Variant length, Self-extracted audio watermark for verification using LWT and random selections

Hala Bhjet Abdul Wahab[*], Abdul-Mohssen Jaber Abdul-Hossen[*] and Sana Ahmed Kadhom[**]

[*]Department of Computers – University of Technology – Baghdad, Iraq
[**]Department of Computer Science – Al Mammon University College – Baghdad – Iraq

Received 17 September 2016 ; Accepted 21 December 2016

Abstract

In the last decade with the expansion of cyber multimedia activities, concepts like authentication, identification and verification became a must. Audio is one of the challenging media in cyber security for its complicated nature. Watermarking rises as an important methods used in securing audio files and other media. In this research a new method is used for extracting the signal features from random positions in the original audio signals by some signal calculations in time domain and hide them within the same audio in other positions after transforming the samples in these positions using lift wavelet transform, all positions were chosen depending on random walk method and a secret key. The extracted features will be compared with the hidden features (watermark) for verification. The proposed method was tested against compression (mp3) and noise addition (White Gaussian noise). Many types of performance measurements like peak signal to noise ratio, bit error rat, mean square error and others were used to measure the efficiency of the proposed method.

Keywords: LWT, Feature extraction, audio, watermark, authentication, random walk.

Variant length, Self-extracted audio watermark for verification using LWT and random selections

Hala Bhjet Abdul Wahab, Abdul-Mohssen Jaber Abdul-Hossen And Sana Ahmed Kadhom

التوليد الذاتي لعلامة مائية ذات طول متغير لاغراض التوثيق باستخدام محول LWT وطريقة الاختيار العشوائي

هالة بهجت عبدالوهاب* ، عبدالمحسن جابر عبدالحسين* و سناء احمد كاظم**

*قسم علوم الحاسوب – الجامعة التكنولوجية – بغداد – العراق.
**قسم علوم الحاسوب – كلية المأمون الجامعة – بغداد – العراق.

الخلاصة

في العقود الماضية ومع التطور السريع لاستخدام الوسائط المتعددة في شبكات السايبر، المفاهيم كالموثوقية، التمييز والتعرف الالكتروني اصبحت ضرورة. الصوت هو احد الوسائط المستخدمة في السايبر والذي يعتبر الاكثر تحديا لطبيعته المعقدة. العلامة المائية تعتبر من الطرق المهمة المستخدمة لحماية الملفات الصوتية عبر الشبكة. في هذا البحث طريقة جديدة لتوليد علامة مائية من اماكن معينة ضمن الملف الصوتي باستخراج خواص الاشارة الصوتية في هذه الاماكن وبطرق رياضية ومن ثم اخفاءها في اماكن اخرى ضمن نفس الملف الصوتي وبعد تحويلها باستخدام LWT ، جميع المواقع المستخدمة في استخراج العلامة واخفاءها يتم ايجادها من خلال مفتاح سري واحد وطرق المسير العشوائية. العلامة المستخرجة من قبل المستلم يتم مقارنتها مع العلامة المحسوبة ليتم التاكد من صحة الملف الصوتي. تم فحص الطريقة المقترحة بعد المهاجمة بطريقة الضغط MP3 وطريقة اضافة الضوضاء. تم قياس كفاءة الطريقة المقترحة بواسطة معاملات الكفاءة مثل PSNR, BERوغيرها.

الكلمات المفتاحية: محول LWT، استخراج الخواص، الصوت، العلامة المائية، الموثوقية، الحركة العشوائية.

