TRANSPARENT AUDIO WATERMARKING USING FIBONACCI SERIES USING IMAGE ENCRYTION

[1]Vijetha Kura, [2]Buchhibabu Rachakonda
[1]Assistant professor, [2]Student
[1,2]Electronics and communication department,
[1,2]Matrusri engineering college, Hyderabad, India

Abstract: This paper will present a audio watermarking method which is highly secured and offers triple layer protection and has very large virtual capacity and large imperceptibility in which watermark/data i.e. an image can be encrypted and hidden by modifying the magnitude values in FFT spectrum. The main idea is to modify magnitude of FFT samples with respect to Fibonacci series .Here an image will be encrypted and is embedded into audio which improves the security of watermarking drastically. XOR sum of image bits and PN sequence is used as embedding bit stream and is chosen as it is fastest and simple in computation when compared to other encryption techniques. XOR sum creates a huge virtual increase in payload or capacity of the algorithm. This technique mathematically proves that maximum changes in FFT samples is less than 61% and the average error rate considering a single sample is 25% .This technique is not only robust and transparent but also highly secured. The additional feature is its ability to handle large capacity i.e. from experimentally its proved to handle 700bps to 3kpbs efficiently, moreover this technique is blind, i.e. original signal is not required near receiver.

***Index Terms*: Audio watermarking, FFT, Image encryption, PN sequence, XOR sum.**

I. INTRODUCTION:

In this progressive era in which everything changes faster than the prick of the eye, inventions followed by exploitation of its weakness is a casual scenario. One of the important affected field is digital audio. As distribution of audio has became very easy, which paved way for illegal distributions by which huge intellectual scholars, authors suffered heavy losses due to copyright infringements by illegitimate methods followed by criminals.

Digital watermarking is a simple process in which a watermark which can be audio/Image can be embedded into the host signal and can be later extracted and used for multiple purposes.Audio watermarking has four different significant properties.

1. Imperceptibility: It is defined by the quality of the embedded signal i.e after adding watermark in terms of objective and subjective measures.
2. Security: The basic theme of the security is it should broadcast any clue from the embedded signal. Security of a watermark defines how well it is ready to face different attacks. The stronger the encryption the stronger is the security.
3. Robustness: Robustness of and audio watermarking is defined by its ability to withstand different types of attacks on embedded signal.
4. Payload: Here the payload is simply watermarking bits .It’s usually measured in bps i.e. bits per second. The payload can be defined as the number of bits that can embedded into host audio signal without losing significant imperceptibility of the audio.

There are different techniques available which includes D.C.T [30],D.W.T [16],M.D.C.T [29], and D.W.T-D.C.T [28] in which imperceptibility and reduction of noise are considered as main theme. This paper considers all properties i.e. imperceptibility, security, robustness and payload and stands at the center of the tradeoff triangle.

Watermark can be embedded using different techniques.

1) Time domain
2) Frequency domain

Watermark can be embedded in frequency domain using different transforms i.e.FFT, DCT ,MDCT , DWT,DWT-DCT etc. out of which FFT is simple in complexity and fastest out of them. One of the added advantage of FFT is its translation invariant property.

II. LITERATURE SURVEY

2.1 Fibonacci series:

Fibonacci series origin takes place us to a scenario when Leonardo Fibonacci was resting in a garden and watching rabbits, wondering how many rabbits would be born in future if two rabbits mate and multiplication take place into their next generation.

This wonder number has distinguished qualities which has multiple applications which include apple design logo,Benz logo .Our ear has a unique shape which can be attributed to Fibonacci series.

All this logos and different designs are designed using golden ratio i.e.1.618, if two numbers/Quantities are defined are golden ration if their ratio is equal to the sum of the quantities to larger quantities.

2.2 Image encryption:

There are different types of image encryption process available for different purposes. Some of the famous techniques are chaotic image encryption, rubics cube based image encryption , steganography and many more out of which encrypting with PN sequence is simpler and faster one. As our main concern is to provide good security with fast computation encryption with PN sequence is chosen.

Stenography is the art of hiding information in a image, this can be done by varying the gray values of the original image and then encrypting the information in it. Now a days it is popular because of its robustness. Image encryption can be of three types i.e.block permutation, pixel permutation and bit permutation In block permutation image is divided into multiple parts and they are permutated with proper techniques and they are inserted embedded into host signal.

