International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A novel DWT based Audio Watermarking adopting Fibonacci Numbers

K Krishna Mohan & K Udaya Kiran
[#1] PG scholar, Dept. Of Electronics and Communication, G.Pulla Reddy College of Engineering & Technology, Kurnool, Andhra Pradesh, India.
[#2] Assistant Professor, Dept. Of Electronics and Communication, G.Pulla Reddy College of Engineering & Technology, Kurnool, Andhra Pradesh, India.
scapeskrisha@gmail.com[1] UDAYAKIRAN_UK@REDIFFMAIL.COM[2]

Abstract

Audio watermarking is the process of embedding audio data in signal. Security is the main aim behind audio watermarking. Audio watermarking is the recent scope due to its reliability and high security depends on the data embedding technique as well as data extraction technique. In this paper we discussed about both embedding the data as well as extracting the data from watermark. The new in this technique is its type of embedding and extracting data in bit extract manner by changing the FFT spectrum magnitudes. The main theme in this implementation is FFT spectrum divided into small frames and we applied Fibonacci numbers to some selected number of FFT samples. By using Fibonacci series we can change the frequency samples. The advantages of using this system is it will provide the data which is having maximum change upto 61% and also the average error is less than 25%.This is very robust and transparent technique of watermarking. Experimental results shows that the proposed audio watermarking with Fibonacci series is having high capacity as well as it is having significant perceptual distortion and also shows its robustness against some audio signal processing attacks such as filtering, echo, added noise and MPEG compression (mp3). Finally we also proved the fidelity is also better for proposed work.

Keywords: watermarking, FFT spectrum, DWT

I. INTRODUCTION

Over the years, there has been tremendous growth in wireless networks. Watermarking has been around for a few decades, as watermarks discovered at first in plain paper and eventually in paper bills. Nevertheless the field of digital watermarking was just evolved among the most recent 15 years and it is presently being utilized for a wide range of uses. Advanced watermarking is a procedure by which a watermark is covered up or inserted into a media (cover information), for example, electronic records, pictures, sound also, video. The web is an important task in day today life. Knowledge transmission has been created very straightforward, quick and correct exploitation through the web. However, one in many of the issues related to transmission of knowledge over the web is that it may create a security threat, i.e., personal or confidential knowledge may be taken or hacked in some ways.

Nowadays hackers are very intelligent and can hack easily the government documents which are very important for some justice. Publishers and artists, hence, could also be reluctant to distribute knowledge over the web because of lack of security; proprietary material may be simply duplicated and distributed with not having the owner's consent. Therefore, it becomes important to give a thought to knowledge security, because it is one of the essential factors that require attention throughout the method of knowledge distribution. Watermarks are planned as the simplest way to tackle the robust issue. This digital signature might discourage copyright violation, and should facilitate and confirm the credibleness and possession of a picture [1]. Watermarking may be inserted in secret transmission of confidential messages, for e.g., military maps, while not the actual fact of such transmission being discovered. Watermarking, being ideally impalpable, may be basically incorporated to mask the existence of the key message, which is explained in [6].

Watermarking is employed to make a covert channel to transmit information steered with higher gain and security as given in [5]. Nowadays secure transmission of data is important. By embedding the watermarks into data we can provide security. Watermarking is an efficient way to protect the information from unauthorized or unwanted users viewing of the data. Watermarking is turning into more and more fashionable, particularly for insertion of undetectable distinguishing watermarks, like author or copyright information to the host signal. Watermarking might in all probability be best employed exertion with another data-hiding technique like steganography, cryptography etc. Watermarking is an idea nearly linked to steganography they both conceal a message inside a digital signal. Anyhow, what separates them is their objective, Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no connection to the message, and it is simply used as a cover to hide its existence. To resist on-line music piracy, a digital watermark might be handier, compelling the user has to purchase a legitimate copy of the data. Watermarking might be employed in voice conferencing systems to point the other party that is presently speaking. Audio watermarking is famous for durable and secure communication of knowledge associated with the host audio signal, which incorporates watermark that is embedded into, and extracted from, the host audio signal [4].