Introduction

Digital data such as video, audio, image and text, became very important with the expansion and development of Internet. Thus, the problem of securing multimedia data has a priority importance in security field. Digital Watermarking is one of the most affected solution to that problem. Watermarking is a process of hiding some critical information within the original file without corrupting the data. The data could be audio signals, images or video. The watermark

should be easily and correctly extracted by the authorized receiver and in the same time should be difficult to be detected by attackers. Any type of data could be used as a watermark (audio, image,…) Since the watermark is hidden in the original file, it could be used for many purposes like authentication, verification, identification and recognition.[1] A lot of watermarking methods use the original audio data (samples in time domain) to hide the watermark which cause the watermark to be fragile and easy attacked and detected. Therefore, all new researches went toward hiding watermark in a transformed representation of the audio data. Transformers like DCT, FFT, SFFT, WLT, DWT and others were used. By using transformers, watermark is distributed in a large spectrum (SS) which makes the watermark immune against many types of attacks. The wavelet methods calculate differences and averages of audio signal, breaking down the signal into spectrum. Wavelet transform gave two groups of values: a group of averages and a group of differences (the second group is called wavelet coefficients). The size of the averages group and the coefficients group is half the size of the original data. For example, if the time series contains 512 samples, the first and second group will be of size 256 each. Most transformers use data of power 2, the spectrum results from a wavelet process reflect the modification in the time series with different resolutions. The first coefficient reflects the largest change in frequency. All later coefficients reflect modifications at lower frequencies.[2] In lifting transform, the wavelet finds the difference between the predicted values and an original values.

Let the data be: S_n, S_{n+1}, S_{n+2},…. , then Haar wavelet will be calculated as shown in eq.(1):

$$Cn = \frac{S_n - S_{n+1}}{2} \qquad \ldots\ldots\ldots(1)$$

Where Cn is the wavelet coefficient.

The LWT uses a different calculation which is close to Haar as in eq.(2)

$$Cn = ODDn - EVENn \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

The LWT is a wavelet algorithms which has excellent reconstruction and the best multi-scale resolution.[3] In ths paper, we focus on audio signals such as music records. Audio watermarking is the process of hiding special data (such as features, names, images, etc.) into the original audio without affecting it.[4] A successful and practical watermark scheme should satisfy some important issues such as robustness, imperceptibility, security and great embedding capacity. Blind watermarking methods, which are able to extract the watermark without having the original audio signal are more practical and desired in cyber security.[5]
The proposed method combines many concepts like LWT, random walk, variant length watermark, and blind extraction method, to present a new powerful, practical, light, and immune watermarking strategy.

The Proposed method

The proposed method is composed of many parts: (position selection, feature extraction, watermark hiding) for sender side, and (position selection, feature extraction, watermark extraction and comparison) for receiver side. Each part will be explained in details.

2-1 Sender:

2-1-1 Position Selection:

This is the first step in the process of watermarking. Locations to extract the features shouldn't be fixed or pre-determined, they must be variant with each new audio file to prevent predicting attack. The variations come not only from the random walk(RW) function, but also from using different keys (initial value for the RW function) in each time. Random walk function is used to produce random numbers which are used as positions of frames to extract features or hide watermark;

Algorithm (1): Position selection

Input: Audio data, secrete key K and number of watermarks N.

Output: Array1 (positions of frames for extracting features);

Array2 (positions of frames for hiding watermark);

Steps:

1- Begin
2- Find the size of audio file (M);
3- Using K as initial position

Array1(1) = K

4- Find other positions for feature extraction frames using random walk function as in eq.(3).

$$Array1(X_{n+1}) = (Array1(X_n) + B) mod\ M \quad \ldots\ldots\ldots\ldots\ldots (3),$$

Where B is the frame size and n=1,2,…N.

5- Use the last position found as initial value for Array2 by multiplying it by K (to make a jump):

Array2(1) = Array1(N) * K.

6- Find the positions of watermark hiding frames using eq(4).

$$Array2(X_{n+1}) = (Array2(X_n) + D) mod\ M \quad \ldots\ldots\ldots\ldots\ldots (4),$$

Where D is the frame size and n=1,2,3…N.

7- End.

By algorithm (1), the positions of feature extraction frames were determined (frames size is 256 samples) and the positions of hiding frames were also determined (frames size is variant depends on the size of extracted features).

