Eng. & Tech. Journal, Vol.29, No.4, 2011

# Watermarking in WAV Files Bases on Phase Coding

**Dr. Salah S. Alrawi *, Dr. Rasheed Abdulshaheed ****
**& Akeel A. Alhadithy***

Received on: 24 / 1 /2010
Accepted on: 2/12 /2010

**Abstract**

The growth of the network multimedia open the illegal ways for users to use the digital media without any hindrance or control. This state created, the need for the copyright protection of various digital media. WAV audio files is one of these media, these media file format itself has no built in copy protection controls. Other systems must be used to prevent illegal copying called watermarking. In this paper, we used the phase coding method to embed the watermark, by using FFT method in two ways. The first way used the block size of the wave data equal to ($2^2$) and the second way used the block size of the wave data equal to ($2^3$).

The results of the above two ways shows that, when we use the first way the noise of the sound will be very smaller than the results of the second way. On the other hand the length of the watermark in second way will be longer than when use the first way. Finally, we can say that the two ways yield good results**.**

**Keywords**: Digital Watermarking, Phase Coding, Steganography, FFT, WAV Files.

## استخدام العلامة المائية على الملفات الموجية بطريقة تشفير الطور

**الخلاصة**

التطور الذي حصل في استخدام الوسائط المتعددة في شبكات الانترنيت فتح المجالات غير المشروعة للمستخدمين للحصول على ملفات مختلفة وبطرق غير قانونية.هذه الحالة دعت الحاجة إلى إنشاء أنظمة حماية للملفات المختلفة كملفات الصوت من نوع WAV والتي لم تنشأ لها حماية خاصة بها، لذا استخدمت أنظمة أخرى لحمايتها من النسخ غير الشرعي سميت هذه الأنظمة بـ (العلامة المائية).

في هذا البحث استخدمنا طريقة تشفير الطور لإخفاء العلامة المائية باستخدام طريقة فورير السريعة وبطريقتين . الطريقة الأولى باستخدام حجم بيانات الصوت ($2^2$ ) والطريقة الثانية باستخدام حجم بيانات الصوت ($2^3$). نتائج البحث للطريقتين بينت في حالة استخدام الطريقة الأولى يكون تشويش الصوت اقل من نتائج الطريقة الثانية, ومن ناحية أخرى فان طول العلامة المائية في الطريقة الثانية هي أطول عما هي في الطريقة الأولى . وأخيرا نتائج البحث في كلا الطريقتين كانت جيدة.

## 1- Introduction

The main concern of this paper is to describe and define the term "Information hiding "and speak in some details about the main types of information hiding (steganography and digital watermark). The proposed system uses digital

*** College of Computer, University of Anbar / Anbar**
****Baghdad College For Economic Sciences/ Baghdad**



https://doi.org/10.30684/ etj.29.4.11
University of Technology-Iraq, Baghdad, Iraq/2412-0758

Watermark technique to obtain audio watermarked files to protect them as much as possible from many types of attacks and illegal copies.

Techniques for information hiding have become increasingly more sophisticated and widespread[1].Data hiding represents a class of processes used to embed data , such as copyright information ,into various forms of media such as image ,audio or text with a minimum amount of perceivable degradation to the " host " signal , i.e,the embedded data should be invisible to a human observer. Its goal to restrict or regulate access to the host signal, but rather to ensure that data remain inviolate and recoverable [2].

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 [3].

There are three different aspects in information hiding system: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the over medium; security refers to an eavesdropper's inability to detect hidden information whereas the robustness is to refer to the amount of modification that can be made such that the stego medium can withstand before an adversary can destroy the hidden information[4].

Steganography and digital watermarking are two areas referred as " Information hiding " .So the main categories of data hiding are separated into two classes : steganography and digital watermarking [5 ]as shown in fig( 1 ) try's focus towards information hiding techniques as opposed to the traditional cryptography area.

## 2- Steganography &Digital Watermarking

The most traditional definition for steganography is the art and science of communication in away, which hides the existence of the communication[6]

A data message is hidden within a cover signal (object) in the block called embeddor using a stego key, which is a secret set of parameters of a known hiding algorithm. The output of the embeddor 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 shown in fig(2).