Thinking about embedding domain, watermarking can be carried out in both frequency and time domains. In time domain theme, the masked bits are inserted directly into the time signal intervals. These methods are not complicated to implement and are usually efficient but weak against some signal processing attacks. Whereas in frequency domain after applying the transform the secret bits are fixed in transform coefficients. Compare to time domain methods, frequency domain methods are strong against signal processing attacks.

In Ref [8] researcher mentioned that replacement framework for knowledge embedding in audio is projected. The essential plan of the algorithmic program is to vary the length of the intervals between salient points of the audio signal to insert knowledge which is used for further analysis. The interims are quantized and the information is inserted in the quantization lists. In our specific implementation, we have a tendency to use the rippling extrema of the signal envelope as the salient points. We have a tendency to propose novel ideas for sensible implementation that may be employed by alternative knowledge embedding schemes yet. The algorithmic program is powerful to common audio process operations, e.g., mp3 lossy compression, low pass filtering, rate conversion, and time-scale modification (TSM). The sensory activity quality of the audio signal when embedding the info depends on the technique used for TSM.

In Ref [9] mentioned concerning continuation to earlier work where the matter of time-scale modification (TSM) has been studied. Time-scale invariant audio watermarking supported the applied math options in time domain except using the frequency domain operation. By modifying the form of bar graph extracted from the time domain, here we tend to take into account the extra element of resisting common signal process operations, like MP3 compression. In alternative words, an effort is made to study the matter of the watermark against each TSM and lossy compression. During this paper we tend to transfer the form of audio bar graph within the time domain to the low-frequency sub-band by (i) segmenting associate audio signal into parts in relevance the bin dimension of the time-domain bar graph, (ii) concatenating the parts in every bin, and (iii) DWT filtering of the concatenation of the parts in every bin. The watermark is inserted by shaping the bar graph. In depth testing shows that compared with the time-domain theme Time-scale invariant audio watermarking supported the applied math options in time domain, DWT-based watermarking technique is additionally strong to TSM, MP3 compression, etc.

In Ref [10] will give us the knowledge activity system in audio signals supported a Rational Dither Modulation is projected, that hides information within the Modulated advanced Lapped rework (MCLT) domain. The projected system is ready to cover around of 689bits per second, whereas keeping a CD-quality audio signal. Objective and subjective evaluations are robust to classical attacks and transparency to the Human sensory system (HAS), separately.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

The algorithm recommended in this paper, chooses bit of the frequency of FFT range for inserting the confidential bits. The chosen waveband is partitioned into small frames and individual secret bit is inserted into each frame. The biggest Fibonacci number particularly lesser than each single FFT magnitude in every frame should be computed based on similar secret bit to be inserted. All samples in each frame are modified. Total FFT samples in single frame must be altered to the nearest Fibonacci number with even index if the confidential bit is "0".All FFT samples in a frame should be modified to nearest Fibonacci number with odd index if confidential bit is "1". To depict a scheme in plenty of watermarking systems FFT is used. To the best of our information this is the first audio watermarking depending on Fibonacci numbers. Utilizing Fibonacci sequence for inserting the secret bits improves translucency and ruggedness in contrast to attack. This method acquires high potentiality, and produce hardiness towards some regular signal processing attacks.

II. PROPOSED METHOD

2.1 Fibonacci Numbers and Golden Ratio

The arrangement of numbers as1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89……is known as the Fibonacci numbers. It has been named by the nineteenth-century French mathematician Edouard Lucas after Leonard Fibonacci of Pisa, one of the best mathematicians present in the Middle Ages, who referred to and presented them in his book Liber Abaci (1202) in connection with the rabbit problem described by him. The Fibonacci sequence has fascinated both beginners and professional mathematicians for centuries due to their abundant applications and their ubiquitous habit of occurring in the totally surprising and unrelated places. In this paper we apply Fibonacci numbers for audio watermarking.

