Digital Information Hiding Techniques

Alyaa Moufaq Abdul-Majeed — *Ass. Lecturer*
Nadia Maan Mohammed — *Ass. Lecturer*
Computer Science Department, College of Computers Sciences and Math.
University of Mosul

ABSTRACT

Information hiding, a form of watermark, embeds data into digital media for the purpose of identification and copyright. Several constraints affect this process: the size of data to be hidden, the need for robustness of these data under conditions where a host_signal is subject to distortions, for e.g., lossy_compression, and the degree to which the data must be immune to interception, modification, or removal by a third person.

Here, we explore two techniques (DC watermarking scheme and Time Domain watermarking technique) for addressing the data-hiding process and evaluate these techniques in light of the copyright protection application.

The measures (SNR, PSNR, NRMSE) were used to improve the results. Besides that the Matlab were used as a programming language in this paper.

تـقنيات إخفاء المعلومات الرقمية

علياء موفق عبد المجيد — **مدرس مساعد**
نـادية معن محمد — **مدرس مساعد**
قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل

المستخلص

إخفاء المعلومات، نموذج العلامة المائية الذي يقوم بطمر البيانـات داخل ملفات الوسـائط الرقميـة والذي يستخدم لغرض التعريف وتحديد الهوية والحفـاظ علـى حقوق الملكيـة، هنـاك عدد من الثوابـت التي تؤثر على هذه العملية: حجم البيانات المراد اخفائها، الحاجة الى مقاومة هذه البيانـات (الصلابة) تحت الظروف المختلفة للمتغيرات الخارجية، حيث تتعرض الاشارة الرئيسية الى تشويش دائم ومثال ذلك الكبس للبيانات بنوعية الفقدان، وكذلك الدرجة التي يجب ان تحملها البيانات لتكون درجة المناعة عالية ضد القطع، التغيير او الحذف من قبل شخص او جهة ثالثة.

في هذا البحث، تم تطبيق تقنيتي (العلامة المائية باسلوب DC و العلامة المائية باسلوب التحويـل الزمـاني) وذلك لغرض عنونـة عمليـة اخفـاء البيانـات ولاثبـات كفـاءة هذه التقنيـات فـي ضـوء تطبيـق حماية حقوق الملكية.

تـم اسـتخدام المقـاييس (SNR، PSNR، NRMSE) لغـرض اثبـات صـحة النتـائج وكفاءتهـا بالاضافة الى ذلك، تم اعتماد Matlab كلغة برمجية في هذا البحث.

1. Introduction

According to the spread of the internet, multimedia becomes treat digital contents, which can be copied easily without any loss in quality and contents. This poses a big problem for the protection of Intellectual Property (IP) rights of the copyright owners and the copyright of these digital media has become a lot of more difficult to manage. As a result, a technique called digital watermarking is introduced to protect the ownership of these contents. Digital watermarking can be realized by many different methods. In common to all of those methods, digital watermarking is a technique of embedding a digital signal or pattern on a digital document. The digital document may be text, audio, image or video. When the digital document is in the form of an audio signal, the embedding technique is called audio watermarking. [1][2]

The digital media that carries the watermark is called a **cover** signal or host signal. The watermark is embedded into the host signal by a watermark embedder and is detected by a watermark detector. A watermark key prevents unauthorized watermark embedding and watermark detection. [3]

Data hiding in audio signals is especially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thousand to one. While the HAS has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out quiet sounds. Additionally, the HAS is unable to perceive absolute phase, only relative ignored by the listener in most cases. [4][5]

2. Audio Watermarking Goals

Audio watermarking is implemented to satisfy four goals: [6]

a. The original intention of watermarking is for copyright protection. Therefore, the most obvious purposes are the needs for proof of ownership and the enforcement of usage policy.
b. Maximizing the difficulty of removing the watermark without destroying the audio.
c. Minimizing the perceptual effect of the watermark.
d. Maximizing the information, which can be encoded per second of original audio.

3. Types of Watermarking

Three types of watermarking system can be classified by the information required in the watermark extraction process: [4][7]

- **Private Watermarking**

  Private watermarking is also called none blind watermarking system requires at least the original data, and watermarks are needed to verify the presence of a watermark. A secret key used in embedding may also be needed.

  It can be used as authentication and content integrity mechanisms in a variety of ways. It may contain information for identifying the license or to prove ownership in disputes.

- **Semiprivate Watermarking**

  Semi-private watermarking is also called semi-blind watermarking. The original secret key and watermark are needed in order to identify a watermark. In applications such as Digital Versatile Disc (DVD) where the disc reader needs to know whether it is allowed to play the content or not, and fingerprinting where the goal is to identify the original recipient of pirated copies.

