Implementation of Robust Audio Watermarking for Real Time Copyright Protection

Gopalakrishnan.E[1] Member IEEE, Silambarasan.D[2], Vijeyakumar.K.N[3]
[1,2]PG Scholar, Department of ECE, Anna University Regional Centre, Coimbatore.
[3]Assistant Professor, Department of ECE, Anna University Regional Centre,Coimbatore.
[1]krishna14ece@gmail.com, [2]simbu.chandran@gmail.com, [3]vijey.tn@gmail.com

***Abstract*— Due to the development of the Internet, security and intellectual property (IP) protection have involved significant feature in the copyright protection field in recent times. The audio watermarking is generally used as a multimedia copyright protection tool. In this paper, we present a watermarking algorithm and its VLSI architecture that can insert a CSS signal in real-time to smooth the progress of copyrighted audio signal. Robust audio watermarking plays a most important role for the development of militaries, RADAR and wireless communication. The watermark is a method of embedding information into digital content by adding a signal to the content data. The process of embedding information into an audio signal is called audio watermarking. The system is initially prototyped and validated in MATLAB/Simulink and subsequently implemented in Vertex 4-XC4VLX25-10FF668 FPGA device using Xilinx system generator, the generated VHDL code is synthesized in Xilinx ISE 12.1. The experimental results demonstrate that the proposed watermarking scheme obtains good robustness and conserve imperceptivity.**

***Keywords*— Chirp Spread Spectrum (CSS), Robust Audio watermarking, Copyright Protection, system generator, Simulink/Matlab, Field programmable gate array (FPGA).**

I. INTRODUCTION

Copyright protection is the most important watermark application. The protection of an original work from unauthorized publication, a designer needs a technique that proves legal ownership .The implementation of Robust audio watermarking in hardware helps to achieve real time performance by integrating an audio watermarking chip with existing audio electronic devices. For the safe communication of the secret messages and data protection, the watermarking should provide good imperceptible, good robustness, high speed and high payload capacity. In this paper we presents a new VLSI architecture to implement Robust audio watermarking using chirp spread spectrum technique. By using chirp signal as a secret key, the message can be transmitted as a noise signal such that intruder cannot retrieve the message which is transmitted, and the message can be retrieve at the receiver side only with the help of secret key. Hence it provides high security protection with a low power and less complexity and it is very difficult to detect and intercept, hence it is used for the application of military and wireless communication to provide a hidden communication.

II. RELATED WORK ROBUST AUDIO WATERMARKING

A. Different Types of Audio Watermarking Technique

LSB coding, echo hiding, phase coding and spread spectrum watermarking are the different techniques that are used for audio watermarking. The Least Significant Bits coding audio watermarking is one of the simplest techniques to embed the data, but the watermark will be distorted when there is a small change in Least Significant Bits of the signal. In phase coding technique the watermark is not dispersed over the entire data signal hence it can be easily removed [4,5]. The robustness is increased in echo hiding techniques by embedding the high energy echoes in the signal, which leads to audio distortion. Hence the noise is increased when the payload is increased [6]. In spread spectrum, the watermark is distributed throughout the signal. Among all these techniques, the spread spectrum audio watermarking technique helps to provide hidden communication, high watermark channel bit rate, good robustness, very good imperceptibility and high security. Implementing the audio watermarking technique in hardware helps to provide real time performance by embedding an audio watermarking chip with an available audio device, gives high reliability, low power and low cost applications [3].

B. Spread Spectrum Audio Watermarking Technique

The spread spectrum audio watermarking embeds information by spreading it in the frequency domain. Due to this nature, it provides robust and imperceptible watermarked signal. Hence this method is used for data hiding communications, to prevent recognition of the signal from the watermarked signal [5].There are two different techniques used in spread spectrum. They are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). For generating watermarked signal, the DSSS and FHSS need pseudo-random noise sequence generator. But the chirp spread spectrum (CSS) technique uses chirp signal instead of a pseudo-noise sequence to embed the information. The high robustness and imperceptibility due to the Low Probability of Interception/Detection, low power consumption, low latency and high security lead to the selection of CSS technique for audio watermarking than other techniques. It is used for the military application as it is very difficult to detect and intercept when operating at low power [9, 10].