Different definitions have been given for the term " watermarking " in the digital context However , a very general definition is given by Cox[7] which can be seen as application independent " and define the watermarking as the practice of imperceptibly altering a work to embed a message about that work " in this definition the word work refers to a specific sing , video

or picture, this means the term watermarking is what is actual imperceptibly added to the cover signal in order to convey the hidden data [8].

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 to human senses. The information watermarked into the content data is extractable even after the data has been changed by various processes, unless the damage to the watermark is too great. This resistance to obliteration is called the "robustness" of the watermark.

In addition, the watermark should be able to resolve multiple ownership claims (known as the deadlock problem),which is achieved by using the original signal (i.e., the unsigned signal) in the signature detection process.

Finally, If we apply Cox's definition of watermarking into the files of audio signal processing ( The proposed system work ) a more precise definition , this time of audio watermark, can be stated :" Digital audio watermarking " is defined as the process of " embedding " user specified bit stream in digital audio such as that the addition of the watermark (bit stream ) is perceptually insignificant This definition should be complemented with the previous one ,so watermark information here refers to the digital audio file [9].

## 3- WAV File Formats

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 [ 10].

Digital audio is the most commonly used method to represent sound inside a computer , many audio processing devices and modern audio storage devices like CD,MD,DVD) [10].

WAV File Format is a file format for storing digital audio (wav form) data . The WAV file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. A RIFF file starts out with a file header followed by a sequence of data chunks. A WAV file is often just a RIFF file with a single "WAVE" chunk which consists of two sub-chunks -- a "fmt " chunk specifying the data format and a "data" chunk containing the actual sample data. Call this form the "**Canonical form** " [9].

So we can say Wav files are 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. Proposed System

Fast Fourier Transform (FFT) is used in the proposal system to hide watermark inside an audio WAV file. This is applied in two different ways, the first one is when

our operation is based on $2^2$ and the second way when our operation is based on $2^3$ in these two ways we will use the butterfly method to find FFT for the data of the Wave file.
The next algorithm use this keys:
4 When use FFT method $2^2$.
8 When use FFT method $2^3$.
as follows:[9]

$$X[k]=\sum x[n]\exp(-j2\pi kn/N)= \sum x[n]W^{kn/N} \quad \ldots(1)$$

From the above formula we can calculate the FFT values from every 8 or 4 WAV data values depending on the main key ( 4 for $2^2$ and 8 for $2^3$ ).
After calculated the FFT values we must find

$$\text{Amplitude} = \text{sqr}\,( Im^2 + Re^2 ) \quad \ldots.(2)$$

Im = Imaginary Values
Re = Real Values

$$\text{Phase} = \text{Tan}^{-1}\,( Im/Re) \quad \ldots.(3)$$

After finding these two values we modify the values of the phase by embedding the watermark as a serial of 1's for every phase as showing in fig(3).
After adding the watermark to the phase the system recalculate the Im and Re values as follows

$$Im` = \text{Amplitude} * \cos ( \text{Phase1}) \quad ..(4)$$

$$Re` = \text{Amplitude} * \sin ( \text{Phase1} ) \quad ..(5)$$

Now we can recalculate the data of the WAV file by calculating the IFFT as follows :

$$x[k]=\sum X[n]\exp(j2\pi kn/N)= \sum X[n]W^{kn/N} \quad --(6)$$

Finally we make comparison between the main source and the resulting sound.

**4.1 Embedded Algorithm**

Input: The WAVE audio file and watermark.
Output: Watermarked WAVE audio file.
Step1: Select the WAVE audio file that to be Watermarked.
Step2 : Input the watermark to be embedded.
Step3 : Open the Wave audio file and extract
the first 44 byte(WAV file header) to put it in the new file that will be Watermarked.
Step4: Embed the watermark in the remainder
data by using phase coding method.
Step5: END.

**4.1.1 Phase coding algorithm**

Input: The Wave audio file
Output: Watermarked Wave audio file
Step1: Open the Wave audio file.
Step2: Extract the first 44 byte (wave header) and save it in the new Wave file that will be watermarked.
Step3: Select one of this two numbers 4 or 8 ( to select FFT method).
Step4: Apply the FFT method (Better fly method) on the remainder data of the wave file (remainder data = data of the wave file – 44 byte ).
Step5: Calculate the power and Amplitude for every result has real and imaginary values.

