Hiding A Text Inside a WAV Audio File By Using The Maze Method

Akeel A. Thulnoon

Al-Anbar University - College of computer

المستخلص :

إن ظهور الانترنيت وانتشار الوسائط المتعددة و الشبكات المحلية أدت إلى صعوبة نقل البيانات والمعلومات بشكلها الطبيعي من دون تعرضها أحيانا إلى عملية سرقة او وصول غير شرعي إلى البيانات ومن ثم تشويهها أو الاطلاع عليها لذا دعت الحاجة إلى إخفاء هذه البيانات بطرق مختلفة وهذه الطرق أُطلق عليها اسم الاستيكانوغرافي أي "علم الإخفاء."

في هذا البحث استخدمت بعض طرق الاستيكانوغرافي لتشفير رسالة نصية ومن ثم إخفاء الرسالة المشفرة داخل خريطة معينة موجودة داخل متاهة من البيانات حيث يتم بعدها إخفاء البيانات الناتجة بعد التشفير داخل ملف صوت من نوع WAVبحيث يكون من الصعب جدا كشف الرسالة النصية من بين مئات الاحتمالات . وقد توصل البحث الى نتائج رائعة جدا من حيث الإبقاء على وضوح الصوت وعدم تغيير حجمه كما وان عملية فك الشفرة لا تحتاج إلى أكثر من ملف الصوت لإعادة الرسالة النصية بشكلها الصحيح.

Abstract :

The appearance of the internet and the spread of multimedia and interanet made difficult the transmission of data and information in a normal way without being pirated or illegally accessed and its subsequent deformation. So, there was a need to hide these data in different ways that are collectively known as "Steganography".

This paper uses some Steganography algorithms to encode a text message and then hiding this encoded message inside a certain map hidden inside a maze of data. The resulting data from encoding are then hidden inside a WAV audio file. This makes it very difficult to identify this text message among hundreds of probabilities . The hiding process was successful .The sound kept clear and its volume suffers no change .Moreover , the decoding process requires nothing other than the audio file to put the text message back to its correct form.

1. Introduction

The growing possibilities of modern communication need special means of security especially on computer network. Data security in the last few years has gained a wider audience. The main concern in this paper is to deal and define the term "information hiding " and describe one of its important classes of it is called "Steganography " which the proposal system applied some of its algorithms to hide messages into WAV audio files to save messages or secret data from some type attacks or illegal access.

2. Information Hiding

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly [1].

An expanded information-hiding problem space should be characterized as a general-purpose data channel. There are three attributes of this channel that expand the potential application domain: (1) techniques that combine strong and weak data embedding offer a flexibility that gives application designers the ability to move fluidly between robustness and bandwidth considerations; (2) embedding meta-data leads to improved management of assets, not just for the purposes of intellectual-property protection, but for general process and application control; and (3) in a network computing environment, a small amount of embedded data is not a significant limitation. [2]

Steganography and digital watermarking are two areas referred to as " Information hiding".

So the main categories of data hiding are separated into two classes : steganography and digital watermarking [1]as shown in Fig(1). These two terminology are explained in details below:

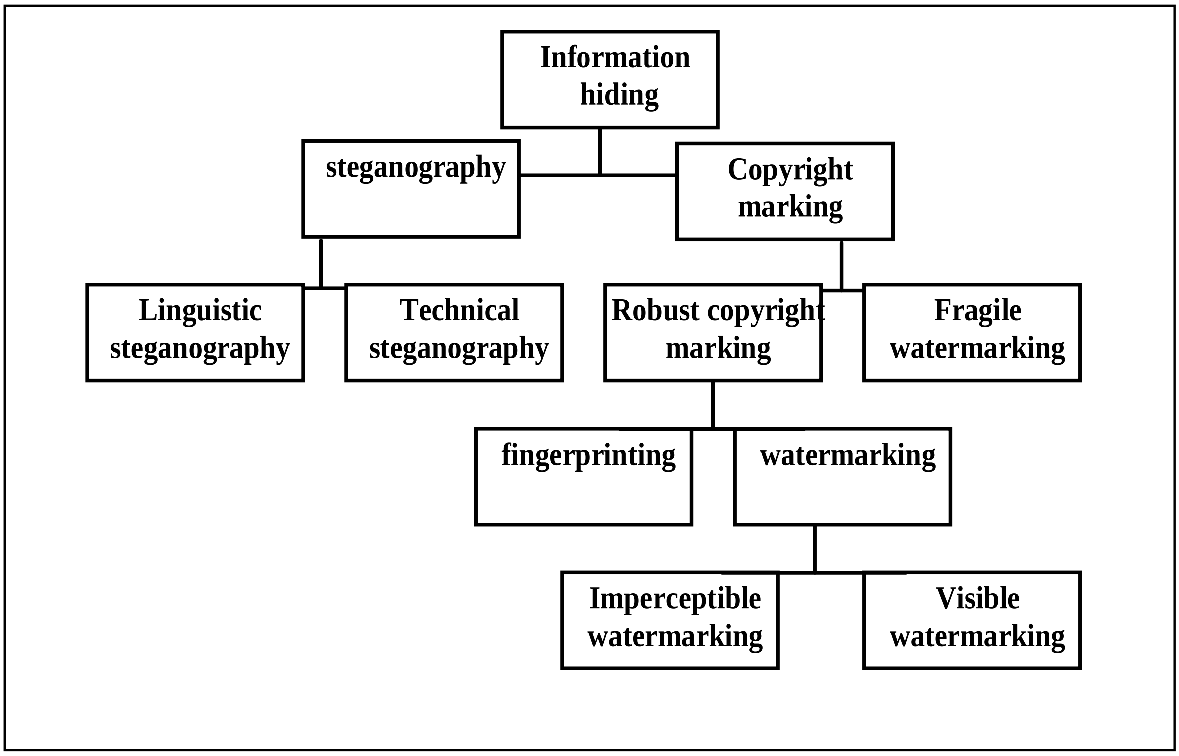


Fig (1) The classification of information hiding[1]

2.1 Steaganography

Hiding information by embedding secret data into an innocuous medium is often referred to as Steganography [3]. Steganography (a word of Greek origin, meaning covered writing), is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. [4]

Steganography is the art of invisible communication. Its purpose is to hide the very presence of communication by embedding messages into innocuous-looking cover objects. In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images,video, and audio files. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a “cover” for hiding secret messages. Each steganographic communication system consists of an embedding algorithm and an extraction algorithm. [5]

A data message is hidden within a cover signal (object) in the block called embedder using a stego key, which is a secret set of parameters of a known hiding algorithm. The output of the embedder is called stego signal (object).

After transmission, recording, and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor as Fig(2)[1] shows :

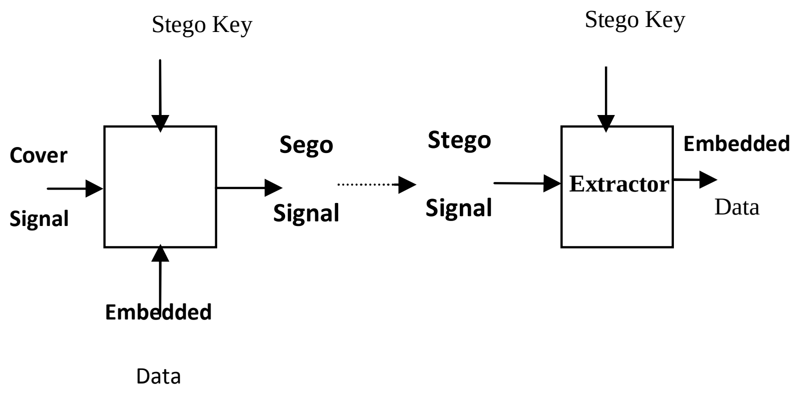
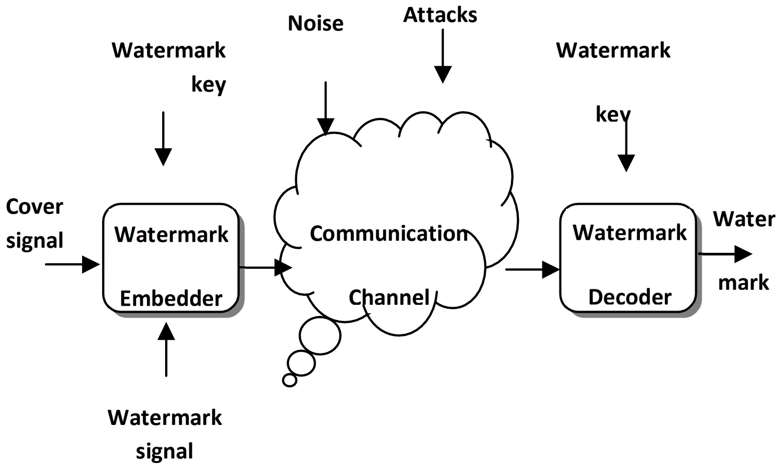