III. METHODOLOGY

The chirp spread spectrum audio watermarking techniques uses a linear frequency modulated chirp pulses to encode the information. According to the modulation process, the chirp spread spectrum techniques are classified in to two different techniques, they are binary orthogonal keying (BOK) and direct modulation (DM). The BOK schemes use the chirp signal to represent the data. The DM scheme is used just as a spreading code, modulation and demodulation is performed separately from the chirp processing, this allows the DM scheme a flexibility to incorporate various modulation techniques. As well as the chirp signal is act as a secret key between the transmitter and the receiver. At the transmitted side watermark message (message signal) is modulated by using one of the digital modulation techniques called DPSK. There are many possible methods to be employed in which two of the suitable methods are frequency shift keying (FSK) and differential phase shift keying (DPSK).

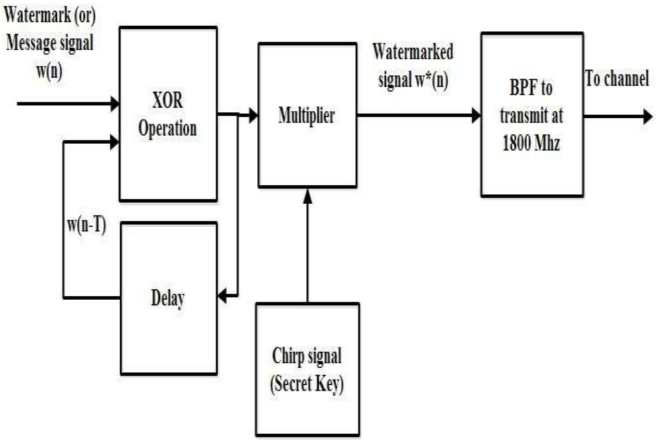
Watermark (or) Message signal w(n)
XOR Operation
Multiplier
Watermarked signal w*(n)
BPF to transmit at 1800 Mhz
To channel
w(n-T)
Delay
Chirp signal (Secret Key)

Fig. 1. Block Diagram of Chirp Spread Spectrum Audio Watermarking Transmitter

The DPSK has an advantage of being bandwidth efficient, incoherent detection or modulation and good resistance to amplitude distortion. The immunity to the amplitude distortion allows them to be insensitive to the effects of multipath. Unlike BPSK, the DPSK modulation technique does not need the synchronous carrier at the demodulator for detecting a signal. The modulated watermark message w*(n), is generated by applying the watermark message to the one of the exclusive-or gate input and the another input is watermark message delayed w*(n - T) with the time T. For example, the watermark message 001001100111, is one of the input of the exclusive-or, The first bit of the modulated watermark message w*(t) is considered as zero so other input w*(n - T) is 0001110111010. Hence the modulated watermark message is 00011101110101. The average spectral density of the signal is reduced by spreading the bandwidth of the transmitted signal; this makes it difficult to detect the watermark message. This technique is meant for the low probability of intercept (LPI) systems. The watermarked signal is formed by multiplying the w*(n) with the chirp signal. This chirp signal c(t) helps to spread the bandwidth of the transmitting signal. The chirp signal can be expressed as,

$$c(t) = ((1/Tc) \exp (j\mu t^2))^{1/2} , |t| < Tc/2 \qquad (1)$$

The bandwidth of the signal can be written as,

$$B = |\mu| Tc \qquad (2)$$

where the Tc denotes the duration of the chirp signal in seconds, μ called the chirp rate denotes the chirp signal in Hz/s instantaneous frequency change rate. The chirp rate is defined by,

$$\mu(t) = dfm(t)/dt \qquad (3)$$

where fm is the instantaneous frequency, it is defined as ,

$$fm(t) = (1/2\pi) (d\o/dt) \qquad (4)$$

where ø is the phase of the signal. The transmitted signal is increased by the increasing the chirp signal time approximately from 1/B to Tc. Some of the properties of the chirp signal is high robustness, wideband signal (low power) constant, uniform power spectral density [12]. Transmit the watermarked signal at 1800 MHz because this band has a license for the low power transmission. Hence the watermarked signal is transmitted in to the receiver through the channel. The transmitted side block diagram is shown in Fig. 1. At the receiver side, the signal is received at 1800 MHz.