The equation presented below gives the sequence of Fibonacci numbers as,

$$F_n = \begin{cases} 0 & if n < 0, \\ 1, & if n = 1, \\ F_{n-1} + F_{n-2}, & if n > 1 \end{cases} \qquad (1)$$

Fibonacci numbers are having interesting features. One of the most famous ones we used in this proposed work is, the ratio between two consecutive Fibonacci numbers which is shown as below

$$F_n = F_{n-1} + F_{n-2}; \qquad (2)$$

$$\frac{F_n}{F_{n-1}} = \frac{f_{n-1} + F_{n-2}}{F_{n-1}} = 1 + \frac{F_{n-2}}{F_{n-1}} = 1 + \frac{1}{\frac{F_{n-1}}{F_{n-2}}}; \qquad (3)$$

$$\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \lim_{n\to\infty} \left(1 + \frac{1}{\frac{F_{n-1}}{F_{n-2}}}\right) e = 1 + \frac{1}{\lim_{n\to\infty} \left(\frac{F_{n-1}}{F_{n-2}}\right)}; \qquad (4)$$

$$\text{if} \lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \varphi; \ \varphi = 1 + \frac{1}{\varphi}; \qquad (5)$$

$$\varphi^2 - \varphi - 1 = 0; \qquad (6)$$

$$\varphi = \frac{1 \pm \sqrt{5}}{2}, \qquad (7)$$

As, φ is positive, then$= 1.618$ .Golden quantitative relation is that, which is real with many curious properties. According to AN, Golden quantitative relation is real, however not a transcendental one (like π), since it's the answer to a polynomial equation. The Golden quantitative relation seemingly obtained its name from the Golden parallelogram, a parallelogram whose sides are within the proportion of the Golden quantitative relation. Therefore, as an example, the facade of temple will be well framed with a Golden parallelogram. Great Egyptian pyramids and famous monalisa art were designed by using golden ratio. Golden ratio plays an vital role in numerous geometric dimensions, such as two dimension and three dimension. Every Fibonacci number will be drawn by the Golden quantitative relation. Below given equation represent how each Fibonacci number is generated by the Golden Ratio.

$$F_n = \frac{\varphi^n - \varphi^{-n}}{\sqrt{5}}, \qquad (8)$$

Where $\bar{\varphi}$ is the negative solution of Equation (7)

To perceive the characteristics of human sensory system (HSS) worked has been performed over the years and implementing this data to audio compression and audio watermarking is more effective solution.

Fig. 1 illustrates the vary of frequencies and intensities of sound to that the human sensory system responds. Absolutely the threshold, the minimum level of sound that's detectable by human ear, is powerfully relying on frequency which is very

effective. At the extent of pain, sound levels are six times higher in magnitude than the token audible threshold. The force per unit area level (SPL) is measured in decibels (dB) which is smallest unit of measure.