In pixel permutation the image pixels are permutated with a secret key and them embedded in the host signal .This method is widely used due to its robustness and high fidelity. In bit permutation bits are permutated and then embedded into host signal, this method is highly reliable due its complexity to decrypt compared to others. In this paper first the pixel gray value are noted down and then converted into bits, Then XOR sum of grey values and pseudo-random bit stream is generated. A simple XOR of watermark bits and PN sequence would produce same number of watermark bits as original but XOR sum of watermark bits and PN sequence would reduce drastically, the total number of watermark bits present after encryption when compared to initial watermark bits available. This helps in increasing the payload or capacity of the audio watermarking without a significant side effects.

This generated bit stream is embedded into different frames of FFT coefficients that are created after choosing requiredparameters (frame size and bandwidth). The FFT co-efficient are manipulated or changed w.r.t Fibonacci numbers and the bit that is going to get embedded. This is main principle of embedding bits.

2.3 Typical maximum distortion proof

Consider a, b (a>b)

Then these two quantities are said to be in golden ratio if

(a+b)/a = a/b

Proofs:

Theorem 1: The typical maximum distortion that gets embedded in the FFT samples (magnitude) using this algorithm is between the span of 0.38 to 0.61

Proof: if ‘l’ is converted to Fn+1

Then Max error rate = Max error / Fn+1

=(Rn-1)Fn/Fn+1

=(Rn-1)Fn/rnFn

=Rn-1/Rn

If ‘l’is converted to Fn

Then Max error rate =Max error/Fn=Rn-1

Here, If we assume the general /typical value of Rn it is i.e golden ratio the max error would be between 0.38-0.61.

Therefore maximum change in FFT is less that 61 %

It also indicates that the maximum error rate is 0.50.

Now if we consider that fft values have equal probabilities then the average error rate is 0.25 which indicates the average change per fft value is 25% only.[27]

Therefore it has good imperceptibility

2.3 Tuning:

The quality of watermarked audio is decided by few parameters i.e. Objective degradation (ODG) , BER (Bit error rate) , payload (capacity) .,etc.

The parameters can be varied to required values by altering two characteristics of the algorithm i.e frequency bandwidth (Fl,Fh) and frame size (d).

Fl – Lower frequency limit

Fh – Higher frequency limit (default value of fl=12 kHz and fh=16 kHz and d=5(samples) is considering Human auditory response).

The default value can be as low as 10 kHz considering Human auditory response, similarly 16 kHz is an average peak frequency in most of the audios.

Initially by setting default parameters we should vary the characteristics as per our requirements .If we look carefully we can observe that all the parameters are interlinked to each other. This indicates the tradeoff triangle .Security, functionality, imperceptibility are the three corners of the tradeoff triangle. This trade of triangle is limited only to certain frequency bands and frame sizes,i.e. varying them smartly we can overcome the inefficiency in tradeoff triangle.

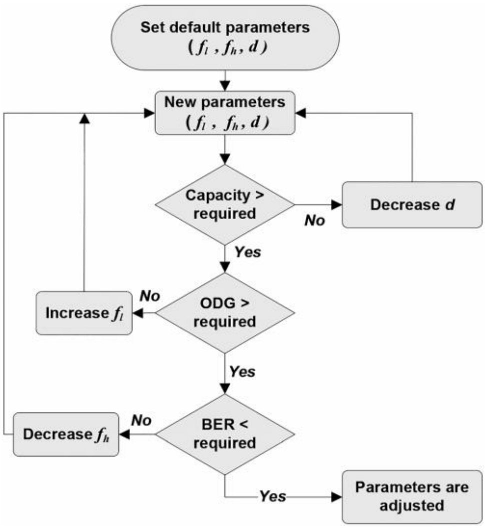


Fig 1 Tuning parameters

2.4 XOR: XOR is a bit wise operation that can be performed only on binary numbers. XOR is mainly used in encryption due to its unique this property: If, A^B=C, then C^B=A
XOR truth table:

A	B	A^B	(C=A^B)
1	0	1	
0	1	1	
1	1	0	
0	0	0	

C	B	C^B	(A=C^B)
1	0	1	
1	1	0	
0	1	1	
0	0	0	

2.5XORsum*:* XOR sum is successive XOR operations on integers until the last given integer mentioned.
XOR sum of A, B, C, D is A^B^C^D
Ex:
XOR sum of 1 to N
Let N =5
First we must convert all the integers from 1 to 5 into their binary representation.
The largest term i.e. 5 = 101 has three digits in it,so we must represent all the integers in 3 digit binary form
1 = 001
2=010
3=011
4=100
5=101
XOR sum is 1^2^3^4^5
1^2 = 001^010= 011
Similarly
(1^2)^3= 011^011=000
(1^2^3)^4= 000^100= 100
(1^2^3^4)^5 = 100^101= 001
Therefore the XOR sum of 1 to 5 is 001

The key observation is XOR sum of 5 successive digits in 3 digit binary representation is also 3 digits. This is used as key applications in many applications.