2-1-2- Feature Extraction:

Audio signals have special nature in construction, so, each chosen frame will be examined to find the special features representing it.

Algorithm(2): Features extraction

1- Begin
2- For each position in Array1, read a frame of size(256 sample);
3- For each frame, find all positive waves and negative waves;
4- For each wave find the start point, number of samples representing it, maximum value(peak), and the position of peak; consider these values as the frame features.
5- Create watermark array, such that:

Watermark = All features of the frame

6- End

Each frame will have its own feature matrix that differs from all other frames. The whole feature matrices will represent the characteristics of the audio file which could be used for verification of the audio or even for identification if the audio file is a personal voice.

2-1-3- Feature Hiding:

After extracting the watermark from some random selected blocks(frames), they will be hidden in other random selected blocks. Hiding process is more complicated than the extraction process, since the hidden data should not affect the sound and should not be perceptible or predictable by attackers.

Algorithm (3): Watermark hiding

1- Start
2- Convert each watermark to one dimensional binary vector. (Note: each WM has different length).

3- For each hiding frame (of size = WM), Convert using lift wavelet transform (type Haar);
4- Take only the coefficient vector of LWT and convert to binary.
5- Replace the least significant bit LSB with one bit of the watermark binary vector.
6- Apply inverse transform (ILWT);
7- Return the sound frame to its original place in the sound file;
8- End

By the end of algorithm(3), a watermarked sound file was created and ready to be sent.

2-2 Receiver:

Since the proposed watermarking algorithm is blind, the receiver doesn't have the original audio file; only the watermarked file is received; he has to apply the same algorithms(1, 2, 3), using the same secret key.

By applying algorithm(1) and (2), the receiver extract the features and is ready to continue with the watermark extraction.

Algorithm(4) : Watermark extraction

1- Start
2- For all features extracted by algorithm(2) on watermarked received audio file, convert to one dimensional binary vector.
3- For each hiding frame (of size = WM), convert using lift wavelet transform. Take only the coefficient vector of LWT;
4- Convert these coefficients to binary;
5- Compare the LSB of each binary coefficient with the binary feature vector; if they are all equal, then the audio file is verified.
6- End

Implementation

The proposed method was applied on different audio files. The following implementation is executed on one audio file (type: mono, frequency: 11025 Hz, duration: 27sec). Five watermarks were hidden within that file; all watermarks were extracted from the same audio file from different frames; each watermark represents the features of one frame.

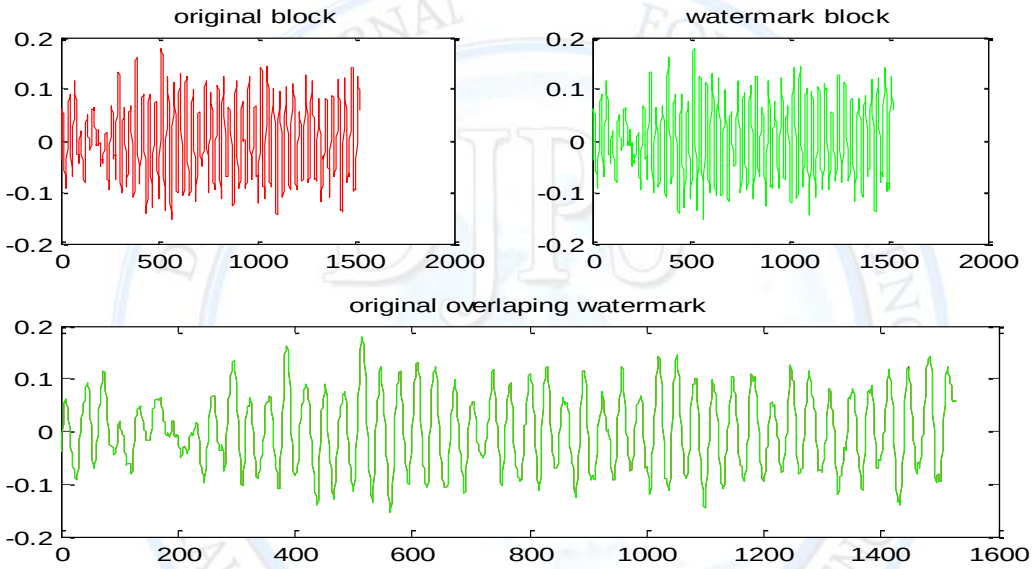

Figure 1: Frame 1(original, watermarked, overlapping)