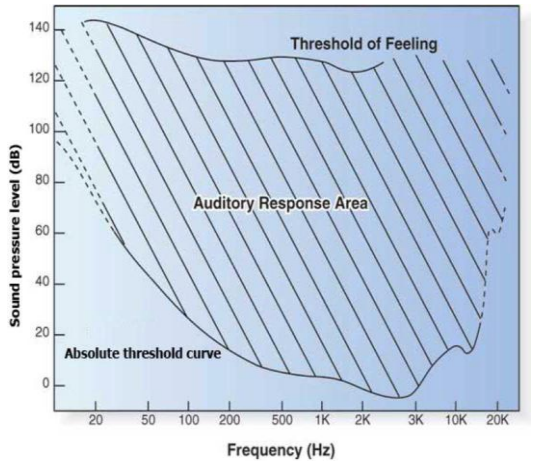


Fig. 1.Characteristic Definite Threshold Curve Of Human Sensory Response

Decibels are represented in a graduated table, where, every 6 dB increase represents a doubling of intensity in the audio. The perceived loudness of a sound is expounded to its intensity. Normally, we tend to hear sounds as low as 20 HZ and as high as 20,000 Hz. Hearing is best at concerning 3-4 KHZ and sensitivity diminishes at higher and lower frequencies, yet more at higher than lower. Thus, it's clear that, by embedding knowledge within the high waveband that is employed within the projected theme, the distortion are largely infrasonic and so additional transparency are obtained in this work. In the instructed watermarking theme, we tend to use the subsequent algorithmic rule to implant a watermark embedding (secret bit stream) into the FFT coefficients. Initial of all, the parameters ought to be adjusted on the basis of the required capacity, transparency and strength of the output compared with input. The waveband and frame size area unit are two parameters that set the properties of the projected watermarking methodology. The chosen waveband is split into short frames then every single secret little bit of the watermark stream is embedded into all samples of a frame, that makes the tactic additional sturdy against attacks.

A. ***Tuning***

The advised system provides two parameters to regulate three properties of the watermarking system. The waveband, and therefore the frame size (d) are the two parameters of this methodology to regulate capacity, sensory activity distortion and ruggedness. During this theme, we've got general standardization rules which may support to pass the necessity. The frame size has additional result on strength, whereas the waveband has additional result on transparency and capacity. In alternative words, by increasing the frame size, higher strength is achieved. Moreover, increasing the waveband results in higher capability and additional distortion. Note that these parameters enable regulation of the ODG between zero (not perceptible) and -1(not annoying), with about 650 to 3000 bits per second (bps) capacity and permitting strength against MP3-128, that area unit very higher than typical needs. As most MP3 cut-off frequencies area unit beyond 16 KHz, the high waveband, is about to 16 KHz rate or lower. Then, to pick the waveband, primarily the low waveband, ought to be adjusted. The default value for low waveband is 12 KHz rates. Decreasing lower waveband implies increasing capability and distortion. Increasing the frame size, ends up in a much better strength, however capacity decreases.

The default value for the frame size is d=5. Fig.2 shows the flow sheet for the choice of the calibration parameters. Within the data formatting, low frequency is 12 kHz, high frequency is 16 KHz and d is 5. This flow sheet facilitates adjusting the parameters based on the necessity. However, adjusting the parameters depending on some demands is extremely troublesome and considering a trade-off between capability, transparency and strength is often necessary.

B. Embedding the Secret Bits

The band and also the frame size are the two needed parameters within the embedding method that ought to be adjusted following the necessity. During this section, for simplicity, we tend not to contend with the regulation of those parameters and simply consider them to be fixed. The effects of those parameters are measured and analyzed within the experimental results section.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