*Re:* Real values, *Im* : Imaginary values

$Power = Re^2 * Im^2$

$Phase = \tan^{-1} Im/Re$

Step6: Modify the *phase* to create *phase**

Step7: Recalculate *Re`* and *Im`* values using this formula

*Re`= power * cos ( phase*).*

*Im`= power * sin ( phase* ).*

Step8: With *Re`* and *Im`* we will inject the watermark in ( a direct method) Step9: Apply IFFT using direct method on the result ( after Embedded watermark ).

Step10: Storage the result as one block in the same new wave file as form "44 byte as header and the new result as data for this header " step11 : End

**4.2 Extract Algorithm**

Input : The watermarked Wave file.

Output : The watermark.

Step1: Open the watermarked Wave file.

Step2: Extract the watermark form the watermarked file by using this method which depend on the Embedded method While not eof( F ) Do If phase > phase` then W=1 If phase < phase` then W=0

Arrange the string of W in an array (A[I])

Take six elements form the array A in every check step Apply ord function to this element to obtain the word which represent the watermark.

I=I+1

Step3: print I " number of repetition of the watermark in the fileStep4: END.

## 5. Implementation of Phase Coding

The proposal system used Butterfly method to calculate FFT ,by dividing the data of WAV file into parts that consist of four elements. The butterfly figure will take the form as shown in the following fig(4).

For example if we have WAV data as shown in the follow fig(5)

The first four parts comprise elements (128,232,56,49) these elements can be represented by $N^2$. To calculate FFT for these elements we use butterfly method as follows:

x1=128 , x2=232 , x3= 56 , x4=49.

m1=x1+x2 ; m1= 128+56=184

m2=x1-x2 ; m2= 128 -56= 72

m3=x2+x4 ; m3= 232+49=281

m4=x2-x4 ; m4= 232- 49=183

X1=m1+m3 ; X1=184+281 = 465

X2=m2-jm4 ; X2=72- 183j

X3=m1-m3 ; X3= 184-281 = -97

X4=m1+jm4 ; X4=184+183j

Now X1 and X3 have only real part but X2 and X4 have real and imaginary part. so we deal with these two parts (X2,X4) in order to calculate phase and amplitude values for both as follows:

X2=72- 183j

X4=184+183j

For **X2**:

Amplitude = 196.66 (as illustrate in Exp(2)).

Phase1 = 1.196 as illustrate in Exp(7)).

For **X4**:

Amplitude =259.509

Phase2 = 0.783

Now the system will add the watermark as a serial of bits like: **101101.** Adding this watermark will take this form :

Every 50 byte we choose 4 bytes for($N^2$)and 8 bytes for($N^3$)to add watermark as shown in fig(6)

Now the system will add the watermark to the phase to produce phase'. In this part we will add only two bits form watermark because we have only two values of phase as below:

Watermark **101101**

Phase1'=phase1+1 → =1.196+1=1.196

Phase2'=phase2+0 → =0.783+0=0.783

After adding the watermark to the phase we now recalculate the Im and Re as illustrate in Exp(4),(5)

Now we can recalculate the data of the WAV file by calculating the IFFT and make comparison between the main source and the resulting sound to extract the watermark (a serial of bits ).

**6- The proposal system evaluation**

We now compute the difference between the source sound and the watermarked sound to compare and test the ratio of errors between these sound .

First computing the mean squared error ( MSE ) of the reconstructed image as follows:[9]

$$MSE=\sum(\text{Original WAV-Watermark WAV})^2/N^2 \text{ - (7).}$$

The summation is over all bits. The root means squared error (RMSE) is the square root of MSE. PSNR is deciabels (dB) which is computed as bellow:

$$PSNR = 20 \log10 (255/MSE) \text{ --- (8)}$$

WAV files are used as cover for many types of data files such as text, image and audio file. The type of data files which are used in our proposed system is a serial of numbers (of 1‘s)

Fig (7) represents the original and the watermarked Wave files

Table(1) shown the result of PSNR when using $2^2$and $2^3$ .

When applying the PSNR to any watermarked wave file we see the result will be carved as illustrate in the fig.(8)&fig.(9).