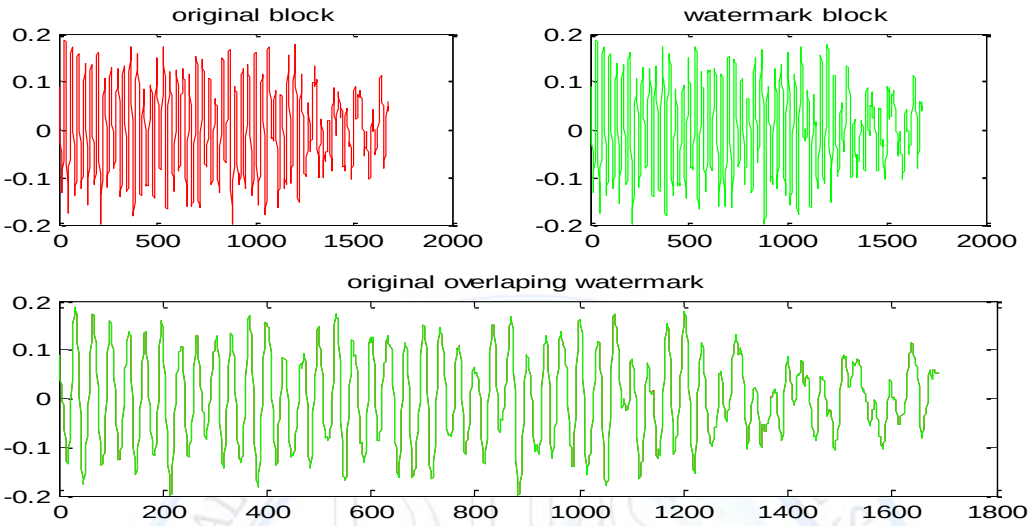

Figure 2: Frame2 (original, watermarked, overlapping)

