Proposed Steganography Method to Hide Image Data in Wav File

Salwa K. Abd Allteef,
College of Computer and Mathematics Science, Tikrit University

Abstract

This paper produces a new suggested method for hidden image information in the wav file. The method takes any type of image file format such as (BMP, GIF or TIFF) that contain the image information to be hidden that represented in binary form, then this file hides in the wav file by replacing image information with wav file digits. The replacement is done into separate distance. This method is done with out making noise in sound file. We implement our proposed system using MATLAB ver. 7.

Keyword

BMP, GIF, Image file format, TIFF, Wav file, RIFF.

الخلاصة

يقدم هذا البحث طريقة جديدة مقترحة لاخفاء معلومات صورة في ملف wav .تاخذ الطريقة اي نوع من صيغ الملفات مثل (BMP, GIF or TIFF) التي تحتوي على معلومات الصورة المراد اخفائها والتي تكون ممثلة بالصيغة الثنائية.ثم يتم ابدال معلومات الصورة بملف ال wav بمسافات منفصلة وتنفيذ هذه الطريقة بدون عمل تشويش في ملف الصوت. تم تنفيذ النظام المقترح باستخدام لغة ال MATLAB اصدار 7 .

1. Introduction

In computer technology, there is much communication system between human like phone, fax, network, radio, and so on, and the spoken device. Each of them must have minimum security for data transfer, to sure only the person in receiver can know the message. To provide this done, either through using systems communication that gives a high level of security or no using Steganography system. The embed process in digital media not easy, it must be proved many condition to success, To get complete hide must be invisible in multi media, for example the hide in voice recorder is very difficult because the human hear is limited and the frequency limited maximum more than thousand to one [Gopalan,2003], so it is difficult to add or remove information from original data. There are a lot of hiding methods using Steganography available in the literature ,first category messages are hidden in the LSB of the 8 bit binary strings [Jupin,2004] so use Steganography within digital images(bmp, png) using LSB substitution [Nabavian,2007], second category hiding information inside audio files used in low bit encoding [Mangarae,2006], hiding data steganographically in four techniques in voice message, low bit coding, phase coding, spread spectrum embedding and echo hiding [Chang,Moskowitz,1997] and hide messages in wave files[Friedheim,2006-2007].

In this paper we introduce a method of Steganography to hide a file of image of any type of format (GIF, BMP,JPEG) but view the size of file in wave(waveform audio file format),and regain image from wave file container .

2-Précis about image

The image represent in a computer by using two dimensional array of the intensity values, the element in this array is called Pixel [Rudin,1990].the image depend on pixel values .

2.1. Image file format

It means the organizing and storing of the image information, depending on application and requirement of the user [Reddy and Shankar, 2006].

File formats are sequence of data for encode digital information for storage or exchange. They have own peculiar rules and structured.

Image files generally begin with an introductory "Header" section followed by a "body" that contains most of data .The file names usually end with an extension or suffix(3 letters),like (gif or tiff) to help computer programs to recognize them [http://www.JISC digital media].

2.2. Image file size

It determines by number of bytes that increases with the number of pixels that compose to image, and the color depth of the pixel. Also the increasing depth color of the image caused increase in pixel size an 8 bit pixel(1 byte) stores 256 colors. A 24 bit pixel (3 bytes) stores 16 million colors [Jubin, 2004].

3.Wave file definition

Wav (or wave), short for Waveform audio format, is a Microsoft *and* IBM audio file format for storing audio on PCs.

Format it is a variant of the RIFF the abbreviation (Resource Interchange File Format) bit stream method for storing data in "chunks"[Wang]. That has a chunk id, a length and a body of data. The chunk id is 4 letters encoded into 32 bits. The chunk id types are typically unique to the file type if lower case and globally standardized if upper case.

Waves are compatible with Windows and Macintosh standard operating systems.

•Various different chunks are defined for wave files [Chandrasekhar].
–Labeled text, cue information.
–Data and silent regions, compression details, etc.

•Most often the wave files only have two such chunks:
–Format chunk (FMT) (information about the data format).
–Data chunk (the actual samples contained within).

Additional chunks can be used as forensic chunks that contains meta-information about the case, e.g.,

•Case serial numbers.
•Time of acquisition or receipt.
•Identifying information about the specialist analyzing the case.
•Call record information and other details.