- **Public Watermarking**

  Public watermarking is also called blind watermarking. The original signal is not required. Only requires the secret key used in embedding for a watermark to be extracted. These public watermarks should not detectable or removable by a third party. It usually contains copyright or licensing information, such as the identifier of the copyright holder, the creator of the material. The receiver (licensee) of copyrighted material retrieves a public watermark.

  Although public watermarking is not secure it is much more difficult to remove than a visible label. Moreover, the failure of detection of the public watermark indicates that the image has been significantly tampered with and the user can be informed of the alteration.

4. Digital Audio Watermarking

Watermarking digital media has received a great interest in the literature and research community. Most watermarking schemes focus on image and video watermarking. A few audio watermarking techniques have been reported. Digital audio watermarking is the process of embedding a watermark signal into audio signal. Audio watermarking is a difficult process because of the sensitivity of Human Auditory System (HAS). The requirements mentioned earlier are common to both image and audio watermarking techniques. Despite their similarities, audio and still image watermarking systems exhibit significant differences. First of all, the fact that images are two-dimensional signals provide attackers with more ways of introducing distortions that might affect watermark integrity e.g. scaling, rotation or removal of rows/columns. Audio watermarking methods need not to deal with such attacks, as audio is a one-dimensional signal. Due to the difference between HAS and Human Visual System (HVS), different masking principles should taken into account in each case. Digital audio watermarking techniques can be classified according to the domain where the watermarking takes place. The following sections will discuss audio watermarking techniques and classify them to four categories: [3]

A) Frequency Domain Audio Watermarking

Audio watermarking techniques, that work in frequency domain, take the advantage of audio masking characteristics of HAS to embed an inaudible watermark signal in digital audio. Transforming audio signal from time domain to frequency domain enables watermarking system to embed the watermark into perceptually significant components. This will provide the system with a high level of robustness, because of that any attempt to remove the watermark will result in introducing a serious distortion in original audio signal fidelity. The input signal is first transformed to frequency domain where the watermark is embedded, the resulting signal then goes through inverse frequency transform to get the watermarked signal as output. See Figure (1). [7][8]

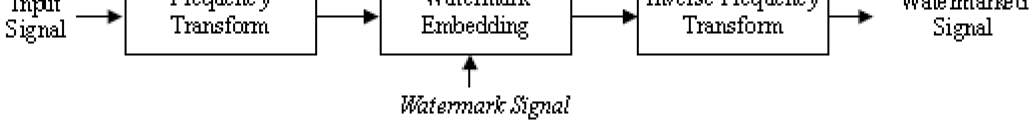

Figure 1

Watermarking in Frequency Domain

B) Time Domain Audio Watermarking

In time domain watermarking techniques, watermark is directly embedded into audio signal. No domain transform is required in this process. Watermark signal is shaped before embedding operation to ensure its inaudibility. The available time domain watermarking techniques insert the watermark into audio signal by simply adding the watermark to the signal. Embedding a watermark into time domain involves challenges related to fidelity and robustness. Shaping the watermark before embedding enables the system to maintain the original audio signal fidelity and renders the watermark inaudible. As for robustness, time domain watermarking systems use different techniques to improve the robustness of the watermark. See Figure (2).

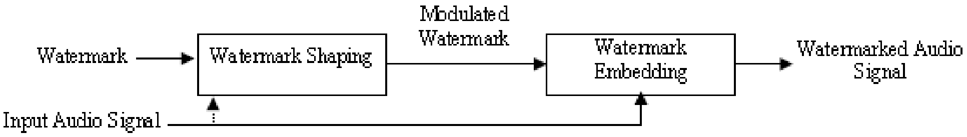

Figure 2
Time Domain Watermarking

5. Related Works

In (2001), Umut Uludag and Dr. Levent M. Arslan executed the audio watermarking using DC level shifting which gave a simple results.[8] In (2003), Dackson Lam & et.al., presented an investigation for an audio watermarking techniques, then they examine and compared 4 audio watermarking methods and recorded the results for the feature use.[2] In the same year, Mikdam A.T. Al-Salami and Marwan M. Al-Akaidi gave a survey that focusing on describing digital audio watermarking techniques.[7] While in (2008), T.C. Thanuja & Dr. R. Nagaraj showed a performance evaluation of popular audio watermarking schemes in prevalence today.[1]

