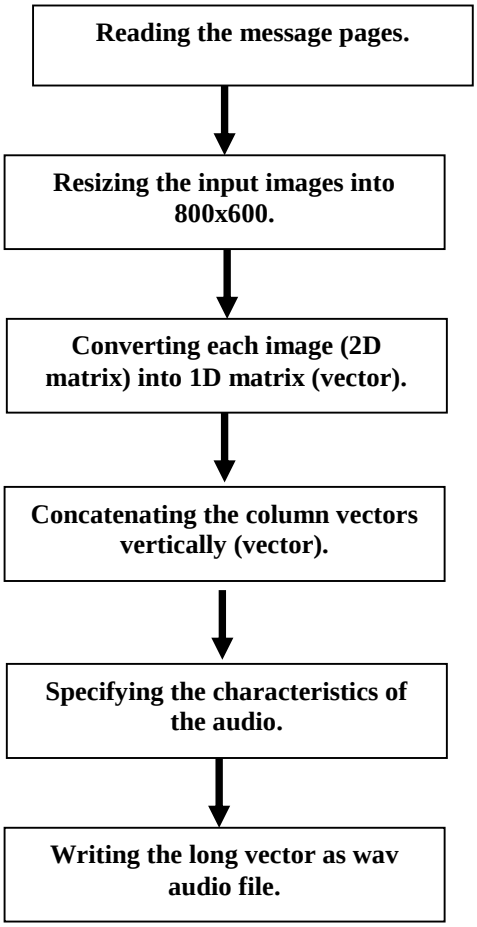


Figure 1. Encoding Subsystem Diagram.

Hiding Book

The idea of hiding a book in an audio file is similar to that of hiding a message, but here we have multiple pages. For hiding a book in audio file we have two options: either to read the pages and transfer them into column vectors and then concatenate them vertically to form the long vector that will represent the audio, or to hide the book pages in an image and then convert this cover image into column vector that will form the audio file, and after recovering this cover image from the cover audio we extract the book pages from it.

No matter how much the book is big, where the size of the cover audio will stay small with respect to the number of pages of the book and the size of each page and its resolution. It is not necessary to arrange the pages of the book or even the message in the normal way proposed where the column vectors which were initially matrices (images) are directly after each other's, but we can distribute the columns as we want in an ordered manner. This point is for ensuring very high security. This means that even if a third party knows about the hidden message which is normally impossible and tries to extract the hidden data, the hidden message will be meaningless to it, since no one can reconstruct the hidden message in a cover data without knowing how the message information are distributed in the cover audio or image.

DECODING SUBSYSTEM

To extract the hidden message from the cover audio which is a column vector, we have to know the dimension of each page, its type, and the number of pages. As in the encoding part, we suppose that the dimension of each page is 800x600. If the images are grayscale, then we have one plane which means that we select 480,000 (800x600) rows (samples) from the column vector to form a page from the secret message, where if the type of images that we have used is RGB, then we have to select 480,000x3=1,440,000 samples for reconstructing the green, red, and the blue planes of the colored image. When a group of samples representing a page is selected from the column vector, it must be converted into 2D matrix to be in the form of the initial image.

Then the values of this matrix will be transformed from the type double in the range -1.0≤0≤1.0 to the initial values that are of type integer between 0 and 255 by using the previous formula after reforming it to be:

initial_value=normalized_value*128+128 .

EXPERIMENTAL WORK

In this experiment we will hide a message made up of 3 pages. Each page is a grayscale image of dimension 800x600 and they are shown in figure 2 below.