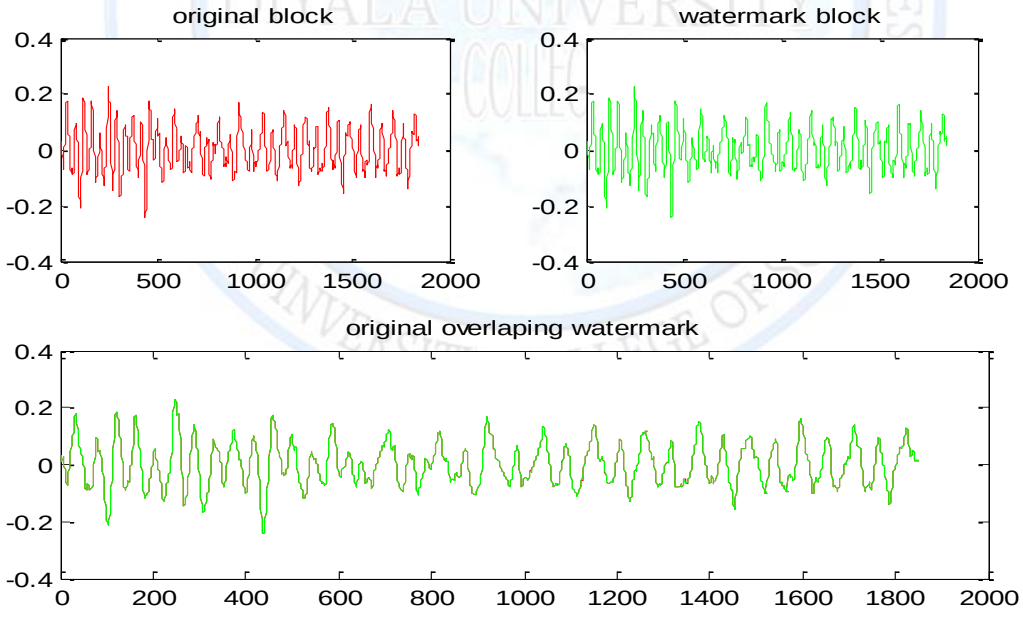

Figure 4: Frame3 (original, watermarked, overlapping)

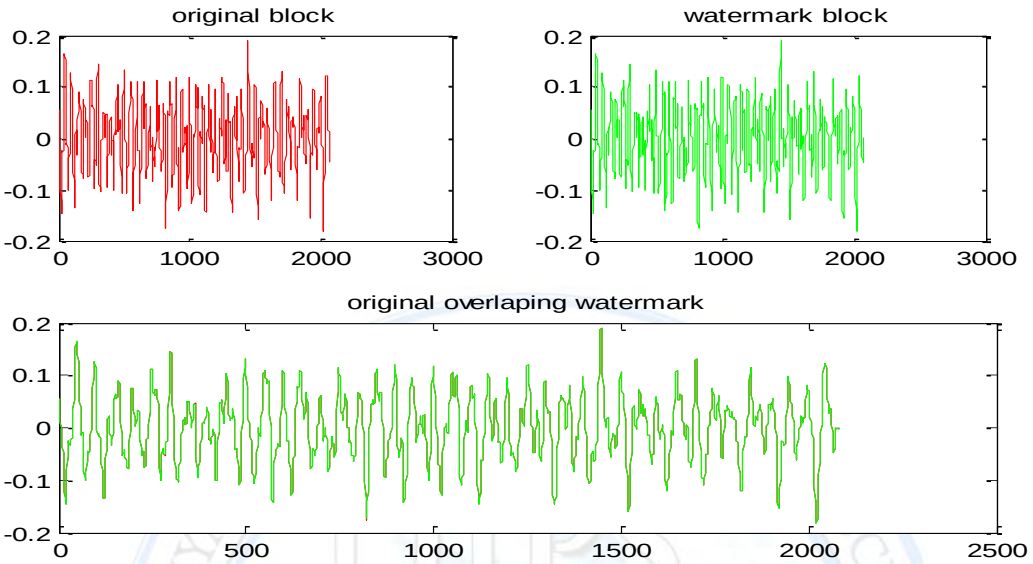

Figure 5: Frame4 (original, watermarked, overlapping)

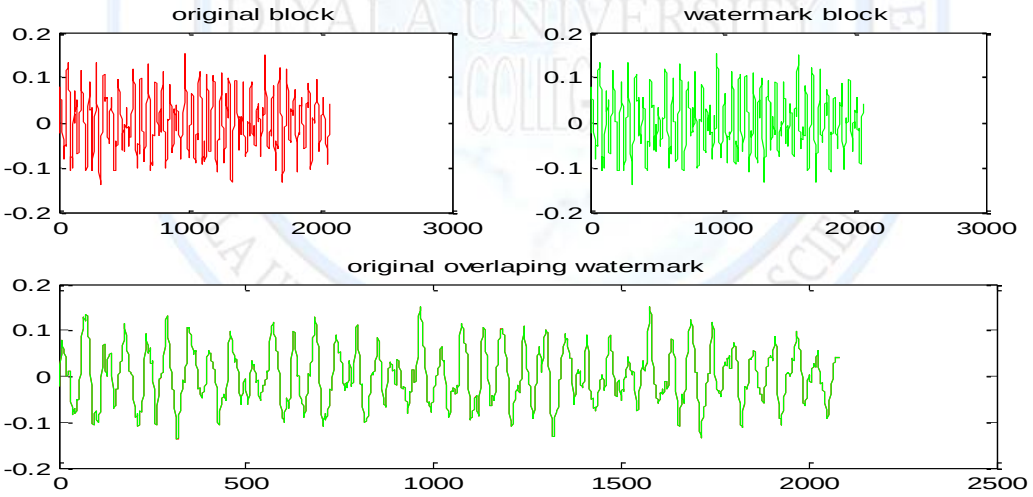

Figure 6: Frame5 (original, watermarked, overlapping)