Also, Saberian, M. J., and et.al. in (2009) introduced a new class of invertible watermarking approach based on quantization, that based on the necessary conditions (blindness, reversibility and imperceptibility).[9]

Essaouabi1, A., and et.al., in (2009), proposes a watermarking scheme that can embed a watermark to an arbitrarily shaped object in an image. The DWT and the (LSB) techniques were used.[10]

Another paper by Singh, A. P., and Mishra, A., (2009), showed a robust watermarking technique based on DWT, insertion and extraction of the watermark in the grayscale image is found to be simpler than other transform techniques.[11]

6. DC Watermarking Scheme

This section details the implementation of a digital audio watermarking scheme, which can be used to hide auxiliary information within a sound file. The DC watermarking scheme hides watermark data in lower frequency components of the audio signal, which are below the perceptual threshold of the human auditory system. [8]

In DC Level Shifting, the watermark is embedded by shifting the DC level of the audio signal:

a. Input signal is divided into frames of fixed length.
b. Compute the DFT for each frame X(n). The first element of this vector represents the DC component of the frame DC(i).
c. Compute the mean and power for each frame as:
   Frame mean = (1/N) DC(i) ………………………..… (1)
   Frame power = (1/N) [DC(i)] * 2 ………..………………... (2)
   Where N represents the number of samples in each frame.
d. Watermark signal is represented by binary number w(i).
e. Embed the w(i) by the following :

```
For i=1 to length(w)
    If w(i)=0 then
        U(k)= - DCBias Multiplier * (Frame Power) ……. (3)
    Else
        U(k)= +DCBias Multiplier * (Frame Power) ……. (4)
    End
End
```

   Where k represent the (index of frame).
f. Compute the Inverse Discrete Fourier Transform (IDFT) of the frame to obtain to the modified frame.

These steps are performed until all the watermark bits are encoded.[1][8]

7. Transform Domain Techniques [1][2]

In this method, the watermarking is embedded in a Transform domain:

a. Divide the input signal into blocks(frames).
b. Used random number generator to choice the block.

c. Compute the DCT of the frame. Let v(i) represent the DCT coefficients.
d. Compute the largest value in block.
e. Modify this value as:

$$v_1 (i) = v(i) (1 + \alpha w (i)) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(5)}$$

Where, ‘α’ is a scaling factor. Here, the value of α=0.2 .
w (i) is the watermark bit (0 or 1).

f. Compute the Inverse Discrete Cosine Transform (IDCT).

8. Result of DC Method using Symphony

The implementation of the DC method was tested on the symphony signal of size 1.21 MB with sampling rate 8 KH_Z and resolution of 8 bits/sample, and the watermark is a speech signal of size 10.63 KB of sampling rate 8 KH_Z and resolution of 8 bits/sample. Figures (3)(4)(5)(6) show a sample of watermark message that to be hidden inside original message before and after applying watermarking algorithm.

