ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

A Novel High Capacity Audio Watermarking Method Based On Fibonacci Numbers

Reeja Jolly[1], Dr. Vishnu Rajan[2]
M.tech Scholar, Electronics and Communication Engineering Department, Sahrdaya college of Engineering and Technology, Thrissur, India [1]
HOD, Electronics and Communication Engineering Department, Sahrdaya college of Engineering and Technology, Thrissur, India [2]

Abstract: Digital watermarking has been mainly used for copyright protection, data authenticity, ownership identification, copy protection against image, audio, video. Audio watermarking is mainly focused in this paper. This paper proposed an audio watermarking scheme with the hardware implementation. Audio Watermarking is valuable procedure for audio systems. Many algorithms are used and try to improve results. Most of the algorithms are focused on providing robustness and imperceptibility. This paper presents a novel high-capacity audio watermarking system to embed data and extract them in a bit-exact manner using FFT method by changing some of the magnitudes of the FFT spectrum. Here the idea behind in this paper is to divide the FFT spectrum into short frames and change the magnitude of the selected FFT samples using Fibonacci numbers. Using Fibonacci numbers, it is possible to change the frequency samples adaptively. Utilizing the nearest Fibonacci number for FFT extents brings about a robust and transparent watermarking procedure. In this paper proposed strategy is executed in hardware Raspberry pi too. The test comes about demonstrate that the technique has a high capacity (700 bps to 3 kbps) and results robustness against difficult audio signal processing such as echo, added noise, filtering and MPEG compression (MP3).

Keywords: Audio watermarking, Fibonacci numbers, multimedia security, FFT Spectrum, Raspberry Pi3 model B

I. Introduction

Presently a days, with the fast improvement of different correspondence strategies, exchanging computerized interactive media content turns out to be more less demanding and an enormous number of creators' and distributers' protected innovation copyrights have experienced infringement, which have prompted colossal harm of their benefits in numerous applications. In this way, it ends up vital to give an idea to learning security, so watermarks are considered as the easiest method to handle the powerful issue. Embedding secret knowledge is known as watermarks, into multimedia content is used as a potential solution to copyright infringement. Steganography and cryptography are the two another data hiding methods. Steganographic methods are not provide robustness against common signal processing attacks and in cryptographic methods once secret information is decrypted then its security lost. Digital watermarking is a process by which a

Secret knowledge is hidden or embedded into a media (cover data), for example electronic documents, images, audio and video. These secret data can later be detected or extracted from the marked signal for various applications.

Thinking about embedding domain, audio watermarking can be done in both frequency and time domains. In time domain method, the masked bits are inserted directly into the time signal intervals. These schemes are easy to implement and are usually efficient but weak against some common signal processing attacks. Considering the frequency domain apply certain frequency transforms like FFT, DWT and DCT, then secret bits are embedded into the transformed domain.

The ultimate goal of this paper is to provide a secure audio watermarking based on Fibonacci numbers. Audio watermarking is helpful for durable and secure transferring of data associated with the host audio signal, which incorporates watermark that is embedded into, and extracted from, the host audio signal. Watermarking can be used for several applications, including copyright protection, monitoring and fingerprinting, showing content manipulation and information carrier. An audio watermarking consists of different properties including Imperceptibility, Security, Robustness, Capacity and Payload.

This paper organization is as follows: The related works done on earliest audio watermarking techniques is discussed in Section II. Section III describes proposed method. Section

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

IV describes about the system implementation of the system, it also evaluates the results provided by the implementation. The work is concluded in Section V.

II. Related Work

This section presents the review of the different papers which mainly focus on the importance of audio watermarking and also based on detection of watermark from the watermarked signal. Past audio watermarking techniques were not very robust and watermarked signal doesn't have good value of imperceptibility. Various audio watermarking techniques have been discussed below:

The paper [2] which gives the work related to DWT-DCT based visually impaired watermarking calculation for copyright security. In this the mix of two algorithm is used, the watermark is first mixed by Arnold and after that the watermark is installed in a spread spectrum pattern using pseudo random. In this watermark procedure starts by applying DWT to the original content and then the DCT is applied on sub band formed by the DWT, as it is visually impaired watermarking technique host signal is not present at the time of extraction. As indicated by the outcomes this algorithm provides better performance as compared to DCT algorithm in accordance to security and robustness.