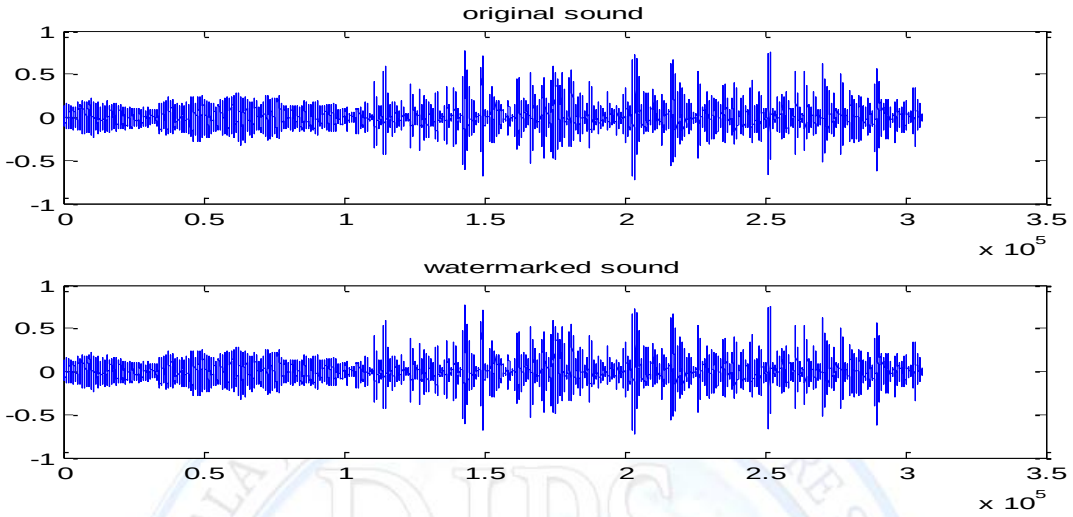

Figure 7: Audio Signal (original, watermarked)

In each figure (2:6), the third plot represents the overlapping between the original file and the watermarked file each with different color (red for original and green for watermarked). It is very clear that the differences between them were tiny so they only sometimes appeared like red dots on the green signal.

The watermarks data which extracted from the frames of each sound file (here 5 frames), were all differ from each other, that's why the proposed method could be used not only as a protection watermarking method but also as a method for verification, identification and even recognition for human voices. Figures (8:16) show the watermarks extracted from each audio file, the differences were clarified by plotting the watermark data.

Variant length, Self-extracted audio watermark for verification using LWT and random selections

Hala Bhjet Abdul Wahab, Abdul-Mohssen Jaber Abdul-Hossen And Sana Ahmed Kadhom

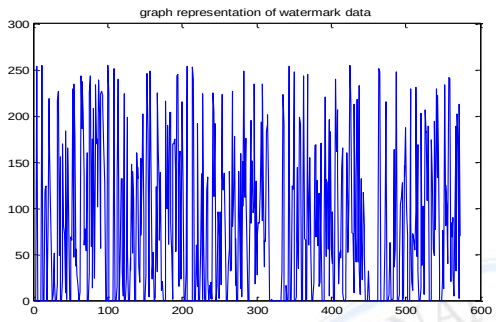

Figure 8: the plot representation of watermark data(sa.wav)