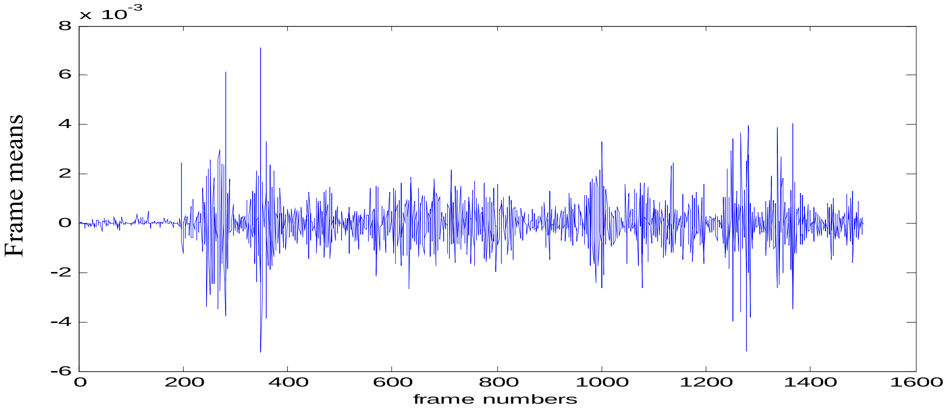

Figure (3) The frame means of original signal

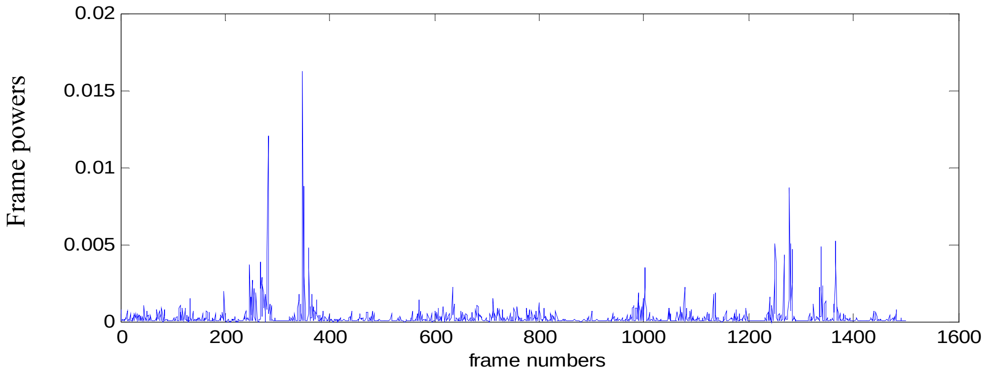

Figure (4) The frame power of original signal

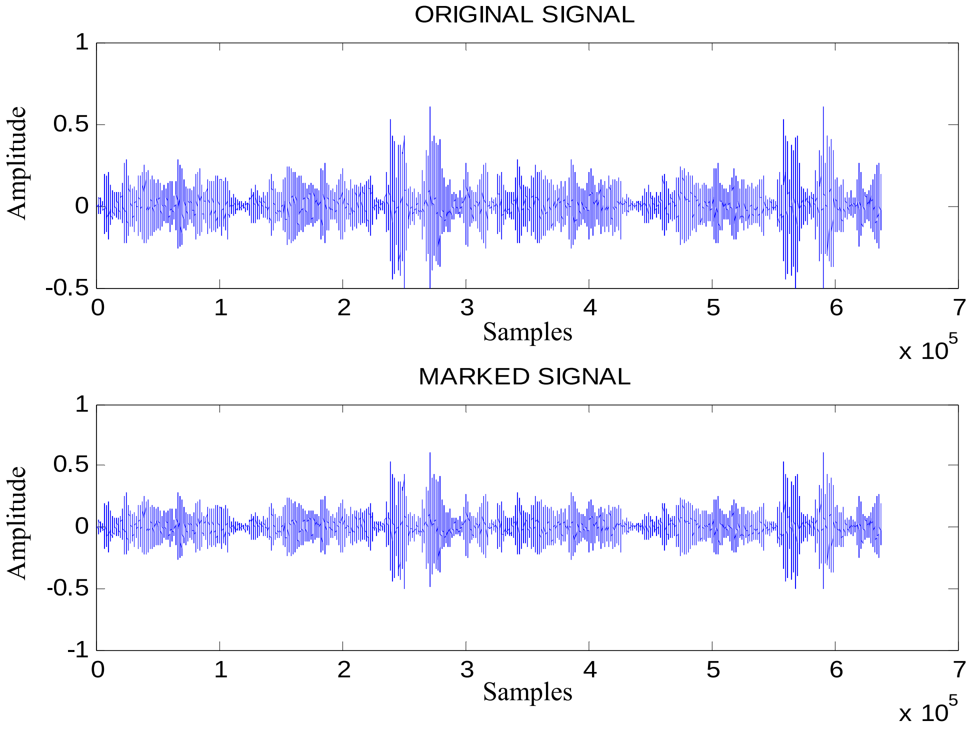

Figure (5) The original signal and the marked (watermarking) signal

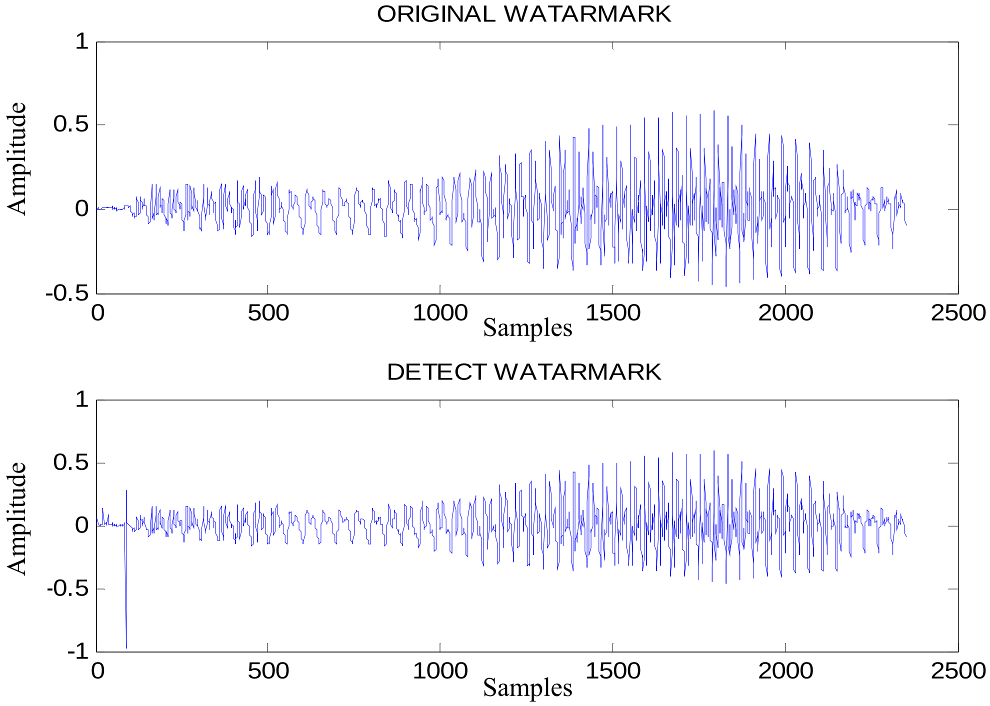

Figure (6) The watermarking signal and the retrieved watermarking signal

9. Results of DCT Method using Symphony

The implementation of the DCT method was tested on the symphony signal of size 1.21 MB with sampling rate 8 KH_Z and resolution of 8 bits/sample, the watermark is a speech signal of size 10.63 KB of sampling rate 8 KH_Z and resolution of 8 bits/sample. Figures (7)(8) show a sample of watermark message that to be hidden inside original message before and after applying watermarking algorithm.