**7. Conclusions**

The proposed system of Audio Watermark in WAV files yields the following findings:

1- Robustness: Watermarks are extracted successfully if the watermark is found and the redundancy of the watermark is useful to avoid the losses of the watermark when one or more of the watermarks are destroyed.

2- Transparency: Subjective tests have shown that most ordinary audience can’t distinguish the difference between the original WAV file and the watermarked WAV file

3- Security: The security was achieved when the watermark is ciphered before embedding operation and spread the watermark in the data of WAV file to give large measure of security against any attacks.

4- The proposed system save the watermark after compressing the WAV file because the watermark was added in different places in the data of WAV file and the watermark was added in a direct method to WAV file. All this makes the watermark able to avoid error when compression attacks are applied.

5- It is found that the user can save more information when FFT uses $2^3$ than using $2^2$ because the number of modified Phase Values in every time is more than that given in the second method .

6- It is found that when watermark is short then the result is better than when watermark is long in controlling the noise. So the results When block size ($2^2$) is better than when use block size ($2^3$) .

**8-Suggestions for Future Work**

1- Use the Watermark in WAV file in another type of audio files likes( MP3 ,au ,…etc).

2- Use the Watermark system in the same type of WAV file but with different attributes ( stereo and more than 8 sample resolution).

**References**

[1] Hany Farid ," Detecting Hiding Messages Using Higher-Order Statistical Models", Department of Computer Science Dartmouth College Hanover NH 03755,(2003). www.springerlink.com.

[2] G. Sahoo[1] and R. K. Tiwari[2] , " Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File , Hybridization", [1]Department of Computer Science &Engineering. , B.I.T., Mesra, Ranchi, Jharkhand, India, [2]Department of Computer Science &Engineering, R.V.S. College of Engg. & Tech., Jamshedpur, Jharkhand, India, (January2008).

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

[4] Stefan Katzenbeisser , " Information Hiding Techniques for Steganography and Digital Watermarking ", Artech House Boton –london (2000).

[5] Ross Anderson and Tyler Moore , " The Economics of Information Security" University of Cambridge, Computer Laboratory 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom. _This review originally appeared in Science 314 (5799), pp.610–613, October 27, 2006.

[6] Uma Devi.G , " Steganography-Survey on File Systems" , MS by Research – CSE I I I T Hyderabad, (19 October 2006).

[7] N. Provos, and P. Honeyman, "Hide and Seek:An Introduction to Steganography", IEEE Security and Privacy Magazine, 2003.

[8] Pierre Moulin," Fundamentals of Watermarking and Data Hiding", University of Illinois at Urbana{Champaign Dept of

Electrical and Computer Engineering (July 9 , 2006).

[9] Akeel A. Alhadithy, " Watermarking in WAV files Based on Phase Coding g " .Theses ,AL-Anbar university-College of Computer (2005).

[10] Nedeljko Cvejic, Tapio Seppnen , " Audio Prewhitening Based On Polynomal Filtering For Optimal Watermark Detection ", Team Information processing laboratory FIN-90014 University of Oulu, Finland Email: {cvejic, tapio.seppanen}@ee.oulu.fi

**Table (1) illustrate the PSNR result for $2^2$ and $2^3$**

| Musics | size | Iteration | PSNR $2^3$ | PSNR $2^2$ |
|---|---|---|---|---|
| Music1 | 507 KB | 2000 | 62 | 65 |
| | | 4000 | 64 | 67 |
| | | 8000 | 66 | 68 |
| | | 12000 | 66.6 | 69 |
| Music2 | 580 KB | 2000 | 65 | 65 |
| | | 4000 | 67 | 67 |
| | | 8000 | 69 | 69 |
| | | 12000 | 69.5 | 69.5 |