In paper [3] portrays audio watermarking framework related to hybrid transform audio watermarking algorithm .Transform domain strategies gives preferred execution than time domain because transform domain technique is largely exploited to Human Auditory System In this two powerful transforms are applied on the original audio signal that is Discrete Wavelet transform and Discrete sine transform using double insertion of the watermark. The watermark utilized in this scheme is gray scale logo image instead of randomly generated Gaussian noise type watermark. Many subjective and objective test have been performed on the proposed watermarking scheme which determines the high quality audio signal quality and robust to different attacks. The advantage of this method is the property of energy compaction of Discrete Sine transform. The Finite Ridgelet Transform also known as FRIT is used for encrypting system to secure the watermarking system.

The paper [4] proposed work related to audio watermarking algorithm for copyright protection of the audio signal using time domain processing. The watermarking algorithm suggested in this paper does not require the original signal for the detection process. The algorithm suggested in this paper is take the host digital audio and divide the host audio into set of embedding segments for increasing robustness of extraction method. The watermark signal is created using a key that means single number known only to the copyright owner. The watermark embedding depends on the amplitude and frequency of audio signal in a way that reduces the audibility of the watermark signal. The advantage of this method is to provide robust to different to common signal properties like cropping, time shifting, filtering, resampling and re-quantization. The disadvantage of this method is that it is not robust against more sophisticated attack like changing in time scale of the original signal.

The paper [5] proposed work related to the blind audio watermarking algorithm for embedding watermark in a binary logo form in an audio signal this technique is known as Dyadic Wavelet Transform. Basically one dimensional DYWT method but here in this work two dimensional DYWT method used by constructing an image from an audio signal , the original signal is divided into some parts and arranged these parts in some rows based on the visualization method. The disadvantage of this method is that it is shift variant that is why a watermarking method based on DYWT is expected to be robust against geometrical distortions such as clipping and desynchronization. The advantage of this method is that it gives redundant representation and can be implemented with a fast algorithm, the amount of information that the watermark must carry is higher than in DWT-based methods.

In paper [6] novel time spread echo-based audio watermarking scheme with optimized imperceptibility and robustness is proposed. This work improves imperceptibility by suppressing the frequency response of the kernel in perceptual significant region. This is achieved by reducing low frequency patterns in the PN sequence. However, such suppression is inexact. In contract, we propose to design the echo kernel from finite-impulse- response (FIR) filter design perspective, where convex optimization is used to obtain a set of filter coefficients to replace the PN or MPN sequence.

The paper [7] proposed a blind audio watermarking technique which does not require original signal at the time of detection process. The proposed algorithm is built in wavelet domain using QR decomposition for inserting a watermark in original audio signal. The above method is carried out in frequency domain having advantages such as high payload capacity and robust against different synchronization attack like compression etc. The major disadvantage of time domain technique is that it is immune to different signal processing attacks. The throughput of this method is that it provides high payload capacity for embedding the watermark in an original signal.

The paper [8] proposed an audio watermarking method which takes the use of spread spectrum watermarking which is basically modulating method for adding a watermark in a host signal. In this paper spread spectrum technique is used for cyclic shift in the pseudo noise sequence because it gives the advantage in embedding information capacity in the host

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

signal while in traditional spread spectrum technique only one bit information is embedded in each frame. Another advantage of this method is that it maintains the transparency in the watermarked audio signal in silent frames i.e. the frame which has low energy content. Diverse preprocessing plans like high pass separating, straight prescient coding and brightening channel guarantee that this approach can be used for exchanging watermark motion through phone lines. According to the experiment performed on different audio samples it is observed that the traditional spread spectrum technique is more robust against different attacks but when band pass filtering and all pass filtering is taken into consideration then spread spectrum technique is best.