The received watermarked signal is multiplied with the chirp signal, produces the output wr(n). Note that the input signal is twice multiplied by chirp signal. Any signal (c(t)) which is multiplied twice $c^2(t) = 1$ which has no effect on the received output signal[14]. Hence the multiplication of the chirp signals both at the receiver and the transmitter side act as a secret key. Only the transmitter and receiver can retrieve the message signal from the noise because only the transmitter and receiver can know the secret key.

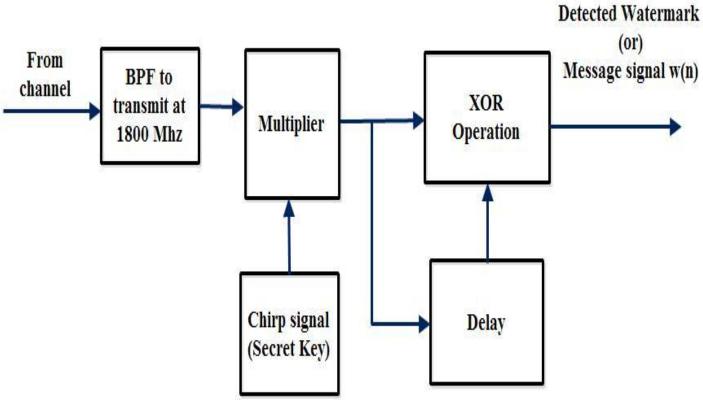
From channel
BPF to transmit at 1800 Mhz
Multiplier
XOR Operation
Detected Watermark (or) Message signal w(n)
Chirp signal (Secret Key)
Delay

Fig. 2: Block Diagram of Chirp Spread Spectrum Audio Watermarking Receiver

The output wr(n) is demodulated by applying it to the exclusive-or gate as one input and the other input is wr(n) delayed with the time T (wr(n - T)). Hence the demodulated wd(n) is the detected watermark message. For example, the wr(n) 00011101110101, is one of the input of the exclusive - or, the other input wr(n- T) is wr(n) delayed with the time T, so the demodulated output is 0010011001111, which is the detected watermark message. The receiver side block diagram is shown in Fig. 2. At the receiver side, the signal is received at 1800 MHz. The block diagram of chirp spread spectrum audio watermarking at the receiver is shown in Fig. 2. The received watermarked signal is multiplied with the chirp signal, and it is demodulated using DPSK demodulation only with the knowledge of the secret key the receiver can retrieve the signal. Hence this technique provides a secret communication between the transmitter and the receiver.

IV. IMPLEMENTATION FLOW

The chirp spread spectrum audio watermarking is implementing in system generator - (Matlab-simulink) in order to implement in hardware. The proposed technique is implemented in Vertex 4-XC4VLX25-10FF668 FPGA device using Xilinx system generator. Fig. 3 shows the implementation flow of audio watermarking in FPGA. With the help of the Xilinx system generator, the VHDL code is generated from simulink for the CSS audio watermarking. The generated VHDL code is synthesized in Xilinx ISE 12.1 and power and area is analyzed for the transmission of the signal at 1800 MHz. The properties of audio watermarking such as robustness and imperceptibility are also analyzed to know the effectiveness of the proposed audio watermarking technique.

V. RESULTS AND DISCUSSION

An efficient and Robust Audio Watermarking for the real time copyright protection was implemented using system generator, chirp signal based on proposed technique is tested with different test patterns. The state-of -the-art proposed CSS achieves the good imperceptibility and robustness. Were the areas was same and power reduced efficiently.

A. *Testing CSS with a Different Test Pattern*

The behavior of the chirp spread spectrum audio watermarking is basically analyzed with different input signals like pulse signal, PN sequence, random number signal, Gaussian noise signal, Rayleigh noise signal and finally with the real time audio signal (wav format). In CSS audio watermarking, the input signal (watermark) is embedded with the chirp signal (secret key), which produces the watermarked signal. The output of chirp spread spectrum for different test patterns is shown in Fig. 4. The original signal (watermark) is the signal which has to be transmitted secretly to the receiver side. This CSS audio watermarking technique uses chirp signal as a carrier for hiding the data hiding (secret message) information. Inserting the watermark signal with the chirp signal helps to transmit the message as a noise to the receiver, such that the unauthorized person cannot recognize the message signal. The watermarked signal is transmitted to the receiver after the modulated original signal (watermark) is multiplied by the chirp signal. Since the 1800 MHz is licensed for low power transmission, the watermarked signal is transmitted and received at 1800 MHz. In order to retrieve the original signal (watermark) at the receiver, one should know the secret key which is used at the transmitter side. Here the original signal (watermark) is extracted from the watermarked signal with the help of chirp signal, which acts as a secret key.