Fig (2) Block diagram of data hiding and retrieval[1]

2.2 Watermarking

Watermarking is a method of inserting information into digital content by adding a signal to the content data so that the difference between the original content and the watermarked version is imperceptible or perceptible to human senses.[thesis],so the main difference between staganography and watermarking is that watermark may be visible or invisible to human senses[6]. Fig(3) shows the watermark system.



Fig(3)The watermarking system[6]

3. WAV Audio File

Sound is energy which travels through the air as one – dimensional continuous wave. Sound is produced by a source and received by a human ear. Sound transmission is not possible without a medium [9].

Digital audio is the most commonly used method to represent sound inside computers, many audio processing devices, and modren audio storage devices like (CD, MD, DVD)[9].

In the proposal system we will use WAV file format because formed by a header part and a data part. As the header part includes binary data with different characteristics, it is appropriate for reading data of different types.The header of a wave file is of 44 byte and the reminder is the data filed .

4. Maze

Maze is the English word for a labyrinth. A maze consists of lots pa paths with hedges in among[7].

Linguistically speaking, the word maze is the colloquial expression for labyrinth which connotes loss of direction or guidance because of endless intersected roads and path that are designed literately for the purpose.[8] .

This meaning of the maze is used in this paper to built a program of hiding and jam the stored messages.

5. Proposed Method

In the suggested system , a method is used to hide a message inside a WAV file. Two encoding methods were used (Nihlist)and (Caiser) , to encode the message, which consists of 169 characters (array 13×13) ,into a encoded message.

After obtaining the encoded message, a maze is created from random data where the message is to be hidden. The maze is a two-dimensional array (25×25) which gives 625 random value of different characters and symbols.

After creating the maze some addresses in it are used a map to hide the data amount of 169 characters inside the maze. After excuting the hiding process inside the maze, the final array (25×25) is hidden inside the WAV file in specific addresses as explained in the following two algorithms :

5.1 Hiding and Execution Algorithm

1..Start.

2. Inputting the WAV file , type mono and sample size 8 bit.

3. Inputting the message intended for encoding which consists of 169 characters as in the following example:

trees are useful to man in three very important ways: they providehim with wood and other products; they give him shade; and they help to prevent drought and floods. In many parts of the world, man has not realized

After removing the spaces among words the following message is obtained:

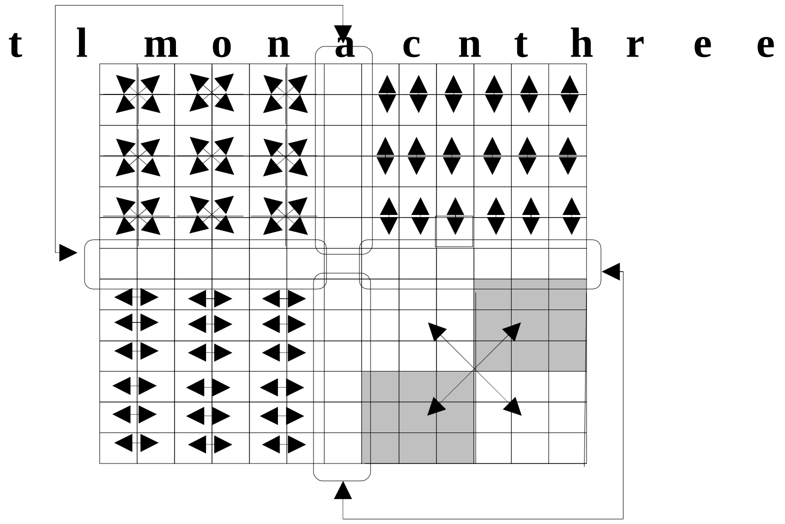
treesareusefultomaininthreeveryimportantways:theyprovidehimwithwoodandotherproducts;theygivehimshade,andtheyhelptopreventdroughtandfloodsinmanypartsoftheworld,manhasnotrealized