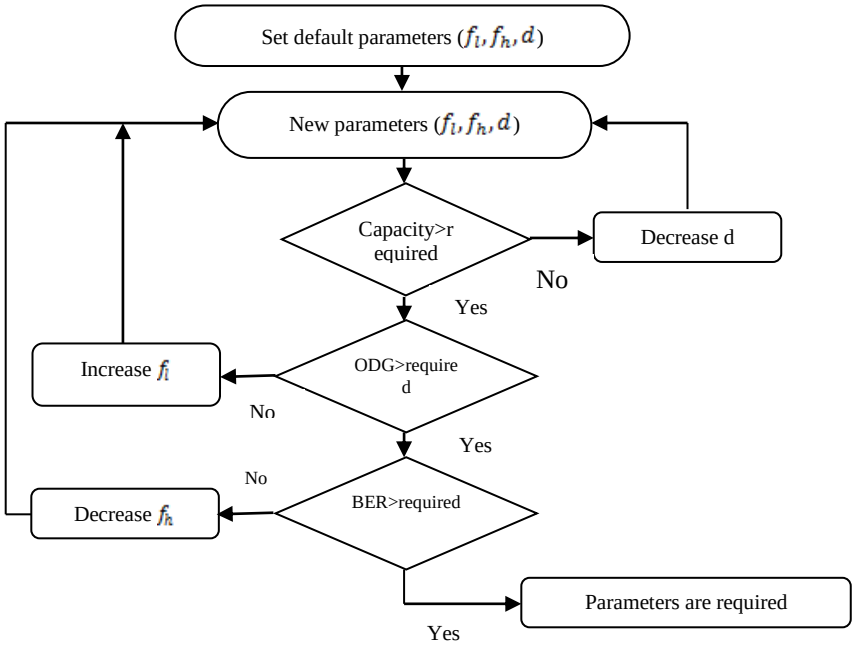


Fig. 2 Flowchart of the Tuning Process.

For embedding the watermark stream, initiallyFFT is applied to the audio signal so the FFT samples are altered to nearest Fibonacci numbers based on the secret bits. Finally the inverse FFT is applied to come up with the marked audio signal. The embedding steps are as explained below.

1. Apply FFT to compute the FFT spectrum coefficients of the audio signal which should be analyzed further. We can use total long length audio (for short clips, e.g. with less than one minute) or blocks of particular length (e.g. 10 seconds) for longer files.

2. Divide the FFT spectrum in some selected frequency band into frames of size.

3. For all the FFT spectrum in the current frame, find out largest Fibonacci number, the n th Fibonacci number for I th FFT sample, which is lower compared with the magnitude of the FFT sample . It is should be known that we use the following Fibonacci set as given below,

F={1,2,3,5,8,13,24,35,55,….}

In the original Fibonacci set there are two ones. We are using only one of them.

4. The marked FFT spectrum samples are obtained by Equation (9).

$$f_i' = \begin{cases} f_{ib_{n,i}}, & \text{if } n \bmod 2 = 0 \text{ and } w_i = 0, \\ f_{ib_{n-1,i}}, & \text{if } n \bmod 2 = 0 \text{ and } w_i = 0, \\ f_{ib_{n+1,i}}, & \text{if } n \bmod 2 = 0 \text{ and } w_i = 1, \\ f_{ib_{n,i}}, & \text{if } n \bmod 2 = 0 \text{ and } w_i = 1 \end{cases} \quad (9)$$

Where l=$\lfloor i/d \rfloor + 1$, $w_l$is the l -th bit of the secret stream and largest integer. Each secret bit is embedded into a given frame that is we can say that each frame represents a single secret bit.

5. At last, use the IFFT to obtain the marked audio signal.

By enlarging the band, the capacity and distortion increase and hardiness decreases. Also, increasing the frame size strengthens the ruggedness against attacks and reduces the capacity. Additionally, the employment of FFT magnitude leads to increased robustness against attacks compared to the employment of the real or the imagined components solely. Fig.3 provides the flow sheet of the embedding algorithmic program.

C. Extracting the Secret Bits

The host audio signal isn't needed within the detection method, and hence, the detector is blind. The detection parameters, the frame size and also the band, will be transmitted securely to the detector or

normal parameters will be used for all audio signals. The detection method is summarized within the following steps:

1. Apply the FFT to calculate the FFT coefficients of FFT spectrum for the marked audio signal.
2. Divide the FFT spectrum samples in the selected frequency band into given frames of size.
3. For each single FFT spectrum sample in current frame, find the closest Fibonacci number which is used further , the I th Fibonacci number for the given j th FFT sample, to the magnitude of the FFT sample . If the FFT sample has the same distance different Fibonacci numbers, then we have to select the lower Fibonacci number. We use as the Fibonacci set which nothing but samples got at final.
4. To detect a secret bit in a frame got by the FFT analysis, each sample we must examine to check if it is a zero ("0" embedded) or a one ("1" embedded). Then, depending on the evaluation for all samples in the current frame, a secret bit can be extracted which is nothing but final extraction. The watermark bit can be extracted by using the following equation:

$$B_i^{'} = \begin{cases} 0, & \text{if} n \bmod 2 = 0, \\ 1, & \text{if} n \bmod 2 = 1, \end{cases} \quad (10)$$

$B_i^{'}$ is the bit extracted from every sample.When obtaining data concerning all samples, supported the quantity of samples that represent "0" or "1" (voting scheme) a secret bit may be extracted for every single frame.