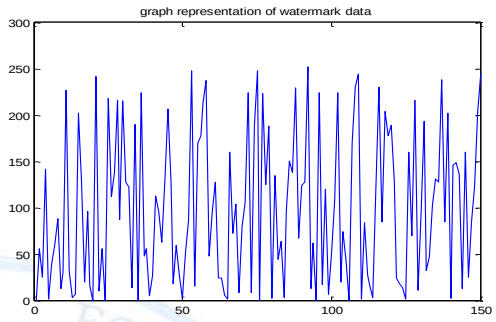

Figure 9: the plot representation of watermark data(w14.wav)

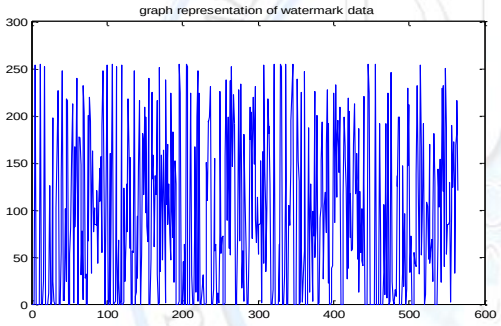

Figure 10: the plot representation of watermark data(w18.wav)

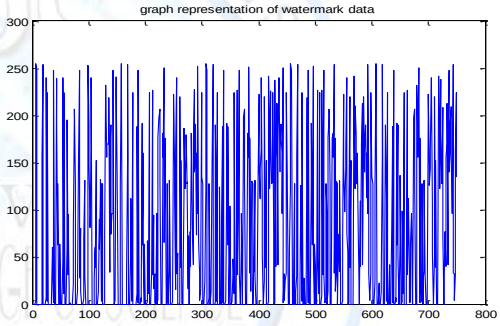

Figure 11: the plot representation of watermark data(w19.wav)

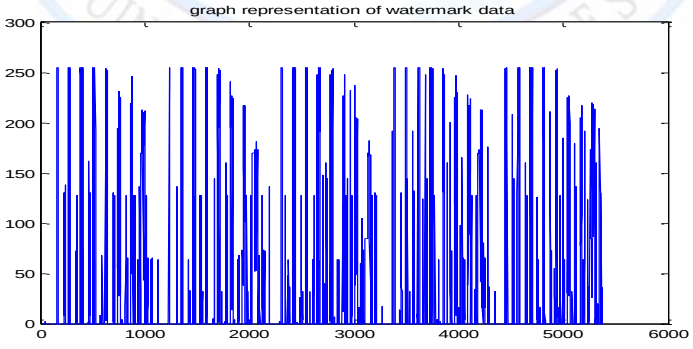

Figure 12: the plot representation of watermark data(Whitney.wav)

Results and Evaluation

I. The proposed algorithm was tested on audio files (mono and stereo), with different frequencies (11025 and 44100) and with different durations (11sec, 24sec, 40sec, 21sec and 27sec).

II. Performance evaluation shows excellent results as shown in table 1. the BER in all cases were less than 50% which means, whatever the size of the watermark file only less than half of its size will actually change the data of the audio file (0→1 , or 1 →. 0) which minimize the effect of the watermark.

III. The change in bits values in the audio files done on LSB of the coefficients of a transformer, which means, the change of one bit is distributed on many samples of audio (spread spectrum SS) and for that reason the watermark has neither perceptual nor predictable effect.

IV. The proposed method applied on audio files for cyber transmission, which means it has to be light and powerful. Applying LWT only on the frames where the watermark was hidden and not on all audio file makes the process fast and efficient.

V. The positions used for feature extraction and hiding changed with the secrete key which was used in random walk function to produce positions; therefore, the watermark could be extracted only by knowing the key otherwise, the watermark is secured.

VI. Using variant (length and value) watermark gave the algorithm more power and resistant against attack since it is difficult to predict the positions and the length of each watermark.

VII. The watermark is found from the audio itself which makes the algorithm really blind. The attacker has no pervious knowledge about the watermark. Also, the watermark describes the characteristics of the audio signal which is unique and could be used for verification, identification and recognition.