3.1. Wave File Format

The wav file format contains the following fields as shown in Figure (1) [Chandrasekhar]:

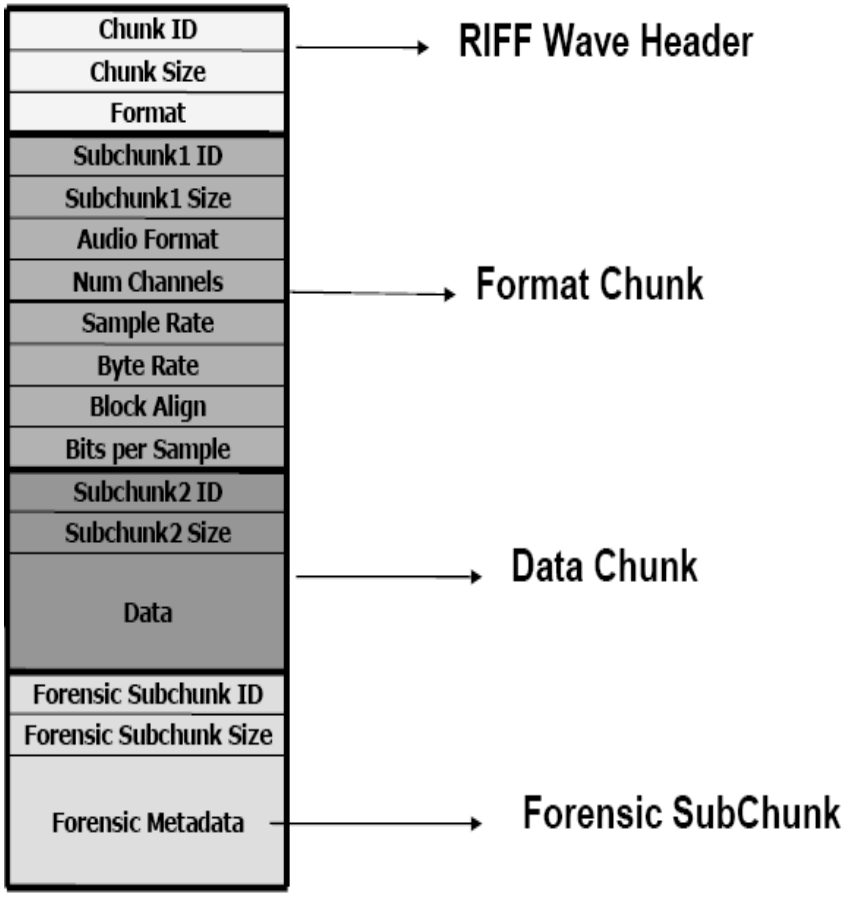


Figure (1): Wav file format

3.2. Wav format chunk

There are general fields and special fields for format wav file shown in table (1): [European broadcasting Union].

Table (1): General and special fields of format wav file

Field	Description
wFormatTag	Number specifying the type of format (Wav) and contain of the format.
wChannal	Specifying the number channels either 1(voice of type mono) or 2(voice of type stereo).
dwSamples Per Sec	Refers to sampling rate per second.
dwAvgbytesPer Sec	Rate bytes pr second operator.
wBlockAlign	Rate of the actual operation sound per second.

4. Steganography

Steganography the art of hiding transmitting data through apparently safe carriers in an effort capability conceal the existence of the data Steganography word originate from Greek, which means covered or hidden writing and includes large array methods of secret communications that conceal the very existence of the message.
Computer based steganographic techniques to embedding foreign information to the native covers, it can be applied in many ways to digital media [Alain].

There are many of the Steganography application such that:-
1- A secret copyright notice or watermark be embedded inside can an image to identify it [Roche and Dugelay,1998].
2- The most important application is to exchange information secret without any doubt the event [Al-dulaimy,2005].

It is not always to be hidden as some system use visible, but most system use invisible.

5. Describe of Binary Files

The binary files are similar in the way that it consists of two main parts:-
1. Header: It the part that contains information about the method, of dealing with data which found in the data part of the file.
These headers are different from each other but it has some basic similarities such as the following:-
-Signature: it consists of Letter symbols or digits give a brief description of the file type, one example in the image files of type BMP start with (BM) letters, which gives a key description of the file in general, and with the header part particularly. The same case with audio files of type (wav), the signature have consists of 4 letters (RIFF) which is the form of multimedia files.
- The complete size of the files which is necessary to know the size that the program will deal with.
- Size of the data part which is necessary when acting with data blocks.
- Size of header part.
2. Data: it is the part that contains the main data for the file, these data will be known in type from the header part information, for example, if we working with image file the data part will contain the image data, which will be after processing and sending to the video card to be drawn could be compressed data or mathematical equation data or specific algorithm data.
What ever the type of all these files, it must contain in the end a set of digits in the binary form. But the way the program interpret these data makes these file understood in a particular form.

6. Proposed algorithms

This paper use idea of Steganography to hiding image information in wav file which the image file and wav file are binary files, and their headers and data parts can be used as set of digits (bytes) in one dimensional array. It is possible to replace its values in a second array which contains the sound data of a wav file. Sound file must be chosen is larger in size according to the image file size. The digital values distributed into different distances in the digital array of sound according to the ratio of the following equation:
Rat= Sound array size / Picture array size

Those replacement digits from sound file will not effect on the sound at the time of operation.