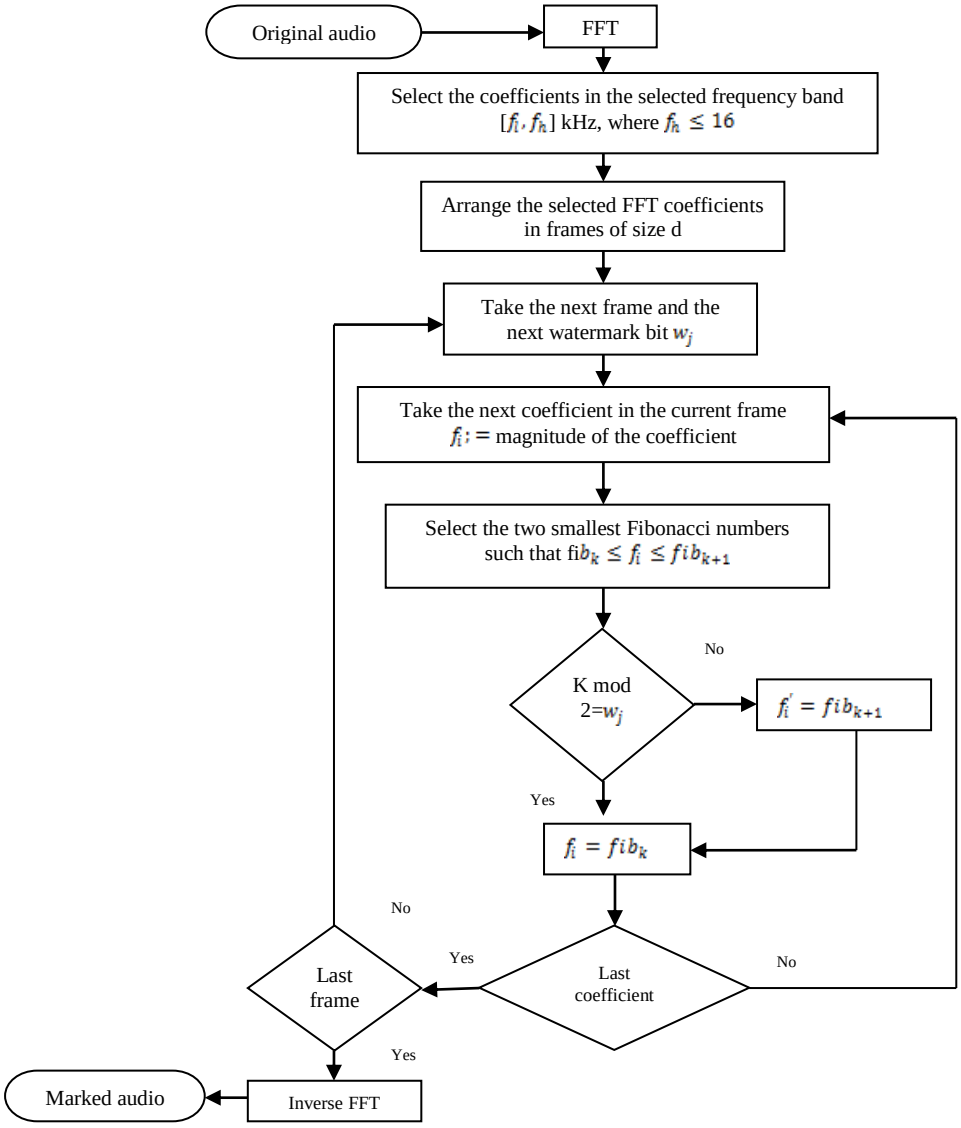


Fig.3 Flow chart of Embedding Algorithm

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

If the quantity of samples known as "0" is adequate or larger than half the frame size, the extracted bit is "0", otherwise it's "1". As an example if the frame size is 5 and that we observe two"0" and three "1", then the extracted secret little bit of the frame would be "1".