VIII. More than one watermark is hidden within each audio file (No. of WM), and that helps when part off the audio file is corrupted, the rest of the file may be checked.

IX. All tested audio files have been attacked by compression (mp3) and noise addition (White Gaussian noise), in all cases the watermarks were successfully extracted.

X. The SNR values for the tested audio files were all greater than 70% depending on the size of the watermark which itself depends on the nature of the signal.

Table 1: Performance evaluation for five audio files

File name (.wav)	File length (sample)	WaterM length (bit)	PSNR	MSE	BER %	SNR	WMSNR
W14 24 sec	1099640	1200	163.0684	3.208017e-012	49.25000	94.98814	0.00006718108
W18 21 sec	962808	4520	156.8201	1.352293e-011	49.95575	82.24048	0.0002931529
W19 11 sec	492920	6000	152.8444	3.377816e-011	49.08333	87.52201	0.0007468250
Whitney 40 sec	1779415	42975	153.8965	2.651114e-011	32.04188	73.031473	0.0009673123
Sa 27 sec	306146	4590	148.7757	8.619987e-011	49.34641	78.51876	0.0009248039

Conclusion

Cyber security is one of the most important concepts these days which made all the effort towards securing transmission and data. Audio files are most challenging media for its complicated and fragile nature. To secure audio files, a light and powerful method is needed. Also the method should have no perceptual or predictable effect on the original audio. The proposed method suggested a new feature extraction algorithm in which the audio signal within a specific frame was analyzed and mathematically calculated the features of that signal. The watermark is extracted from specific locations in the audio signal and hidden in other locations all these locations differ from file to file and that by using the secrete key as initial value to the random walk function which produces random locations. Using LWT made the watermark distributed on a large spectrum(SS) since each coefficient results from LWT came from many samples in the original signal, which makes the effect of hiding watermark unperceptual. The

proposed method was proved to be strong against compression and noise addition attack. The suggested method is blind since the original audio is not required in the extracting the watermark, the only data that should be available for extraction is the secret key.

References

1. Monika Patel, Priti Srinivas, Sajja Ravi, K. Sheth,, "*Analysis and Survey of Digital Watermarking Techniques"*, International Journal of Advanced Research in Computer Science and Software Engineering Research, Volume 3, Issue 10, October 2013.
2. Jensen and la Cour-Harbo , *"Ripples in Mathematics: the Discrete Wavelet Transform"*, 2001
3. Yves Nievergelt, Birkhauser, *"Wavelets Made Easy"*, 1999.
4. Yong Xiang, Yue Rong, "*Spread Spectrum Based High EmbeddingCapacity Watermarking Method for AudioSignals",* 2015.
5. N.K. Kalantari, M.A. Akhaee, S.M. Ahadi, and H. Amindavar, "*Robust multiplicative patchwork method for audio watermarking"*, IEEE Trans. Audio, Speech, and Language Process., vol. 17, no. 6, pp. 1133-1141, Aug. 2009.
6. Mohamed I. Mahmoud, Moawad I. M. Dessouky, Salah Deyab, and Fatma H. Elfouly, "*Comparison between Haar and Daubechies Wavelet Transformions on FPGA Technology"*, World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:1, No:2, 2007.
7. Rubinstein, R.Y.; Kroese, D.P., "Simulation and the Monte Carlo Method", 2007. (2nd ed.). Wiley. ISBN 978-0-470-17794-5.
8. A. H. Ali, M.R.Mokhtar and L.E. George, "A Review on Audio Steganography Techniques", Research Journal of Applied Sciences, Engineering and Technology, 2016, ISSN:2040-7459, Maxwell Scientific Publication Corp.
9. S.K. and B.G. Banik, Int. J.Emerg., "*Multilevel steganographic algorithm for audio steganography using LSB modification and parity encoding technique",* Trends Technol. Computer Science, (IJETTCS), 2012.