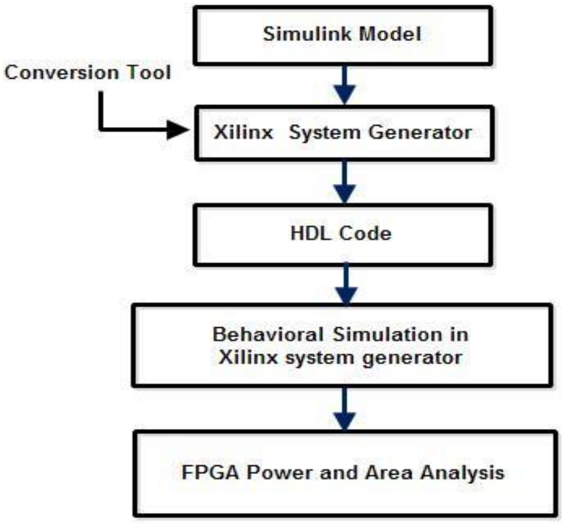
Simulink Model
Conversion Tool
Xilinx System Generator
HDL Code
Behavioral Simulation in Xilinx system generator
FPGA Power and Area Analysis

Fig. 3. Implementation flow

B. Power Consumption of CSS based Audio Watermarking

The proposed technique is tested for different test input signals and real time audio signal. The watermarked signal is in the form of noise in spread spectrum technique such that the intruder cannot detect the signal. The watermarked signal is transmitted at 1800 MHz because transmission at 1800 MHz band is licensed for low power transmission. It is concluded that transmitting the signal at 1800 MHz consumes low power than transmitting the signal without any filter. Usually power consumption is increased by adding a component (filter), but using a filter to transmit the signal at 1800 MHz consumes low power than without using a component (filter). Analyzing the power consumption for the FPGA based implementation is one of the most important factors. The power consumption of CSS based audio watermarking is analyzed with the help of Xilinx power analyzer in Xilinx ISE 12.1.

The power consumption of CSS technique is tested for the different frequencies and it’s shown in Fig. 5. While comparing the power consumption of proposed CSS based robust audio watermarking with various frequencies from

Fig.5. We can conclude that, the watermark ed signal at 1800 MHz consumes less power than other frequencies.

C. Imperceptibility of CSS based Audio Wate rmarking

Imperceptible audio watermarking hel ps to prevent the intruder from detecting the signal. The power spectral density plays a major role in audio watermarking. T he power spectral density describes how the power of the si gnal is distributed with frequency. By lowering the power spectral density (PSD), It is possible to hide the transmi tting signal, thus making it extremely difficult to detect, this is termed as Low Probability of Detection/Intercept (LPD/LPI) [1]. The main advantage of the spread spectrum water marking technique is the low power spectral density. Transmit ting the watermarked signal with low PSD provides very good resistance to eavesdropping. Due to this adv antage the spread spectrum is widely used in military, in dustrial, avionics, scientific and civil to provide the hidden com munication.

The power spectral density explains ho w the power of the signal is distributed with frequency. Hence the PSD of a transmitted watermarked signal helps to measures, the distribution of the signal power, with a fr equency. The low power spectral density of a watermarked sig nal provides Low Probability of Intercept (LPI), which hel ps to prevent the intruder from detecting the transmitted sig nal (watermarked signal). Hence low power spectral density helps to achieve good imperceptibility by preventing the intruder from detecting the message, which is in needed to be transmitted secretly. The PSD of the transmitted waterm arked signal with filter (1800 MHz) and without filter is an alyzed by giving different input signals to CSS based audio watermarking and the results are shown in Fig. 4. Fig. 4 shows that, transmitting the watermarked signal at 1800 MHz achiev es low PSD when compared with the transmission of waterm arked signal with filter.