D. Security

The standardization parameters give a primary level of security within the system. An aggressor making an attempt to erase, replace or extract the embedded watermark won't be able to perform these actions if he or she doesn't recognize the embedding frequency limits and/or the frame size. However, if an aggressor is aware of or guesses these secret values, the embedded watermark will be additionally protected with cryptography. To increase security, we can make use of a pseudo-random number generator (PRNG) that can amend the key bit stream {to another to a different} that makes it tougher for an aggressor to extract the key info. As an example, the embedded bit stream can be constructed as the XOR of watermark and a pseudo-random bit stream. The seed of the PRNG would be needed as a secret key each at the sender and also the detector. Several cryptography techniques exist which are useful in increasing the safety of the system. Supporting the necessities of the watermarking system, a cryptanalysis technique ought to be chosen. As an example, if we would like to extend security, AES encoding could be a sensible or fine choice in terms of complexness.

II. SIMULATION RESULTS

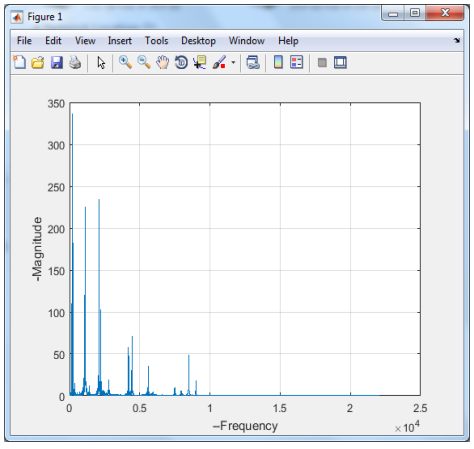


Fig .4 Magnitudes vs. frequency spectrum for watermarked signal (Using FFT).

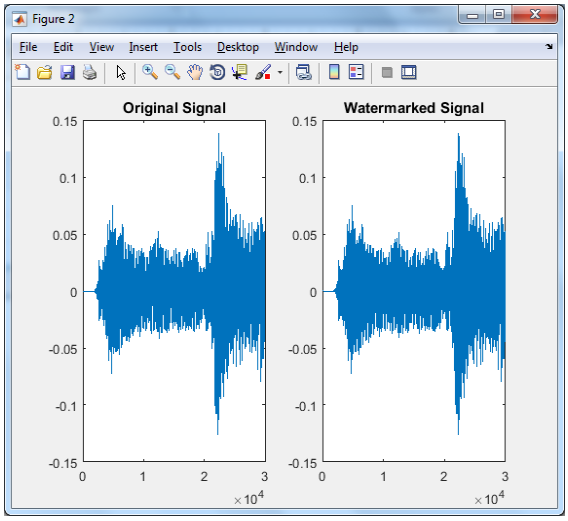


Fig. 5 Spectrum of original signal and spectrum of watermarked signal using proposed work (FFT spectrum).

Calculated value in MATLAB for SNR and BER for proposed work.

```
SNR_prp =

    45


BER_prp =

    27
```