2.6 PN sequence:

PN sequences are set of bits which looks like random but has a definite relationship between them. This relation reoccurs and continues till infinity. Most of the time PN sequence is considered as random noise.

PN sequence is generated using linear feedback shift register. Linear feedback register along with a simple shift register will produce a series of pseudorandom bits which can be used for multiple applications mostly security.

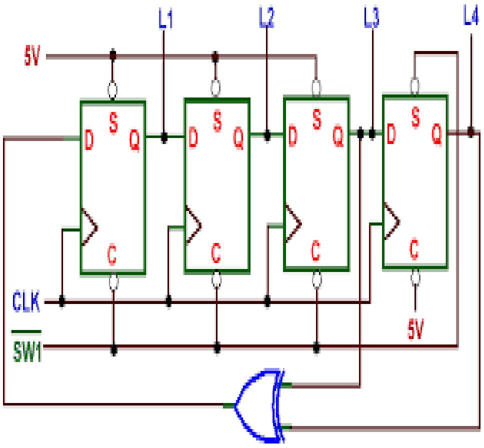


Fig 2 PN sequence generator

PN sequence of required length can be generated using Matlab.

III. PROPOSED:

This paper is extension to audio water marking using Fibonacci series [27] .Here instead of embedding simple bits we are embedding an image into the audio (Encrypted image).

This is achieved by first encrypting the image with PN sequence generated by PN generator (PNRG) i.e. XOR sum of image bits and pseudo random bit stream and embedding them into frames that are obtained after applying FFT to original audio. By using XOR sum the payload or capacity can be increased drastically.

3.1 Image Encryption

Fig 3.1 shows a rose image which we are going to modify and embed into host audio signal .Encryption key represents PN sequence that we are going to use. The below image is of 128*128 matrix similarly PN sequence is generated which is length 128*128 and they are arranged in 128*128 fashion as shown in figure (i.e. 128 numbers in a row of total 128 rows present) .

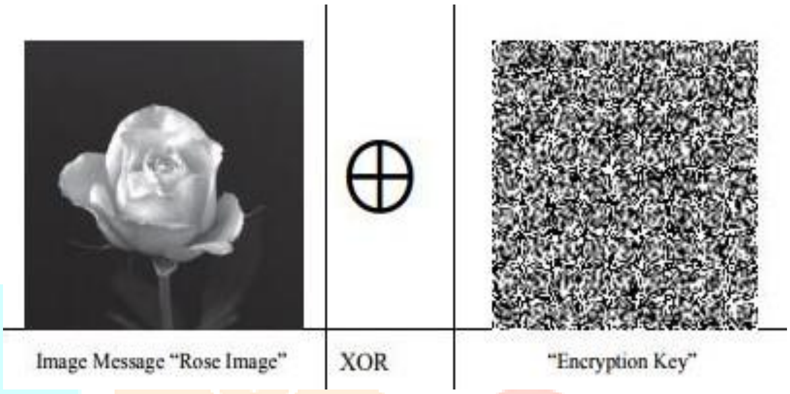


Fig 3 Xor of rose image and PN sequence (encrytpion key)

1) Rose image gray values are converted into its binary form(Matrix 1)
2) PN sequence values are converted into its binary form(Matrix 2)
3) Now XOR is applied to these matrixes , i.e Matrix 1 and Matrix 2
   Let P be Matrix 1 and Q be Matrix 2
   Now P^Q = R (Matrix 3)
   Below figure represents Encrypted image i.e. matrix 3

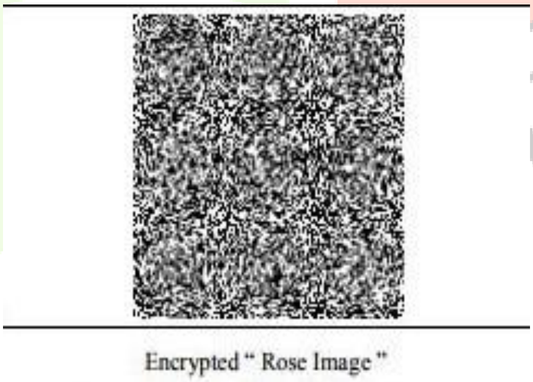


Fig 4 Encrytped rose image obtained after XOR operation done of rose image and encrytion key

Now XOR sum of this encrypted values is calculated. 'This XOR sum is embedded into the audio'. To decrypt the image the receiver must have information about

1) Seed of PN sequence
2) Encrypted gray values or Encrypted Image.