The output of chirp spread spectrum is shown in Fig. 5. The message signal (watermark message) is show n in Fig. 5a. The watermark message is the message which is needed to transmit secretly to the receiver side. This CSS techniques uses chirp signal as a carrier for hiding the hidden (secret message) information. The message is transmitted as a noise to the receiver after the modulated message signal is multiplied by the chirp signal– secret key. This CSS techniques uses chirp signal as a carrier for the data hiding (secret message) information. The noise signal is shown in the Fig. 5b. Since the 1800MHz is licensed for low power transmission, the noise signal is transmitted and received at 1800 MHz. In order to retrieve the message, the receiver should know the secret key which is used at the transmitter side. The detected watermark message is shown in Fig. 5c. This implementation of CSS in the system generator can be converted into VHDL code using the Xilinx system generator token for the FPGA implementation of audio watermarking.

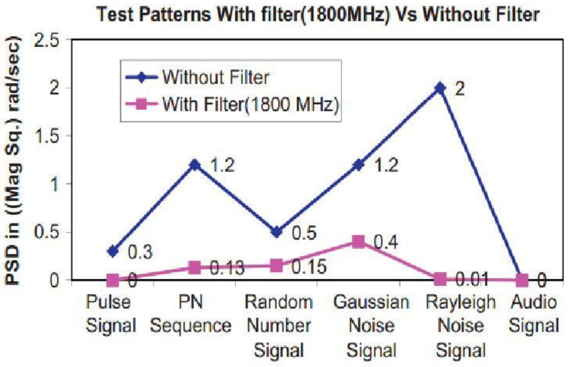

Fig.4.PSD for different test patterns with filter (1800 MHz) vs. without filter

Fig. 5. Chirp spread spectrum outputs

The low PSD provides LPI, which helps to prevent the Intruder from detecting the watermarked signal. The audio signal is modulated and multiplied with the chirp signal-secret key which produces the noise spread spectrum is shown in (watermark message) is show message is the message which the receiver side. This CSS the carrier for hiding the hidden The message is transmitted as modulated message signal is m secret key. This CSS technique for the data hiding (secret me signal is shown in the Fig. 5b. for low power transmission, the received at 1800 MHz. In receiver should know the sec transmitter side. The detected w Fig. 5c. This implementation o can be converted into VHDL generator token for the FPG watermarking.

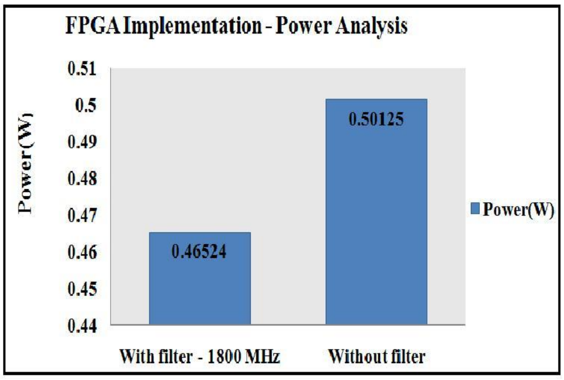

Fig. 6. FPGA Implementation – Power Analysis

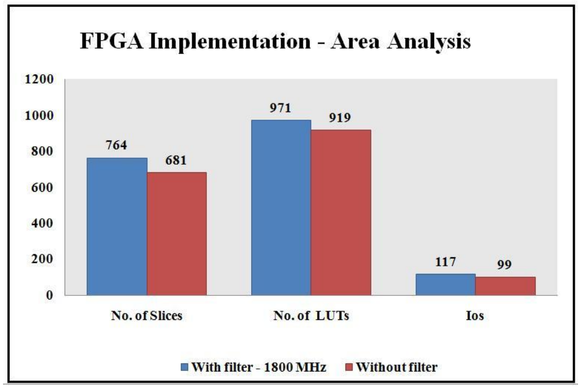

Fig. 7: FPGA Implementation – Area Analysis

Hence the converted code can be synthesized in Xilinx ISE, thus the CSS can be generated.The power and the area reports are tabulated by synthesizing and translating the generated code in Xilinx ISE is shown in Fig.6 and Fig. 7. The comparison of power at different frequencies is shown in Fig. 8.

D. Robustness of CSS based Audio Watermarking

An audio watermarking is said to be robust, if it resists any transformation in the message signal. To check the robustness of the audio watermarking technique, the performance of the watermarking technique should be analyzed in the presence of the standard watermarking attacks. One of the standard watermarking attacks is noise addition attack.