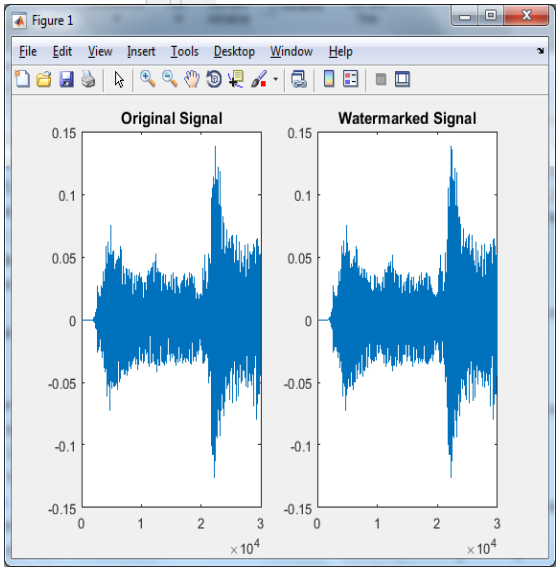
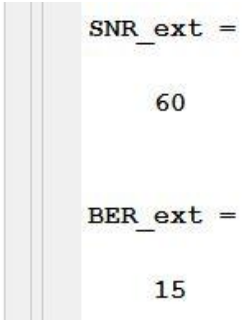


Fig. 6 Spectrum of original signal and spectrum of watermarked signal using extension (DWT)

Calculated value in MATLAB for SNR and BER for extension work.



III. CONCLUSION

The given work shows the robustness of the proposed work for embedding and extracting huge information which is famously known as watermarking technique. In the presented work high capacity and transparent watermarking based on Fibonacci series is proposed which is having better state and as well as robustness among all existing techniques. By opting for Fibonacci series, we have advantage of changing the frequency samples.

The advantages of using this system are: the maximum change in FFT samples is not more than 61% and also the average error is less than 25%. This is very rugged and transparent technique of watermarking. Further we can say the proposed work is a blind work since it does not require the original signal for extracting the hidden bits. The experimental results conclude that, this method has high capacity (700 bps to 3 kbps) without significant perceptual distortion (ODG about -1) and provides robustness against common signal processing attacks such as echo, added noise, filtering or MPEG compression (MP3) even with rates as low as 64 kbps. The proposed method clearly overcomes the results of recent methods that can be compared with it in terms of capacity.

REFERENCES

1.J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, written by the I. J. Cox, M. L. Miller, J. A. Bloom, in 2nd Edition, Morgan Kaufmann, 2008, p. 31.

2. "Mean squared error: love it or leave it? - A new look at signal fidelity measures,"written by Z. Wang and A. C. Bovik, IEEE Signal Processing Magazine, Vol. 26, No. 1, pp. 98-117, January 2009.

3. "A Novel Area Efficient Folded Modified Convolutional Interleaving Architecture for MAP Decoder," given by the authors S. Shiyamala and Dr. V. Rajamani, International Journal of Computer Applications (IJCA), Vol. 9, No. 9, p. 1, November 2010.

4."Algorithms for audio watermarking and steganography," by the authors p. 5. N. Cvejic, Academic Dissertation, Faculty of Technology, University of Oulu,

5. "Adaptive wavelet domain audio steganography with high capacity and low error rate,"given by the Shahreza S.S. and Shalmani M.T.M., in Proceedings of the IEEE International Conference on Information and Emerging Technologies, (ICIET,,07), pp. 1729-1732, 2007.

6."Information hiding using LSB technique with increased capacity," Dr. H. B. Kekre and A. A. Archana, International Journal of Cryptography and Security, Vol. 1, No. 2, p. 1, October 2008.

Thesis, Indian Institute of Technology Kharagpur. M. Adya, M.Tech

7."Data embedding in audio using time-scale modification," given by M. Mansour and A. Tewfik,in IEEE Trans. Speech Audio Process., vol. 13, no. 3, pp. 432–440, May 2005.

8. "Audio watermarking robust against time-scale modification and MP3 compression,"given by the S. Xiang, H. J. Kim, and J. Huang, in Signal Process., vol. 88, no. 10, pp. 2372–2387, Oct. 2008.

9."Data hiding in audio signal using rational dither modulation," is given by J. J. Garcia-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana,in IEICE Electron. Express, vol. 5, no. 7, pp. 217–222, 2008.