This method is adapted because it creates a very high virtual imperceptibility and payload or capacity as we are just embedding the XOR sum instead of whole image.

Watermarking using Fibonacci series has a huge payload of 700 to 3Kbps [27] but by using above method that is by embedding sum we have designed a very high capacity and high imperceptivity audio watermarking algorithm

Here we can encounter very less degradation of noise as we are embedding very less bits compared to other watermarking techniques which does not use XOR sum to embed data[1-30].

3.2 Watermarking process

The audio watermark that to be embedded must be available in binary form

3.2.1Encryption:

1) First the frame size and frequency band length will be sent toreceiver securely.

2) Convert the given audio into frequency domain signals,i.e. by applying FFT

3) Now select the coefficients which falls between the selected frequency band.(Fl, Fh)

4) The above step can be achieved using different bandpass filters

5) Afterfiltering,divide the coefficients into numerous frames

6) The size of the frame is 'd'.

6) The Fibonacci series we use in this process doesn't consist of 0 and 1.

Fk={1,2,3,5,8,13,21,34,55,…}

Here k=1, 2, 3, 4, 5,… n.

7) Now add the watermark signal to the FFT co-efficient according to Fibonacci numbers and bit that to be embedded.

8) Selected two largest Fibonacci numbers between which our FFT coefficient resides.

9) Watermark is embedded using these formulae:

f ' = fib(k,i) , if k modulus 2=0 and wl=0
fib (k+1,i) , if k modulus 2 =1 and wl=1
Similarly
f' = fib(k+1,i) , if k modulus 2 =1 and wl=1
fib (k,i) , if k modulus 2 =1 and wl=1

Here k represents kth Fibonacci number

10) Repeat the same process to all the FFT coefficients in the frame

11) Continue this process to all the frames available.

12) Finally apply IFFT

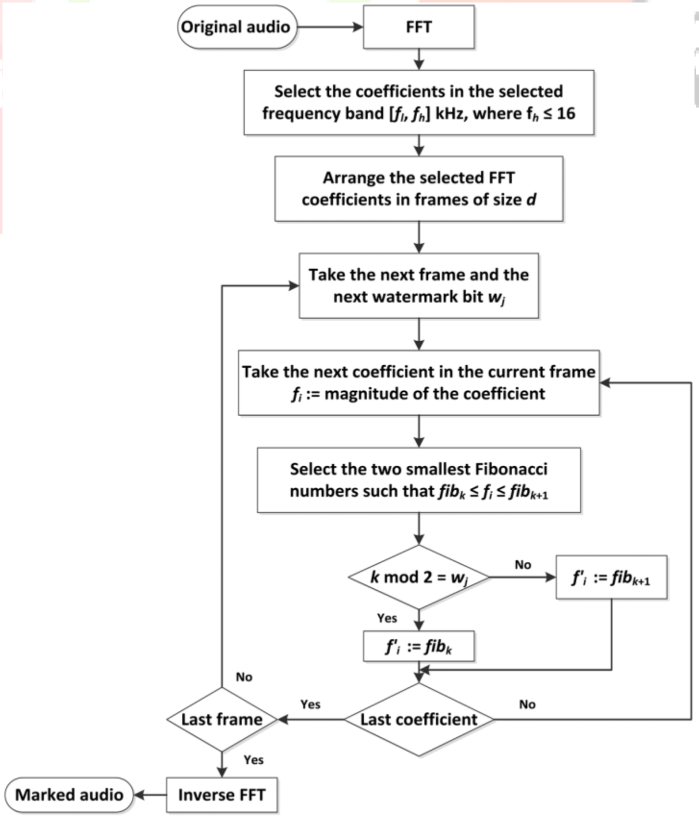

Original audio
FFT
Select the coefficients in the selected frequency band [f_l, f_h] kHz, where $f_h \leq 16$
Arrange the selected FFT coefficients in frames of size d
Take the next frame and the next watermark bit w_j
Take the next coefficient in the current frame f_i := magnitude of the coefficient
Select the two smallest Fibonacci numbers such that $fib_k \leq f_i \leq fib_{k+1}$
k mod 2 = w_j
No
$f'_i := fib_{k+1}$
Yes
$f'_i := fib_k$
No
Last frame
Yes
Last coefficient
No
Yes
Marked audio
Inverse FFT

Fig 5Encryption flowchart

3.22 Extracting /Decrypting:

1) Apply FFT to watermarked signal as the operations are to performed in frequency domain.