So the rate value of operation of data for sound is (128 kb/s), that is 128*1024 = 131072 Byte / second, this means that it is possible to replace tremendous amount of bytes about 1-100 without affecting the sound. And can be restoring image file form wav file based on the last bytes in signature, are described in as follows:-

1-Algorithm of hidden:-

Input: Image file, Wav file.

Output: Wav file.

Step1: Read image file size (IS).

Step2: Read wav file size (WS).

Step3: If WS /4 < IS file then exit(the wav file is too small to contain this image).

Step4: else calculate ratio (R) distributed into different distance according to: R=WS / IS.

Step5: Replace Byte of image by Byte of wave as 1:R(1 byte for number of bytes R).

Step6: Storage a modified matrix in wav file with signature (the R the image size IS).

2-Algorithm of restore image:-

Input: Wav file contain Image.

Output: Image file.

Step1: Open wav file.

Step2: Read last 8 bytes (signature) will contain R the ratio.

Step3: Loop I=1 to IS

Array [I]=Wav[J]

J=J+R

Next I (stop when the I = IS the image size ,means that wav already done with reading the image information).

Step4: Store the array in an image file.

7. Results

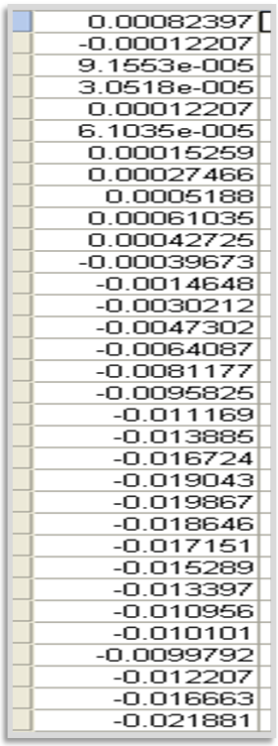
Mat lab tools have been applied the program to read color image file show in Figure (2) that obtain data in Figure (3) which the size of image 100 bytes of BMP Image, so read all three bytes RGB (example above 250 is nearest to white color), and read the wav file so that data are real type can be shown in Figure (4), the size of wav 446 bytes, sample rate 8 kHz, sample size 8 bit. When has selected color or not color image is no difference about hiding because the program deals with the whole file.

The results are plotted in Figure (5), Figure (6), and show the wav file wills no effecting.

Figure (2): Image file

255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
249	249	249	249	249	249	249	249	249	249	249	249	249	249	249	249
253	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
250	250	250	250	250	250	250	250	250	250	250	250	250	250	250	250
251	251	251	251	251	251	251	251	251	251	251	251	251	251	251	251
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
244	244	246	244	246	244	246	244	246	244	246	244	246	244	246	244
248	248	248	248	248	248	248	248	248	248	248	248	248	248	248	248
254	254	254	254	254	254	254	254	254	254	254	254	254	254	254	254
255	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255
253	253	253	253	253	253	253	253	253	253	253	253	253	253	253	253
234	232	232	232	232	232	232	232	232	232	232	232	232	232	232	232
19	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure (3): Part of Image file



0.00082397
-0.00012207
9.1553e-005
3.0518e-005
0.00012207
6.1035e-005
0.00015259
0.00027466
0.0005188
0.00061035
0.00042725
-0.00039673
-0.0014648
-0.0030212
-0.0047302
-0.0064087
-0.0081177
-0.0095825
-0.011169
-0.013885
-0.016724
-0.019043
-0.019867
-0.018646
-0.017151
-0.015289
-0.013397
-0.010956
-0.010101
-0.0099792
-0.012207
-0.016663
-0.021881