3. Converting the message into a two dimensional array (13×13) as shown bellow:

t	r	e	e	s	a	r	e	u	s	e	f	u
l	t	o	m	a	n	i	n	t	h	r	e	e
v	e	r	y	i	m	p	o	r	t	a	n	t
w	a	y	s	:	t	h	e	y	p	r	o	v
i	d	e	h	i	m	w	i	t	h	w	o	o
d	a	n	d	o	t	h	e	r	p	r	d	u
c	t	s	;	t	h	e	y	g	i	v	e	h
i	m	s	h	a	d	e	;	a	n	d	t	h
e	y	h	e	l	p	t	o	p	r	e	v	e
n	t	d	r	o	u	g	h	t	a	n	d	f
l	o	o	d	s	i	n	m	a	n	y	p	a
r	t	s	o	f	t	h	e	w	o	r	l	d
m	a	n	h	a	s	n	o	t	r	e	a	l

Fig(4) The message array (13*13)

4. Applying (Nihlist) method with some modification as shown bellow :



Fig(5) shown Nihlist method

*The symbol ⧗ represent Exchange among four addresses

*The symbol ◀▶ represent Exchange between two addresses in a different row

*The symbol ▲▼ represent Exchange between two addresses in a different column

*The symbol ⤧ represent Exchange between two Groups of 9 addresses

*The symbol ▯ represent Groups of 6 addresses in vertical

*The symbol ▭ represent Groups of 6 addresses in horizontal

*The symbol ↳ represent Exchange between horizontal and vertical addresses

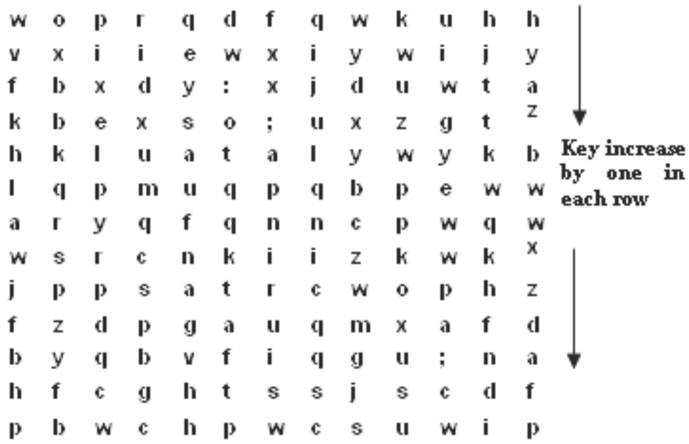
And the final array will be as follows:

r	**t**	**e**	**e**	**a**	**s**	**t**	**e**	**u**	**s**	**e**	**f**	**u**
a	**w**	**s**	**y**	**t**	**:**	**s**	**e**	**y**	**p**	**r**	**o**	**v**
e	**v**	**y**	**r**	**m**	**i**	**;**	**o**	**r**	**t**	**a**	**n**	**t**
a	**d**	**e**	**n**	**t**	**m**	**t**	**e**	**r**	**p**	**r**	**d**	**u**
d	**i**	**h**	**e**	**m**	**i**	**h**	**i**	**t**	**h**	**w**	**o**	**o**
r	**i**	**p**	**h**	**w**	**h**	**e**	**e**	**t**	**g**	**n**	**h**	**n**
m	**i**	**h**	**s**	**d**	**a**	**y**	**y**	**p**	**a**	**m**	**a**	**n**
y	**e**	**e**	**h**	**p**	**l**	**g**	**r**	**l**	**d**	**e**	**w**	**o**
t	**n**	**r**	**d**	**u**	**o**	**i**	**e**	**a**	**l**	**o**	**t**	**r**
o	**l**	**d**	**o**	**i**	**s**	**v**	**d**	**t**	**h**	**;**	**a**	**n**
t	**r**	**o**	**s**	**t**	**f**	**e**	**e**	**v**	**e**	**o**	**p**	**r**
a	**m**	**h**	**n**	**s**	**a**	**h**	**n**	**d**	**f**	**h**	**t**	**a**

Fig(6)The message array after applying nihilist method

Caiser method is applied to the array resulting when key=3 ,with systematic increase by one for each row as in the following array results:

F(a)=(a+key) mod 26------(1)



w	o	p	r	q	d	f	q	w	k	u	h	h
v	x	i	i	e	w	x	i	y	w	i	j	y
f	b	x	d	y	:	x	j	d	u	w	t	a
k	b	e	x	s	o	;	u	x	z	g	t	z
h	k	l	u	a	t	a	l	y	w	y	k	b
l	q	p	m	u	q	p	q	b	p	e	w	w
a	r	y	q	f	q	n	n	c	p	w	q	w
w	s	r	c	n	k	i	i	z	k	w	k	x
j	p	p	s	a	t	r	c	w	o	p	h	z
f	z	d	p	g	a	u	q	m	x	a	f	d
b	y	q	b	v	f	i	q	g	u	;	n	a
h	f	c	g	h	t	s	s	j	s	c	d	f
p	b	w	c	h	p	w	c	s	u	w	i	p

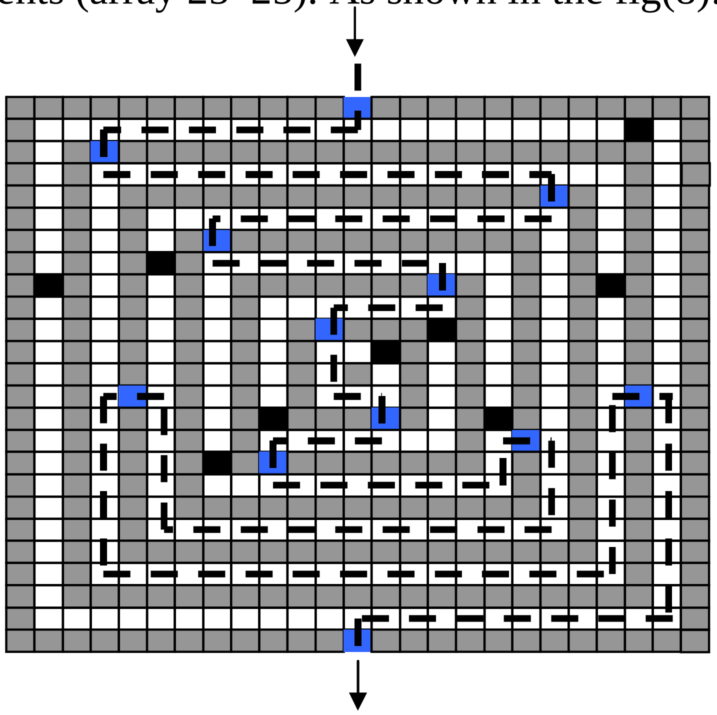
Key increase by one in each row

Fig7)The message array after applying caiser method

The following message is arrived at after final encoding :

woprqdfqwkuhhvxiiewxiywijyfbxdy:xjduwtakbexso;uxzgtzhkiuataiy wykbiqpmuqpqbewwaryqfqnncpwqwwsrsnkiizkwkxjppsatrcwophzfz dpgauqmxafdbyqbvfiqgu;nahfcghtssjscdfpbwchpwcsuwip

The resulting message is stored in specific addresses (map) inside a maze of elements (array 25*25). As shown in the fig(8):



Fig(8) Two dimensional array (25*25) represent the maze

Gray color represents the walls of the maze while white color represent its path. Both of them are a group of random letters and symbols which change after each execution. Blue color represent \s the access to the path while black color represents path end. Dotted line are the map of storage .