2) Divide the samples with given frame size d

3) Now change the FFT magnitude of given samples approximating to Fibonacci series according to given formulae

4) Formula: D(i)= 0 , if k modulus 2 = 0

1, if k modulus 2 =1

5) Now by polling method we can decide whether it is 1 or 0 , if the number of samples found to be zero out of half of the samples present in the frame , Then it is considered as 0 else 1 .

Considering there are 6 FFT coefficients in a frame and 4 of the FFT coefficients when decoded gives zero then the water bit embedded in the frame is ‘0’.

6) Now re-frame the encrypted image by using the extracted watermark bits

7) Now to decrypt the encrypted image that we already have, we will calculate the XOR sum near receiver side and compare it with one embedded into host signal.

8)Now decrypt the image by using PRNG i.e. XOR sum (same method), the decryption cannot be done without the seed of XOR

9) We will get the decrypted image as output

.

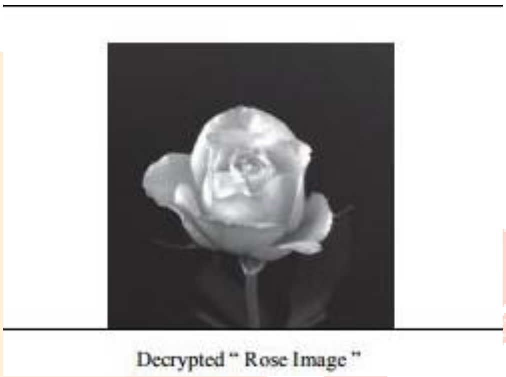


Fig 6, it represents the decrypted image that we imbedded initially (Without any attacks)

IV. EXPERIMENTS RESULTS:

4.1 Transparency, Robustness, capacity, security:

Signal to noise ration and ODG is used to measure imperceptibility, i.e. greater the SNR greater the imperceptibility similarly if ODG=0 ODG (Objective degradation).it indicates that there is no degradation, if ODG=-4 then it indicates very annoying distortion is present in the watermarked signal.

Similarly SDG (Subjective degradation) is five-point subjective grade i.e. if S.D.G =1 it is excellent and if S.D.G =1 it’s ridiculous

BER (Bit error rate):%BER = Number of error bits / Total number of bits

The first layer of security in this algorithm is its frame size and frequency band length,without knowing these two parameters it is merely impossible to decrypt the watermark.