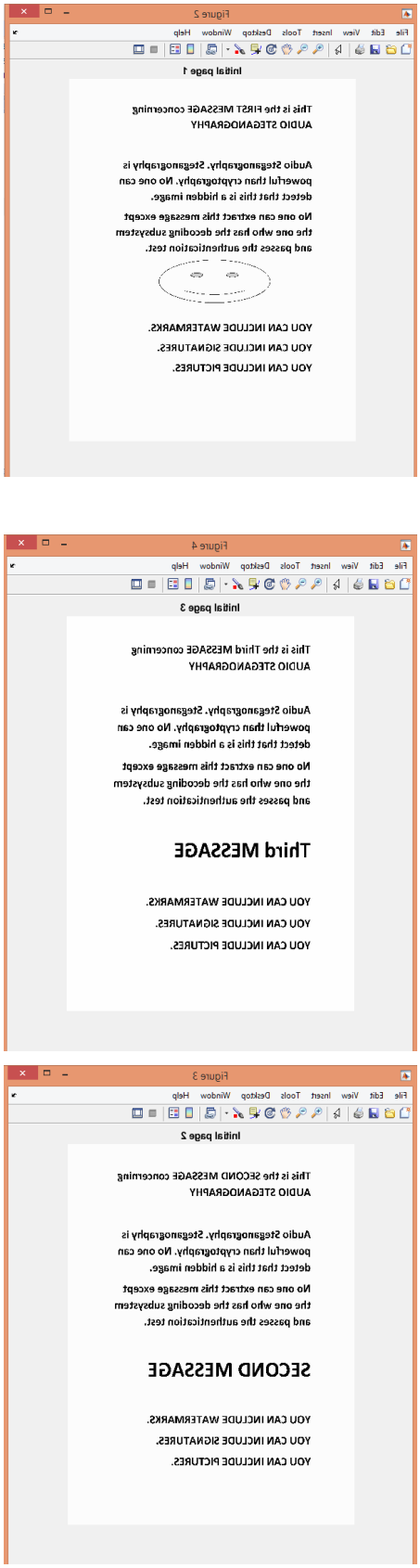


Figure 2. The Three Pages of the Secret Message.

Each page is a 2D matrix of dimension 800x600. We will convert every matrix into vector (1D matrix) to obtain 3 vectors representing the three images, where these vectors will be concatenated vertically or places over each other to form a single long vector. Dealing with grayscale images is simple than RGB images, since here we have in each image only one plane instead of three. This vector will be written as wav file to avoid compression that will destroy the embedded information. The audio file that we have obtained is of size 1.1 MB and of length 32 seconds. This audio file has one channel because it consists of one single vector. Portion of the audio signals is shown in the figure above.

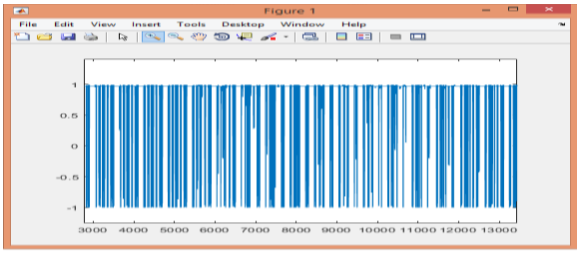
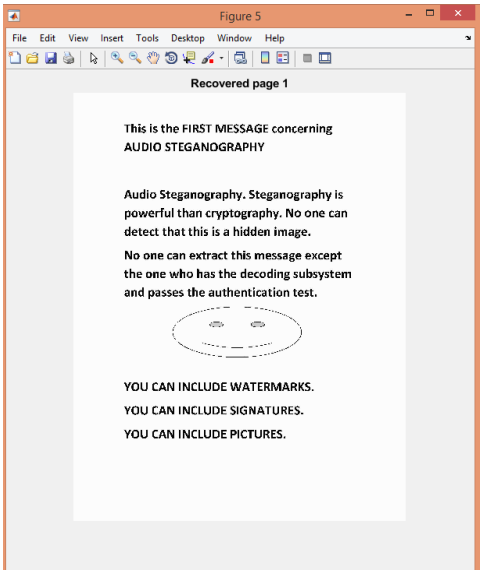


Figure 3. Sample of the Audio File.

To extract the message from the audio file we have to read the audio file holding the secret message first. Since each page is of dimension 800x600, we have to select 480,000=800x600 rows or samples from the column vector to reconstruct the initial 2D matrix that forms the image.

We will obtain 3 matrices. Each element in each matrix holds a normalized value of type double belonging to the range $-1.0 \leq 0 \leq 1.0$. The initial values of the message images are normalized by matlab since it is easier for processing audio. We apply the formula mentioned in the decoding section in order to recover the initial values. Then we cast the obtained initial values to be represented as integer values between 0 and 255 using the "uint8" function in matlab.