5. The storage of the elements of the resulting array in a larger two dimensional array by (25*25) which, in turn , represents the maze. Each elements in the maze will be transform to its ASCII.The storage is done in a previously chosen specific addresses. as shown in fig(8)

6. The storage of the resulting array inside a WAV file in specific addresses resulting from the division of the of the WAV file on 625 (number of the array maze elements 25*25).

$$\text{Address storage=Int}\ \left(\frac{\text{WAV file size}}{625}\right)\text{------}(2)$$

7. Store the resulting files in a new name.

8. End

5.2 Extract Algorithm

The program executes the following steps to decode and retrieve the message :

1- Start.

2- Recalling the audio WAV file after the hiding process.

3- Extracting the stored values from the WAV file where they are stored at specific addresses as explained earlier.

4- Transforming these values into a two dimensional array (25*25).

5- Using the storage map to extract the values of the message , and then transforming them into a two dimensional array(13*13).

6- Applying decoding operations on the resulting array.

7- change the resulting array into a one dimensional array in order to comprehend the message.

8- End.

6. Code strength

The strength of the code lies in the following points:

1. There is a remote probability to uncover the stored message patterns because each execution yields a totally different array.
2. Retrieving a message encoded in array by using the maze method is extremely difficult as it requires hundreds of probabilities .
3. The storing of the maze array contents in distancing addresses in the WAV file reduces the jamming greatly. It is quite inaudible.

4- The program can give another message other than the original message to deceive the hacking people seeking the encoding message

7. Conclusion

1. Maze methods can be used to store large amounts of data ,but it must be taken into consideration that the size of the maze increase with that of the amount of the data , in order to hide the data properly. This in turn , increase the size of WAV file.
2. Used of maze method is flexible as it is possible to execute more than one map from a small maze.
3. The larger of the distance among data storage sites in WAV file, the clearer is the voice.

8. Suggested Future Work

1. Using more than one map to store data in the same program.
2. Making the message array larger.
3. Using other types of audio file likes Mp3,Audio.

Experimenting with the programs on other file types like images and videos.

References

1- Akeel A. Thulnoon, " Watermarking in WAV File Based on Phase Coding",Al-Anbar University College of Computer 2005.

2- Peter Wayner " Information Hiding : Steganography and Watermarking", Third Edition,(October 2009), http:// www.wayner.org/.

3- Kathryn Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Steganography" , University of Waikato Department of Computer Science 2005

4- Ahmed Al-Jaber and Khair Eddin Sabri "Data Hiding In A Binary Image" University of Jordan, Department of Computer Science Email: jahmed@sci.ju.edu.jo , sabrikm@ju.edu.jo

5- Jessica Fridrich1, Miroslav Goljan1, Dorin Hogea2 "Steganalysis of JPEG Images: Breaking the F5 Algorithm , (1) Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton , (2) Department of Computer Science, SUNY Binghamton, Binghamton, NY 13902-6000,

6- Inderjeet Kaur1, Anuradha Rani2 , "DESIGN EVALUATION OF ROBUST ALGORITHM FOR DIGITAL IMAGE WATERMARKING",(1)CSE/ITdepartment, PTU, CEC Landran, inderjeet_k@hotmail.com ,
(2) CSE Department, PTU, AIET Faridkot,
chopra_anuradha@rediffmail.com.

7- "A brief history of mazes " paper form internet www.**mazes**.co.uk/**history**.htm

8- Adrian Fisher "A Short History Of Maze ",internet Paper P9-20 March 2001 www.mazemaker.com

9- Nedeljko Cvejic ,"Algorithms For Audio Watermarking and Steganography", Department of Electrical and Information Engineering, Information processing Laboratory , University of Oulu 2004 P56-65.