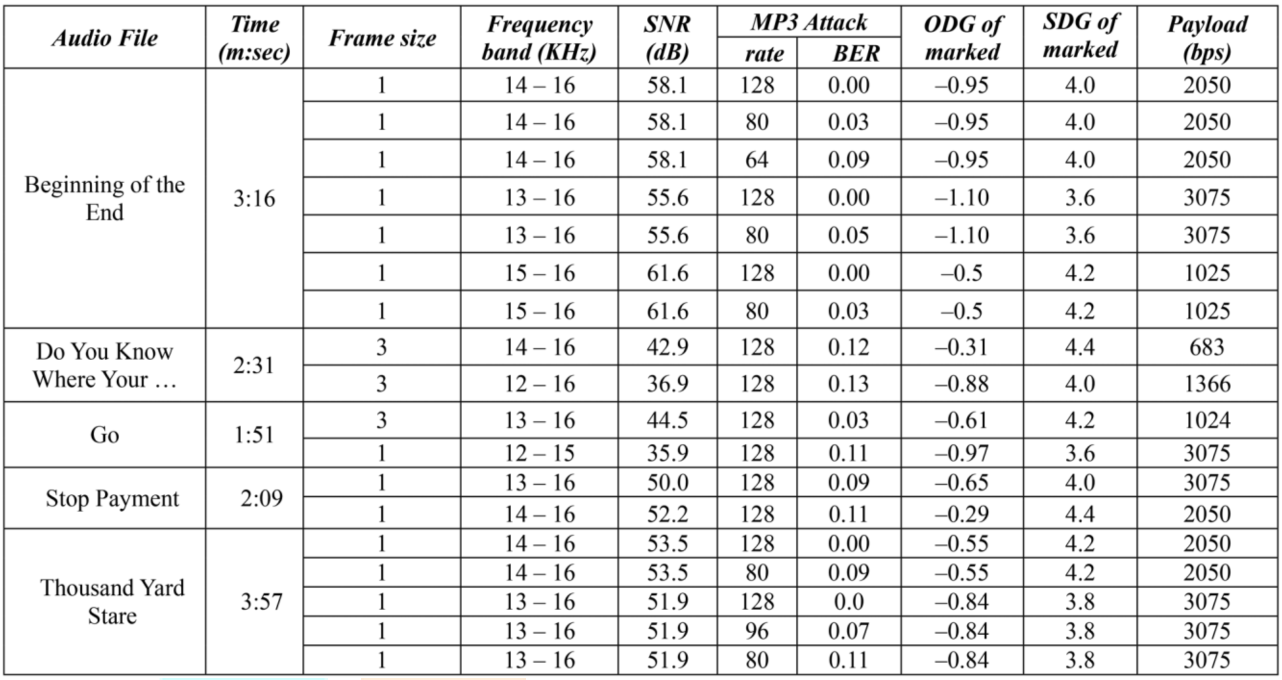
The second layer of security is the seed of PNRG that is required at both at sender and receiver end without which decryption would be practically impossible. The third layer of security is XOR sum embed into it,i.e.

The embedding rate or capacity can be increased by either increasing the frequency bandwidth (Fl,FH) or decreasing the frame size.

Aftermath has little side effects as some of the security is sensitive to certain attacks if frequency bandwidth is significantly increased.

Below table shows the trade between capacity, transparency and frame size which decide the quality of encryption.