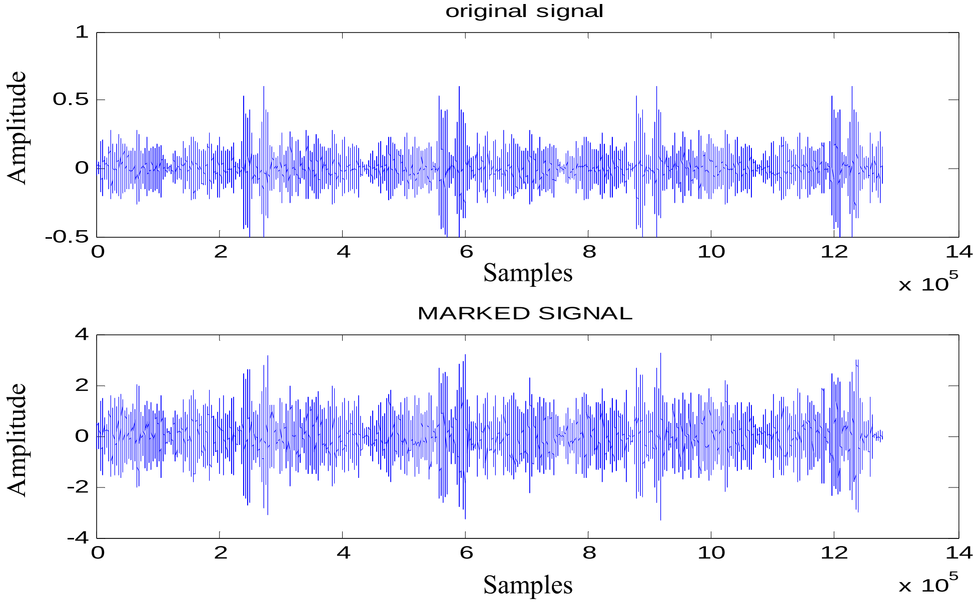

Figure (7) The original signal and marked (watermarking) signal

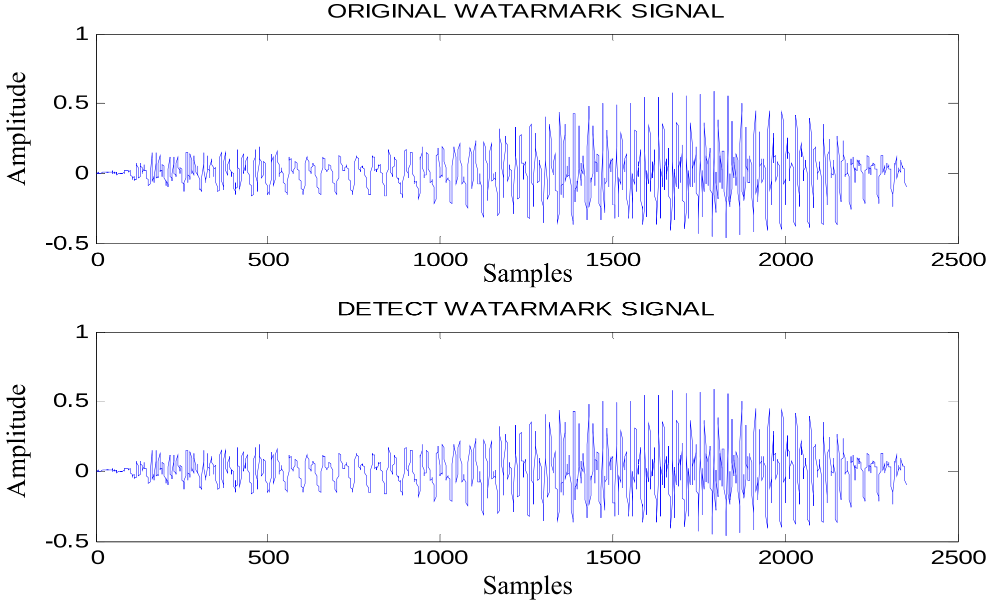

Figure (8) The watermarking signal and the retrieved watermarking signal

10. Results of DC Method using Speech

The implementation of the DC method was tested on the speech signal of size 493 KB with sampling rate 8 KH_Z and resolution of 8 bits/sample. The watermark is speech signal of size 10.63 KB with sampling rate 8 KH_Z and resolution of 8 bits/sample. Figures (9)(10) show a sample of watermark message that's hide inside original message before and after applying watermarking algorithm.