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 [1].

III. Proposed Method

There are various steps involved in Raspberry pi based implementation of audio watermarking based on Fibonacci number. Fig.1. shows steps involved in proposed method. The first step is the Fibonacci number generation, then input the host audio signal and converting original audio signal into frequency domain using FFT transformation. Next step is input the secret, then embedding the secret bit into audio and apply inverse FFT to obtain watermarked audio signal. Next is the watermark extraction. Finally encryption and decryption step to increase the security of the proposed method.

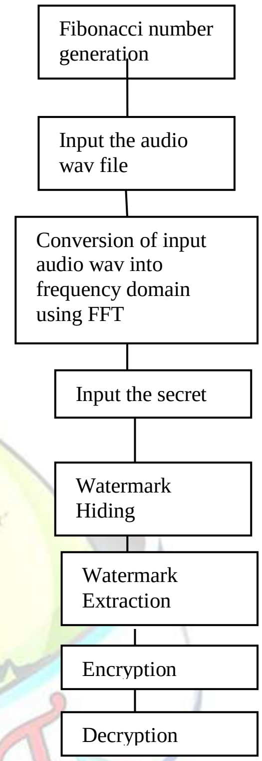

Fig. 1. Steps involved in proposed method

A. *Fibonacci Numbers*

The arrangement 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89… … is known as the Fibonacci arrangement. It has been named by the nineteenth-century French mathematician Edouard Lucas after Leonard Fibonacci of Pisa, a standout amongst other mathematicians exhibit in the Middle Ages. In this paper we apply Fibonacci numbers for sound watermarking. The equation (1) in [1] utilized for creating Fibonacci numbers are given below:

$$Fn = \left\{ \begin{array}{c} 0, \quad if\ n < 0 \\ 1, \quad if\ n = 1 \\ Fn - 1 + Fn - 2, if\ n > 1 \end{array} \right\} \ldots (1)$$

Hearing reach clarifies the scope of frequencies that can be heard by people or different creatures. The human range is ordinarily given as 20 to 20,000 Hz, however there is impressive variety between people, particularly at high frequencies, and a gradual loss of sensitivity to higher frequencies with age is considered normal Hearing is best at

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

concerning 3-4 KHz and affectability decreases at higher and bring down 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.

B. Parameter Selection

The waveband and frame size are the two parameters that set the properties of the projected watermarking technique. The chosen waveband is split into short frames then every single secret bit of the watermark stream is hidden into all samples of a frame that makes the system robust against attacks. The parameters of this methodology used to regulate capacity, sensory activity distortion and ruggedness. 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 and by increasing the waveband results in higher capability and additional distortion. As most MP3 cut-off frequencies area unit beyond 16 KHz, the high waveband, is about to 16 KHz rate or lower. The default value for low waveband is 11 KHz rates in this methodology. The default value for the frame size is d=6. The selection of these parameters depending on some demands is extremely troublesome and considering a trade-off between capability, transparency and strength is often necessary.

C. Watermark Hiding

The band and also the frame size are the two needed parameters within the embedding method. For embedding the watermark stream, initially FFT 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. 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. Watermark hiding steps summarized below:

1. Apply the FFT to transferring host audio signal into frequency domain for computing frequency coefficients.
2. FFT spectrum in the selected frequency band is divided into number of frames of size equal to 6.
3. The largest Fibonacci number that is lower than each single FFT magnitude in each frame must be computed and, depending on the corresponding secret bit to be embedded, all samples in each frame are changed. The following Fibonacci set is used for this algorithm:

$$\{F= 1,2,3,5,8,13,21,34,55\ldots.\}$$

4. Then each single secret bit is embedded into a given frame that is we can say that each frame represents a single secret bit.
5. If the secret bit is “0”, all FFT samples in a frame should be changed to the closest Fibonacci number with even index. If the secret bit is “1”, all FFT samples in a frame should be changed to closest Fibonacci number with odd index.
6. At last, use the inverse FFT 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.