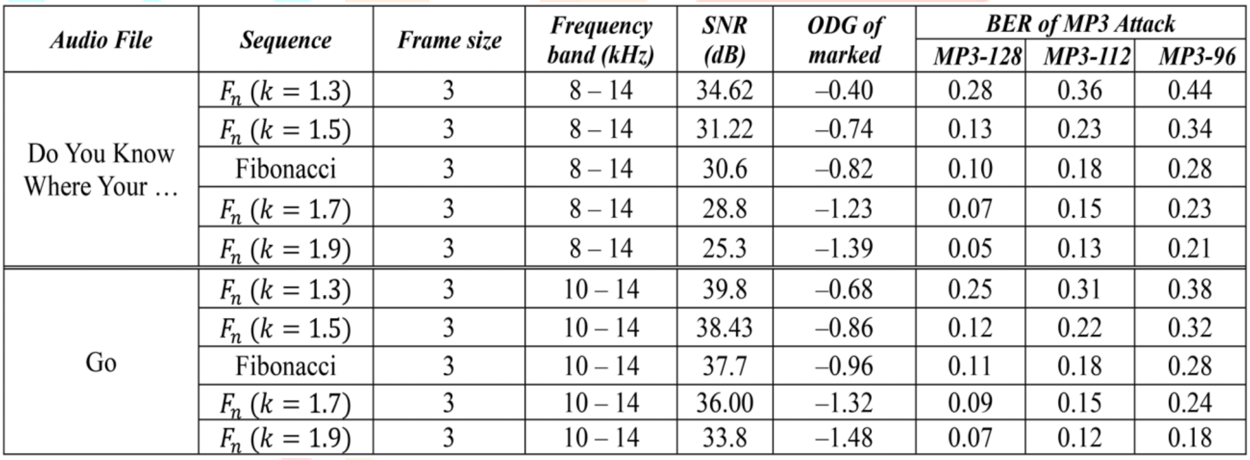
Table 4.1 Results of 5 Mono signals



Audio File	*Time (m:sec)*	*Frame size*	*Frequency band (KHz)*	*SNR (dB)*	*MP3 Attack*		*ODG of marked*	*SDG of marked*	*Payload (bps)*
					rate	*BER*			
Beginning of the End	3:16	1	14 – 16	58.1	128	0.00	–0.95	4.0	2050
		1	14 – 16	58.1	80	0.03	–0.95	4.0	2050
		1	14 – 16	58.1	64	0.09	–0.95	4.0	2050
		1	13 – 16	55.6	128	0.00	–1.10	3.6	3075
		1	13 – 16	55.6	80	0.05	–1.10	3.6	3075
		1	15 – 16	61.6	128	0.00	–0.5	4.2	1025
		1	15 – 16	61.6	80	0.03	–0.5	4.2	1025
Do You Know Where Your …	2:31	3	14 – 16	42.9	128	0.12	–0.31	4.4	683
		3	12 – 16	36.9	128	0.13	–0.88	4.0	1366
Go	1:51	3	13 – 16	44.5	128	0.03	–0.61	4.2	1024
		1	12 – 15	35.9	128	0.11	–0.97	3.6	3075
Stop Payment	2:09	1	13 – 16	50.0	128	0.09	–0.65	4.0	3075
		1	14 – 16	52.2	128	0.11	–0.29	4.4	2050
Thousand Yard Stare	3:57	1	14 – 16	53.5	128	0.00	–0.55	4.2	2050
		1	14 – 16	53.5	80	0.09	–0.55	4.2	2050
		1	13 – 16	51.9	128	0.0	–0.84	3.8	3075
		1	13 – 16	51.9	96	0.07	–0.84	3.8	3075
		1	13 – 16	51.9	80	0.11	–0.84	3.8	3075

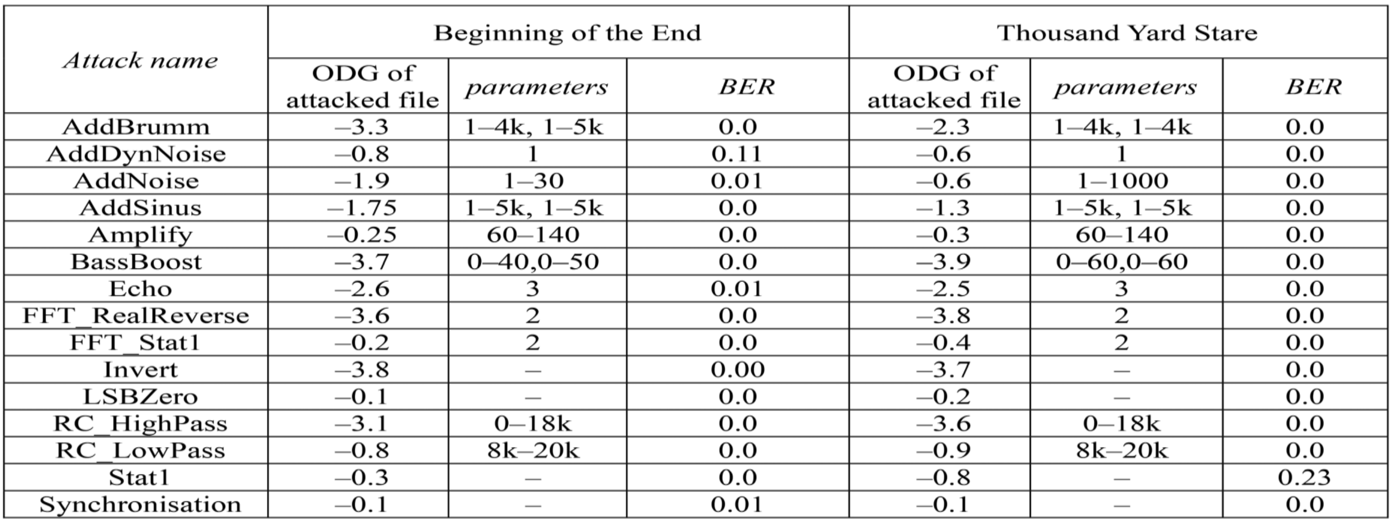
Below table indicates the reason why we have chosen only Fibonacci series in this encryption algorithm.

Table 4.2 Comparisons between different series that are generated with different k values (K- ratio)