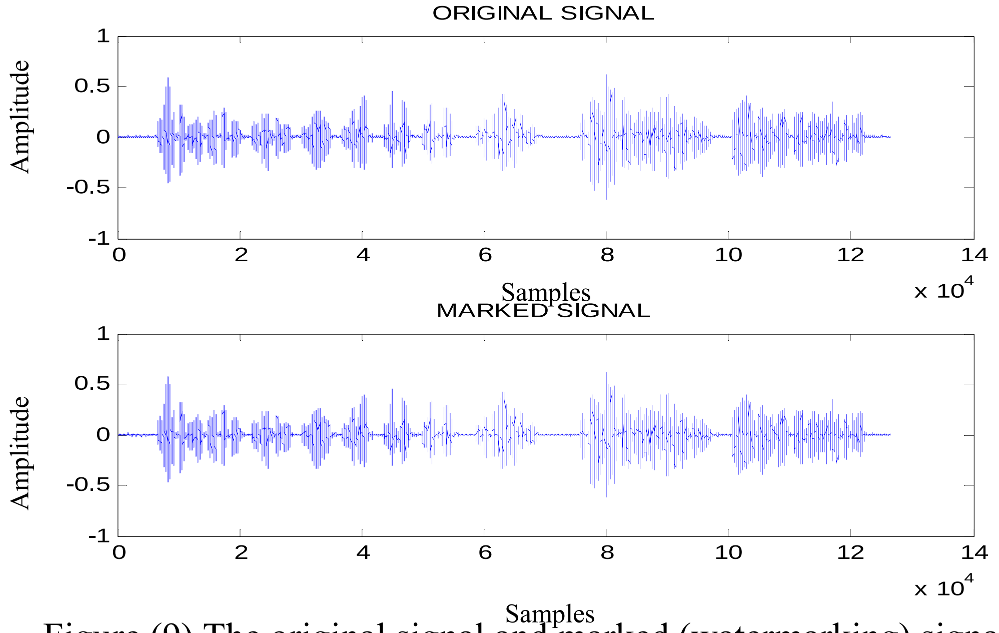

Figure (9) The original signal and marked (watermarking) signal

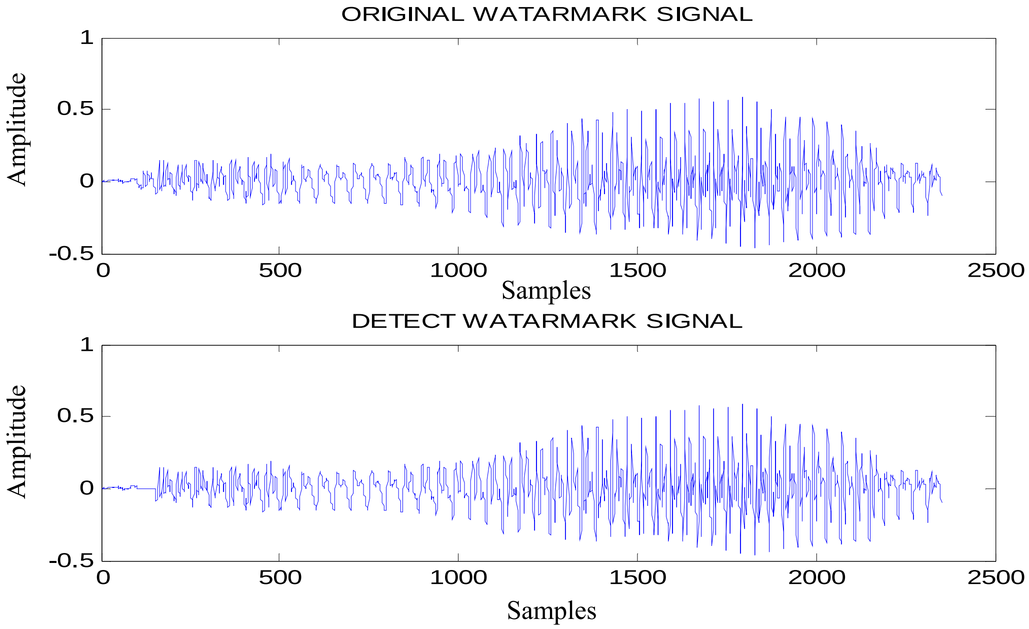

Figure (10) The watermarking signal and the retrieved watermarking signal

11. Results of DCT Method using Speech

The implementation of the DCT method was tested on the speech signal of size 493 KB with sampling rate 8 KH_Z and resolution of 8 bits/sample. The watermark is speech signal of size 10.63 KB with sampling rate 8 KH_Z and resolution of 8 bits/sample. Figures (11)(12) show a sample of watermark message that to be hidden inside original message before and after applying watermarking algorithm.