D. Watermark Extraction

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 (2) in [1]:

$$B_i' = 0, if\ n\ mod\ 2 = 0\ \&\ 1, if\ n\ mod\ 2 = 1 \ldots.(2)$$

Bi’ is the bit extracted from every sample.

E. Encryption And Decryption

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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

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 [1]. 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.

IV. IMPLEMENTATION AND RESULTS

The proposed system is implemented on Raspberry Pi3 model B. The proposed audio watermarking is simulated using Python programming language. The usage of Python platform made the system to give efficient result. Python version 3 is used. The results are shown in below:

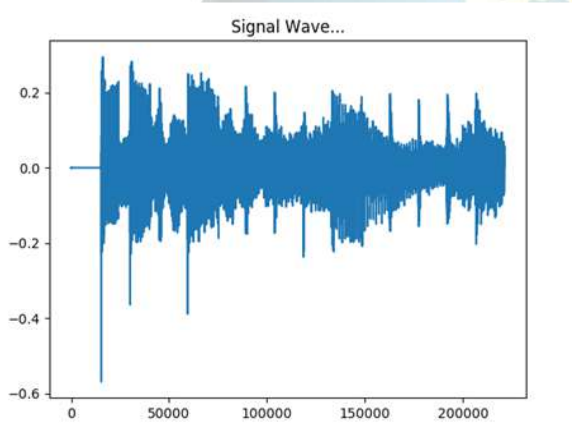

Fig. 2. Spectrum of original signal

The spectrum of host audio signal in time domain is shown in Fig.2. The audio signal is in WAV format. The x-axis shows the time and y-axis shows the amplitude. Fig.3. shows host audio signal in frequency domain. Here original audio signal is transformed in frequency domain by FFT (Fast Fourier Transform) method.

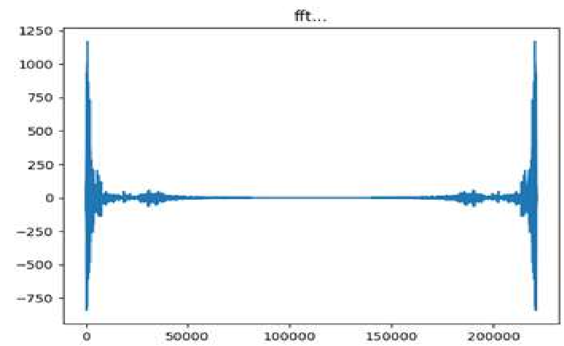

Fig. 3. Spectrum of original signal is transformed into frequency domain using FFT transform

The watermarked audio signal is shown in Fig.4. The inverse FFT is used to obtain the marked audio output in the proposed method. By analysing Fig.2 and Fig. 3 that is original and watermarked signal we can understand that both the waves are unique and identical, that means quality of the watermarked signal is retained after adding the watermark into the host signal. That is the proposed method achieves better Imperceptibility also this method achieves high capacity about 700 bps to 3 kbps.

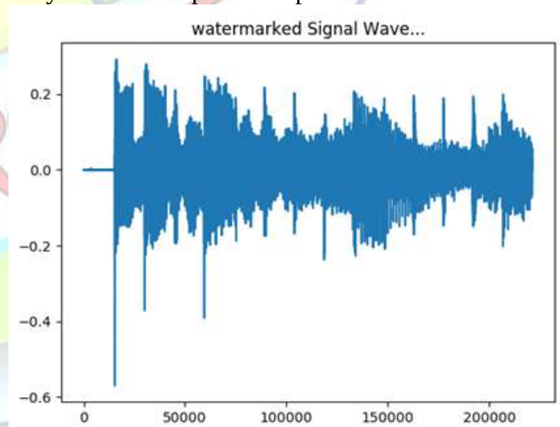

Fig. 4. Spectrum of watermarked signal using proposed work

In this paper proposed method is also implemented using hardware Raspberry pi 3 model B. The output of this proposed method also obtained from raspberry pi 3 model B. The system was able to operate in a good performance. The method provides high capacity audio watermarking method using Fibonacci numbers to embedded data and extract the secret into bit exact manner using FFT method.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