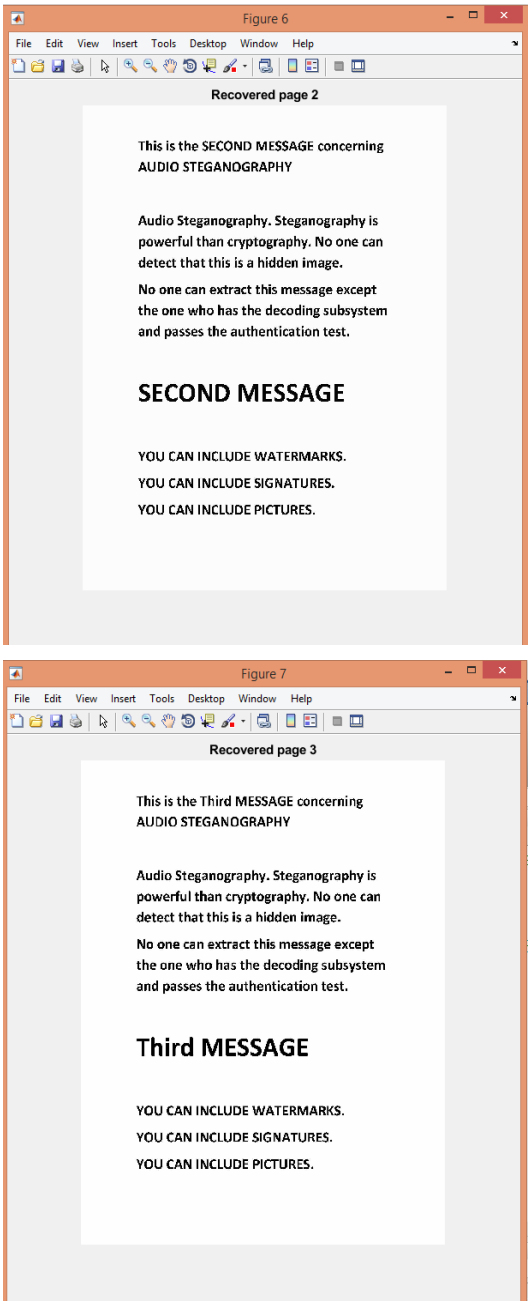


Figure 4. Extracted Message.

The recovered message is completely identical to the initial one, where there is no loss in quality at all. Any image of these can be holding also hidden information which can be extracted without any loss. Hiding a book means hiding multiple pages or images that can be processed in the same way.

CONCLUSION

In this novel we discussed a new method of steganography which is hiding message and book in an audio file without losing any information or quality and without facing size issues with the cover audio even if the hidden data are somehow large in size. The science of steganography is being developed and will still. In addition, the radius of this science is widening to cover more fields. There is no limits for modern steganography growing, because all media and data types are represented in memories in binary form, so we can also hide images in video or even video in a single image.

The system we discussed is a windows version. Our future plans are focused on 2 parts: The first one is releasing an android version of this system to make it easier for smart phone users to benefit from securing their exchanged messaged and information over the internet. The second part is hiding a video in a single image and images and books in a video to be able then to hide a digital library of data in a single video.

REFERENCES

[1] Djebbar, F., Ayady, B., Hamamz, H., Abed-Meraimx, K.: “A view on latest audio steganography techniques”, In: International Conference on Innovations in Information Technology (IIT), IEEE, 2011.

[2] Vipul Sharma and Sunny Kumar.,“A New Approach to Hide Text in Images Using Steganography”, ISSN: 2277 128X, pp.701-708, Volume 3, Issue 4, April 2013.

[3] Nishith Sinha, Anirban Bhowmick ,B. Kishore, “Encrypted Information Hiding using Audio Steganography and Audio Cryptography”, International Journal of Computer Applications, pp. 0975–8887, Volume 112 – No. 5, February 2015.

[4] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, pp. 1-5, 2009.

[5] Jayaram P, Ranganatha H R, Anupama H S, “Information Hiding Using Audio Steganography – a Survey”, The International Journal of Multimedia & Its Applications (IJMA), pp. 86-96, Vol.3, No.3, August 2011.

[6] Sridevi, R., Damodaram, A., Narasimham, S.: “Efficient Method of Audio Steganography by Modified lsb Algorithm and Strong Encryption Key with Enhanced Security”, Journal of Theoretical and Applied Information Technology, pp. 767-671, 2009.

[7] R SRIDEVI, DR. A DAMODARAM, DR. SVL.NARASIMHAM, “Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security”, Journal of Theoretical and Applied Information Technology, pp. 768-771, January 2009.

[8] Asad, M., Gilani, J., Khalid, A.: “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”, International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, July 2011.

[9] Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F.J., Pogreb, S.: “Techniques for data hiding”, IBM

SYSTEMS JOURNAL, VOL 35, Issue 3.4, pp. 313-336, 1996.

[10] Jyh-Shing Roger Jang, "Audio Signal Processing and Recognition," available at the links for on-line courses at the author's homepage at http://www.cs.nthu.edu.tw/~jang.