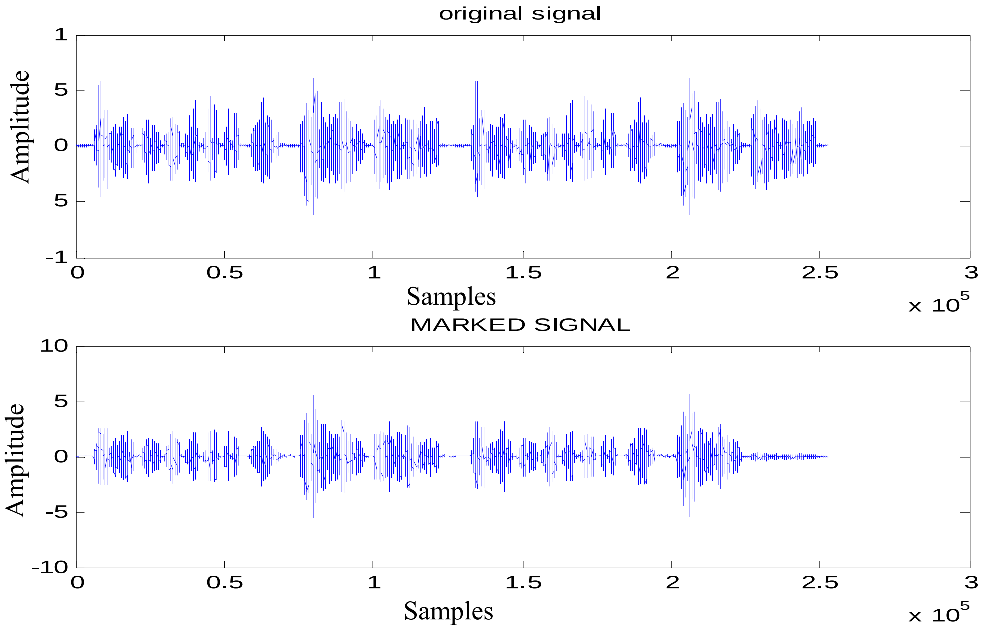

Figure (11) The original signal and marked (watermarking) signal

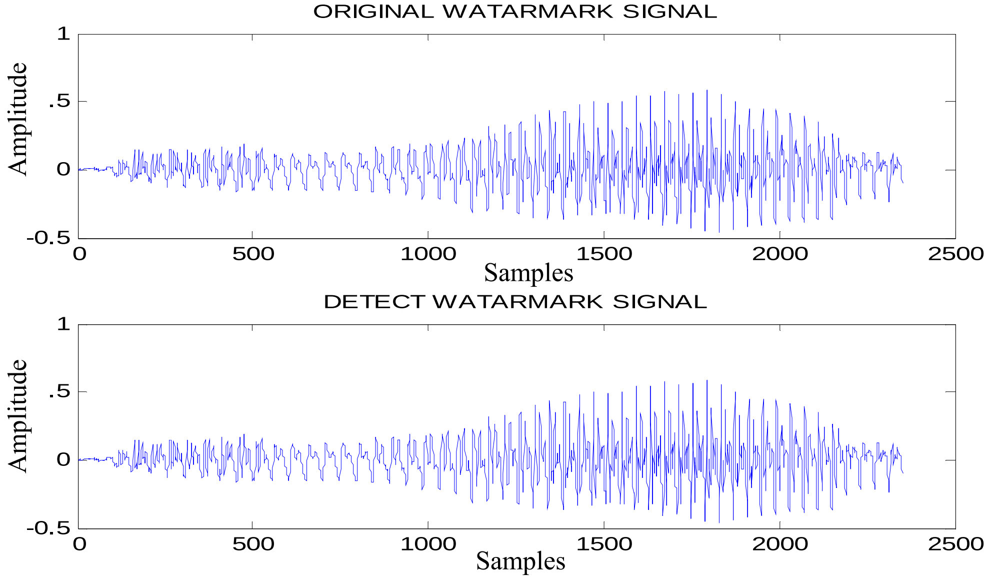

Figure (12) The watermarking signal and the retrieved watermarking signal

12. Summary

After applying the (DC and DCT) methods, a summary can be given for the last results using the following performance measures (SNR, PSNR, NRMSE) as shown in Table (1).

Table (1) Results of applying the performance measures

Type of Signal	Method	Performance Measures		
		SNR	PSNR	NRMSE
Signal1 (symphony)	**DC**	55.4229	61.5409	0.0053
Signal1 (symphony)	**DCT**	21.2506	17.8921	4.2302
Signal2 (speech)	**DC**	29.2226	33.9736	0.0948
Signal2 (speech)	**DCT**	19.7124	12.3249	3.1256

13. Conclusions

a. After executing the 2 above methods (DC, DCT), it concluded that the DC method is better and has a good performance than the DCT method for embedding the watermark data of type (speech) in both types of signal (Symphony, Speech), as it's clear from table (1).

b. Some audio watermarking systems require the original audio signal, or any information derived from it, to be presented in detection process. This will leads to a large number of original works have to be stored and searched during detection. Here, the applied methods don't required the original signal to detect the watermarked signal.

c. The methods mentioned in this paper are very useful to hide data of type sound signals.

d. The measures (SNR, PSNR) well be increase in each time the frame size is increased, but they well be decreased in each time the size of hidden data is increased. So, it's important to choose the suitable size of frame and the data to be hide.

14. References

[1] Thanuja T. C., and Dr. Nagaraj R., (2008), "Schemes for Evaluating Signal Processing Properties of Audio Watermarking", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July.

[2] Lam D., et. al., (2003), "Audio Watermarking", Electronic and Electrical Engineering, COMPSYS401A Project, University of Auckland.

[3] Al-Haj A. and Mohammad A., (2010), "Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition", European Journal of Scientific Research, ISSN 1450-216X Vol.39 No.1, pp.6-21.

[4] Cvejic N., (2004), "Algorithms For Audio Watermarking And Steganography", Faculty of Technology, University of Oulu.

[5] Verma H., et. al., (2009), "Random Sample Audio Watermarking Algorithm for Compressed Wave Files", International Journal of Computer Science and Network Security, VOL.9 No.11, November.

[6] Dhar, P. K., et. al., (2010), "A New Audio Watermarking System using Discrete Fourier Transform for Copyright Protection", International Journal of Computer Science and Network Security, VOL.10 No.6, June.

[7] Al-Salami M. A. T., and Al-Akaidi M. M., (2003), "Digital Audio Watermarking: Survey", School of Engineering and Technology, De Montfort University, UK.

[8] Uludag U., and Dr. Arslan L. M., (2001), "Audio Watermarking Using DC Level Shifting", Electrical & Electronics Engineering Department, Bogazici University, Istanbul, Turkey.

[9] Saberian, M. J., et. al., (2009), "An Invertible Quantization Based Watermarking Approach", ICASSP of IEEE.

[10] Essaouabi1, A., et. al., (2009), " Digital Image Watermarking for Arbitrarily Shaped Objects Based On SA-DWT", IJCSI International Journal of Computer Science Issues, Vol. 5.

[11] Singh, A. P., and Mishra, A., (2009), " Wavelet Based Watermarking On Digital Image", Indian Journal of Computer Science and Engineering, Vol. 1, No. 2, pp86-91.