V. CONCLUSION

In this paper, a high-capacity transparent digital audio watermarking system using Fibonacci number is presented. The proposed method simulated using Python Programming language and it's implemented in hardware using Raspberry pi 3 model B. The system is robust against difficult signal processing attacks like echo, filtering and added noise. The given work shows the robustness of the proposed work for embedding and extracting huge information. By using Fibonacci series for audio watermarking, we have advantage of changing the frequency samples.

The frame size and frequency band are the two adjustable parameters of this system that determine the capacity, the perceptual distortion and the robustness against attacks. The proposed work is a blind work since it does not require the original signal for extracting the hidden bits. This method has high capacity (700 bps to 3 kbps). The proposed method clearly overcomes the results of recent methods that can be compared with it in terms of capacity 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.

ACKNOWLEDGMENT

I wish to record my indebtedness and thankfulness to all those who helped me to prepare this paper titled A Novel High Capacity Audio Watermarking Method Based on Fibonacci Numbers and present it in a satisfactory way. First and foremost I thank God Almighty for his providence and for being the guiding light throughout the seminar.

I want to start expressing my thanks to my guide Dr. Vishnu Rajan, Head of the Electronics and Communication Department, for his valuable advice and guidance towards this work. I received motivation, encouragement and hold up from them during the course of work.

REFERENCES

[1]. Fallahpour, Mehdi, and David Megias. "Audio watermarking based on Fibonacci numbers." IEEE Transactions on Audio, Speech, and Language Processing 23, no. 8 (2015): 1273-1282.

[2]. Feng, Liu Ping, Liang Bin Zheng, and Peng Cao. "A DWT-DCT based blind watermarking algorithm for copyright protection." In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 7, pp. 455-458.

[3]. Yassine, Himeur, Boudraa Bachir, and Khelalef Aziz. "A secure and high robust audio watermarking system for copyright protection." International Journal of Computer Applications, (2010): 53, no. 17.

[4]. Bassia, Paraskevi, Ioannis Pitas, and Nikos Nikolaidis. "Robust audio watermarking in the time domain." IEEE Transactions on multimedia 3, no. 2 (2001): 232-241.

[5]. Minamoto, Teruya, Yuji Ogata, and Masahiro Sawai. "Visualization of Digital Audio Watermarking Based on the Dyadic Wavelet Transform." In Information Technology: New Generations (ITNG), 2012 Ninth International Conference on, pp. 640-645.

[6]. Hua, Guang, Jonathan Goh, and Vrizlynn LL Thing. "Time-spread echo-based audio watermarking with optimized imperceptibility and robustness." IEEE/ACM Transactions on Audio, Speech and Language Processing (TASLP) 23, no. 2 (2015): 227-239.

[7]. Kaur, Arashdeep, Malay Kishore Dutta, Krishan Mohan Soni, and Nidhi Taneja. "A high payload audio watermarking algorithm robust against Mp3 compression." In Contemporary Computing (IC3), 2014 Seventh International Conference on, pp. 531-535.

[8]. Tafreshi, Hosein Fami, and Ali Asghar Soltani Farani. "Spread spectrum audio watermarking: Enhancement of detection and watermarking capacity." In Electrical Engineering (ICEE), 2014 22nd Iranian Conference on, pp. 1477-1482.

[9]. Seo, Jung-Hee, and Hung-Bog Park. "Hardware Based Real Time Audio Watermarking Using Embedded Module." Journal of Next Generation Information Technology 4, no. 5 (2013): 1.

[10]. Unoki, Masashi, and Ryota Miyauchi. "Method of digital-audio watermarking based on cochlear delay characteristics." Multimedia Information Hiding Technologies and Methodologies for Controlling Data (2012): 42-70.