Figure (4): Part of Wav file

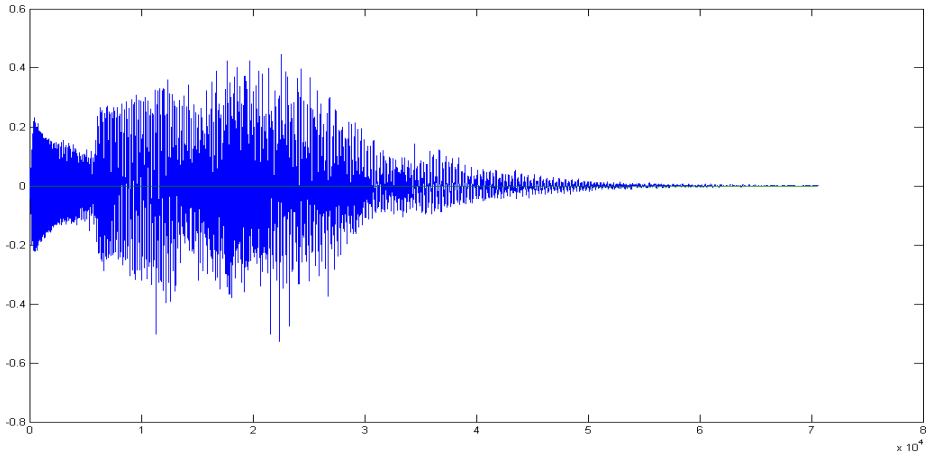


Figure (5): Wav before encryption

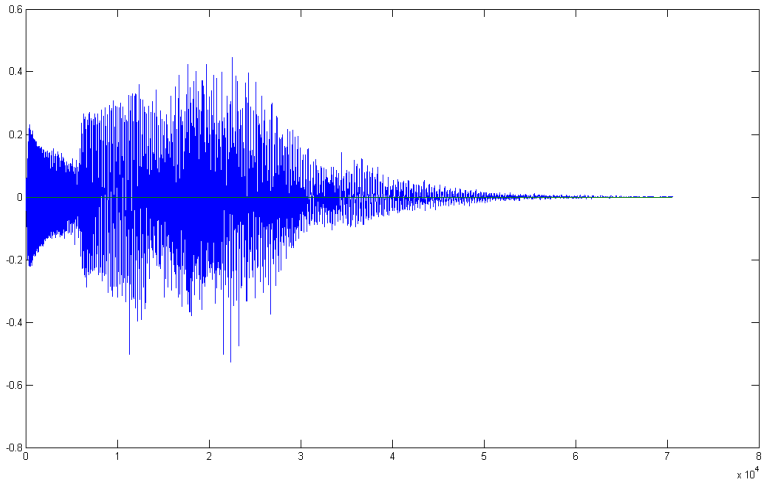


Figure (6): Wav after encryption

7. Conclusion

The proposed method have advantage of simplicity and suitable of hiding ,and can be conclusion:

1- The container file must be larger than concealment file 4 times.
2- In using this method, the image was hidden in wav file without any noise.
3- Adding signature to the container give a key property to the encoding that in the program that encoding this hidden image ,try to look for signature if finding it the program will do the job or the file not contain any image.
4- Steganography takes the safer method in hiding data.

8. Future work

Several futures lines are suggested:

1- This method can be development of action for any kind of hiding the files in wav.
2- The container use a combination of the wav files and not a single file. so we divide the image file into segment ,then store each segment into wav file, and can later be retrieved and merge into wav file.
3- A future step is the hide image into wav file ,then convert wav file format to another ,for example MP3.

References

[Alain] Alain C. Brainos II, "A study Of Steganography And The Art Of Hiding Information", East Carolina University,pp.1-8.

[Al-dulaimy] Meithem. M. Al-dulaimy, 2005," 3D watermark system" ,thesis submitted to the council of college of computer science in the university of technology. [Chandrasskhar] M.chandrasekhar (96D07008), Documentation on Audio sound formats (wav, midi, aiff,au.). "Wave audio sound file format",pp.1-2.

[Chang] L.W.Chang, I.S.Moskowitz,1997,"Critical Analysis of Security in Voice hiding techniques",China,ISBN 3-540-63696-x,pp.203-216.

[European Union] European broadcasting Union,2001,"BWF- a format audio data files in broadcastin",version 1, Geneva, Switzerland, pp.7-8.

[Friedheim] Danny Friedheim,2006-2007,"Implementation of steganographic techniques", Tjhsst *computer* system lab, pp.1-3.

[Gopalan], Kaliappan Gopalan,2003,"audio steganography using bit modification", IEEE International Conference on Acoustics Speech &Signal processing, Hong Kong,pp.629.

[Jupin] Joe Jupin,2004,"Final project-Staganography",pp.3-8.

[Mangarae] Aelphaeis Mangarae,2006,"Steganography FAQ",[Zone-H.Org],pp.6.

[Nabavain] Nick Nabavian, 2007,"CPSC 350 data structure: Image steganography", pp.1-4.

[Reddy] M.Anji Reddy and Y, Hari Shankar ,2006,"Text book of digital Image Processing" ,published by , BBP, ISBN 81-7800-122-5,pp.1-10.

[Roch] S. Roche and J. l. Dugelay ,1998,"Image watermarking based on the fractal transform ", In workshop multimedia signal processing", IEEE,Los angeles , California, U.S.A ,pp.358-363.

[Rudin] B. Rudin, Making ,1990, paper {A look into the history of an ancient craft}V"alling by ,Sweden:Rudins, ISNB 91-970-8882-X,translate from Swedish by Roger G,Tanner.

[Wong] Wai Wong, "data and file format standard", Comp 3600Multimedia systems. [www.JISC] Http://www.JISC digital media-still images file format and compression.htm.