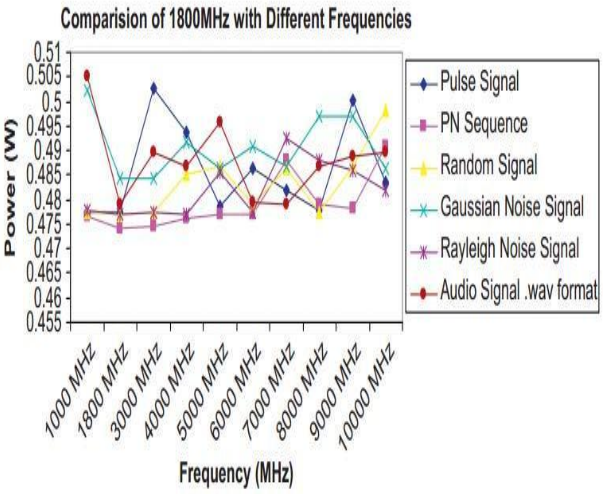

Fig. 8.Frequency Vs. Power (W)

The robustness of the proposed technique is determined by giving real time audio signal (.wav) as an input to the CSS based audio watermarking with noise addition attack and the results are shown in Fig. 9. The acceptable PSNR values for wireless transmission quality loss are considered to be about 20–25 dB. The Peak Signal to Noise Ratio plays the most important role in transmitting the signal to receiver. It is used to evaluate the quality of watermarked signal.

$$PSNR = 10\log_{10}\frac{X^{2}peak}{\sigma_e^{2}} \qquad (5)$$

The PSNR for the detected watermark signal from the attacked watermarked signal is 53.67. From Fig. 9, it is concluded that the watermark (message) signal is detected from the attacked signal. In CSS based audio watermarking, the watermarked signal is transmitted as noise. So, though the channel noise is added with the watermarked signal, the receiver can retrieve the signal with the help of a secret key. Hence the CSS based audio watermarking provides good robustness by detecting the message (watermark) signal from the attacked signal.

E. Performance Evaluation of CSS based Robust Audio Watermarking.

The watermark is undetectable to a listener or viewer. This ensures that the quality of the host (or) Original audio signal is not perceivably distorted, and does not indicate the presence or location of a watermark. So the quality of the watermarked signal is evaluated in terms of Signal to Noise Ratio (SNR).Which is measured by the equation (6). The robustness of the Scheme can be increased up to certain level by selecting longer audio files or embedding the watermark signal multiple times. It is observed that SNR values depend on types of the music or songs. CSS based audio watermarking gives improved SNR as compared to traditional watermarking methods.

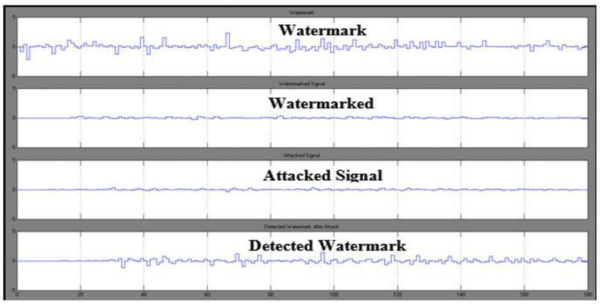

Fig. 9. Noise addition attack.

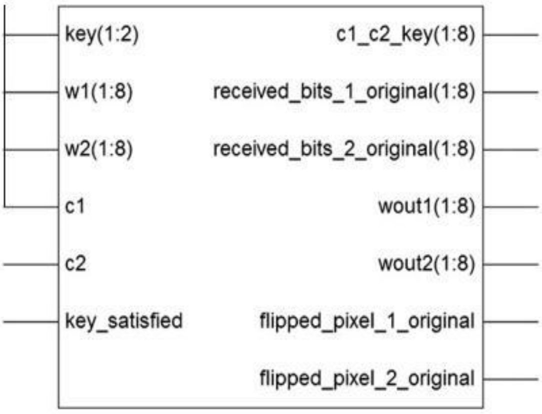

Fig.10. Pin Diagram of Proposed Watermarking algorithm using EDA Tool.

$SNR = {}^{10\log}10\ \{\sum_{n-1}^{N} w(n)^{2} / \sum_{n}^{N} -_{1[w(n)\ -\ w\ *\ (n)]}2\ \}$......(6)

Where w (n) – Original Audio Signal (or) Host signal. W*(n) – Watermarked Audio Signal.