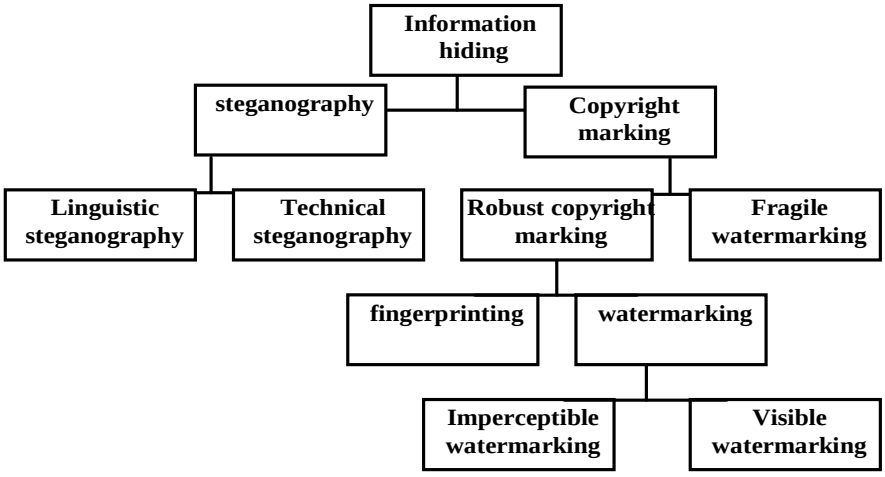


**Figure (1) The classification of information hiding**

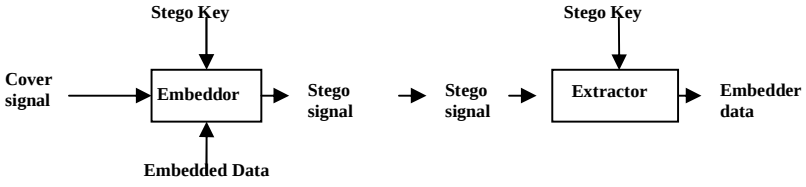


**Figure (2) Block diagram of data hiding and retrieval**

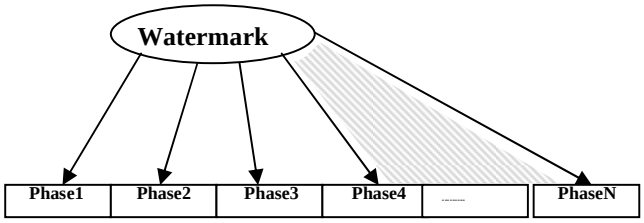


**Figure (3) Describe watermark embedding**

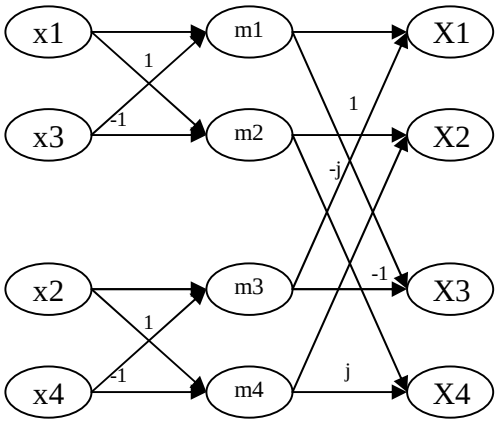


**Figure (4)Butterfly method when $N^2$**

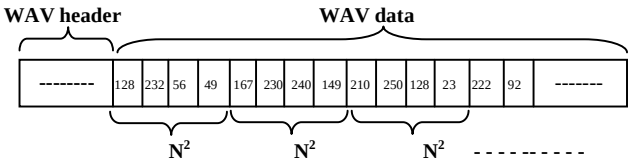


**Figure (5) Shown wav data divide to (4 bytes , $N^2$)**

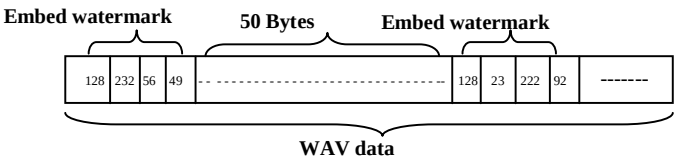


**Figure (6) shown watermark embed**

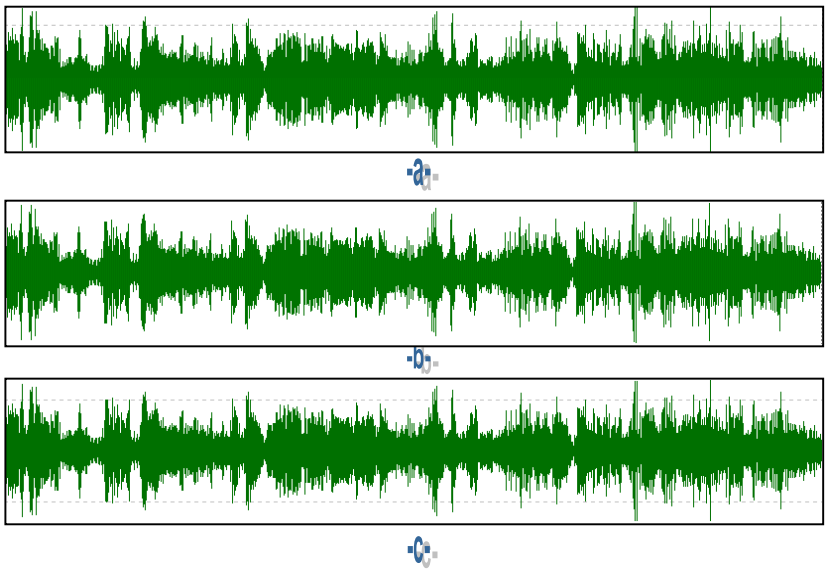

**Figure (7) –a- original WAV –b- Watermarked WAV when $2^3$–c- watermarked WAV when $2^2$**

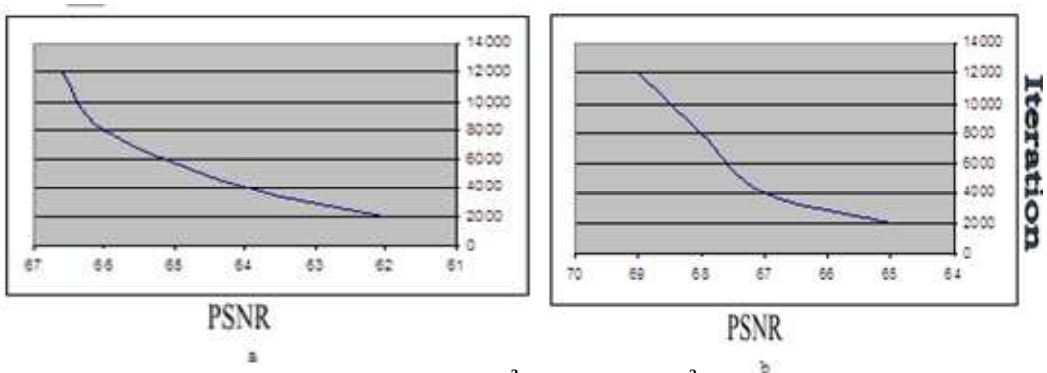


**Figure (8) Shown the PSNR curve -a- when $2^3$ and -b- when $2^2$ for Music1**

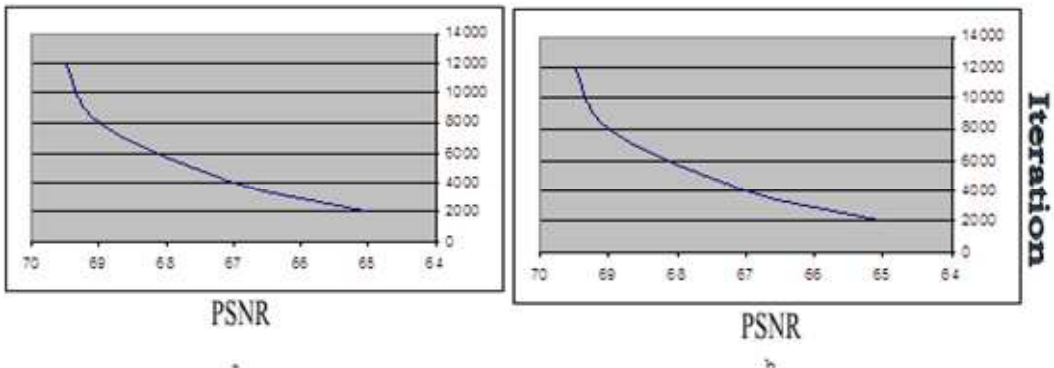


**Figure (9) Shown the PSNR curve -a- when $2^3$ and -b- when $2^2$ for Music2**