F. Area Analysis of CSS based Audio Watermarking

The tradeoff between the power and area for different test input signals is shown in Table 1. Hence the CSS based audio watermarking can achieve low power by trading the area.

TABLE I
Trade off between power and area

S.no	***Experimental inputs***	***Power reduced (%)***	***Area increased (%)***
1	Pulse signal	4.90	5.46
2	PN sequence	5.19	
3	Random signal	0.01	
4	Gaussian noise signal	1.55	
5	Rayleigh noise signal	4.59	
6	Audio signal	4.07	

VI. CONCLUSION

A novel FPGA based Robust audio watermarking chip using chirp spread spectrum (CSS) audio watermarking technique is proposed in this paper. This technique provides covert communication with 4.07% reduction in power consumption. Hence by transmitting the watermarked signal at 1800 MHz with the help of a band pass filter, consumes low power than by transmitting the signal without any filter whereas the area is increased. Thus this paper presents a new concept of performing a robust audio watermarking using chirp spread spectrum techniques. By implementing the audio watermarking in a chip, helps to integrate with an existing audio devices.

The proposed CSS based Robust audio watermarking provides good robustness hence it is concluded that the proposed CSS based audio watermarking provides low power, good imperceptibility and robustness, which is used for the development of militaries, wireless communication and RADAR.

ACKNOWLEDGMENT

The authors would like to thank firstly, our GOD, and all friends who gave us any help related to this work and the most thank is to our families and to our country INDIA which born us. The authors would also like to acknowledge the Anna University, Regional Centre, Coimbatore for providing us with all the tools and the necessary support to carry out the work successfully.

REFERENCES

[1] P.Karthigaikumar, K.Jaraline Kirubavathy, K. Baskaran, FPGA based audio watermarking—Covert communication, Microelectronics Journal, 2011, pp. 778–784.

[2] D. Mukhopadhyay, A. Mukherjee, S. Ghosh, S. Biswas, P. Chakraborty, An approach for message hiding using substitution techniques and audio hiding in steganography, IE(I) Journal CP 86 (2005) ,pp.41–44.

[3] Elias Kougianos, Saraju P. Mohanty, Rabi N. Mahapatra, Hardware assisted watermarking for multimedia, special issue on circuits and systems for real- time security and copyright protection of multimedia, International Journal on Computers and Electrical Engineering 35 (2) (2009), pp. 339–358.

[4] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM System Journal 35(1996) ,pp.313–335.

[5] Cvejic Nedeljko, Algorithms for audio watermarking and steganography, Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu, 2004.

[6] A. Springer, W. Gulger, M. Huemer, L. Reindl, C.C.W. Ruppel, R. Weigel, Spread spectrum communication using chirp signals, in: Proceedings of EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security, IEEE/ AFCEA, 2000, pp. 166–170.

[7] Fernando Perez-Gonzalez, Juan R. Hernandez, "A Tutorial on Digital Watermarking", In Proc. of the 33rd IEEE annual carnahan conference on security technology, madrid, Spain, October 1999.

[8] Dr. K. Gopalan, "Information Hiding in audio signals for watermarking, steganography and covert communication application", in ISSNIP, Vol 3, issue 1, July 2009.

[9] John V. Lampe, "Chirp spread spectrum for real time

[10] locating systems" from Nanotron technologies GmbH, Presented to ISO SC31 WG5, VP business development, Co-Technical editor IEEE 802.15.4a.

[11] John V. Lampe, Chirp spread spectrum for real time locating systems from Nanotron technologies GmbH, Presented to ISO SC31 WG5, VP Business Development, Co-Technical editor IEEE 802.15.4a, June 2005.

[12] A. Springer, W. Gulger, M. Huemer, L. Reindl, C.C.W. -Ruppel, R. Weigel, "Spread spectrum communication using chirp signals", EUROCOMM 2000, Information systems for enchanted public safety and security, 2000, pp 166- 170.

[13] John Pinkney, "Low complexity indoor wireless data links using chirp spread spectrum", Ph.D. Thesis, University of Calgary, December 2003.

[14] Bender. W, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM System Journal Vol.3, No.42, pp. 313–335,1996.

[15] Herbert Taub, Donald Schilling, Principles of Communication Systems, second ed., Tata McGraw-Hill Publishing Company Limited, 1991.