Audio File	*Sequence*	*Frame size*	*Frequency band (kHz)*	*SNR (dB)*	*ODG of marked*	*BER of MP3 Attack*		
						MP3-128	*MP3-112*	*MP3-96*
Do You Know Where Your …	F_n $(k = 1.3)$	3	8 – 14	34.62	–0.40	0.28	0.36	0.44
	F_n $(k = 1.5)$	3	8 – 14	31.22	–0.74	0.13	0.23	0.34
	Fibonacci	3	8 – 14	30.6	–0.82	0.10	0.18	0.28
	F_n $(k = 1.7)$	3	8 – 14	28.8	–1.23	0.07	0.15	0.23
	F_n $(k = 1.9)$	3	8 – 14	25.3	–1.39	0.05	0.13	0.21
Go	F_n $(k = 1.3)$	3	10 – 14	39.8	–0.68	0.25	0.31	0.38
	F_n $(k = 1.5)$	3	10 – 14	38.43	–0.86	0.12	0.22	0.32
	Fibonacci	3	10 – 14	37.7	–0.96	0.11	0.18	0.28
	F_n $(k = 1.7)$	3	10 – 14	36.00	–1.32	0.09	0.15	0.24
	F_n $(k = 1.9)$	3	10 – 14	33.8	–1.48	0.07	0.12	0.18

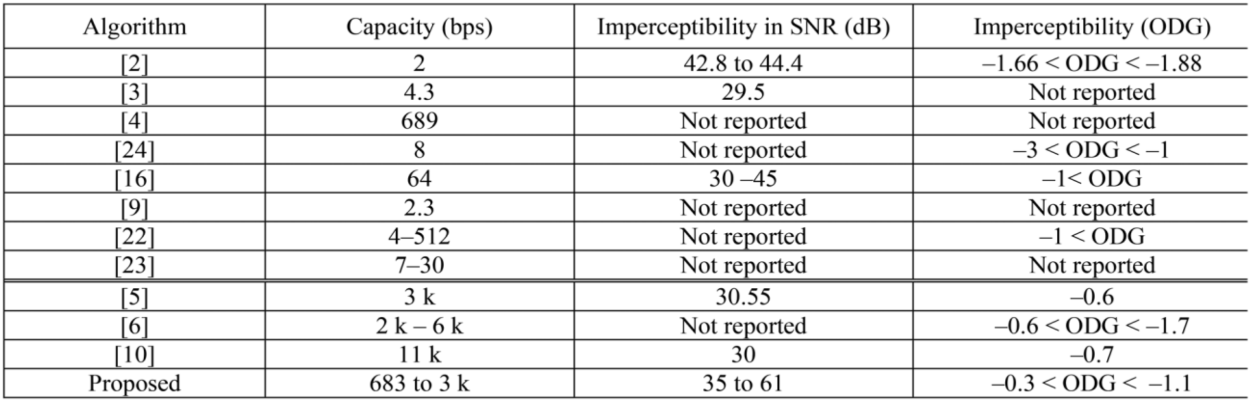
Table 4.3 represents different types of attacks and different parameters which defines robustness of embedded signal



Attack name	Beginning of the End			Thousand Yard Stare		
	ODG of attacked file	*parameters*	*BER*	ODG of attacked file	*parameters*	*BER*
AddBrumm	–3.3	1–4k, 1–5k	0.0	–2.3	1–4k, 1–4k	0.0
AddDynNoise	–0.8	1	0.11	–0.6	1	0.0
AddNoise	–1.9	1–30	0.01	–0.6	1–1000	0.0
AddSinus	–1.75	1–5k, 1–5k	0.0	–1.3	1–5k, 1–5k	0.0
Amplify	–0.25	60–140	0.0	–0.3	60–140	0.0
BassBoost	–3.7	0–40,0–50	0.0	–3.9	0–60,0–60	0.0
Echo	–2.6	3	0.01	–2.5	3	0.0
FFT_RealReverse	–3.6	2	0.0	–3.8	2	0.0
FFT_Stat1	–0.2	2	0.0	–0.4	2	0.0
Invert	–3.8	–	0.00	–3.7	–	0.0
LSBZero	–0.1	–	0.0	–0.2	–	0.0
RC_HighPass	–3.1	0–18k	0.0	–3.6	0–18k	0.0
RC_LowPass	–0.8	8k–20k	0.0	–0.9	8k–20k	0.0
Stat1	–0.3	–	0.0	–0.8	–	0.23
Synchronisation	–0.1	–	0.01	–0.1	–	0.0

Below table show comparison of different methods

Table 4.4 Comparisons between different methods



Algorithm	Capacity (bps)	Imperceptibility in SNR (dB)	Imperceptibility (ODG)
[2]	2	42.8 to 44.4	–1.66 < ODG < –1.88
[3]	4.3	29.5	Not reported
[4]	689	Not reported	Not reported
[24]	8	Not reported	–3 < ODG < –1
[16]	64	30 –45	–1< ODG
[9]	2.3	Not reported	Not reported
[22]	4–512	Not reported	–1 < ODG
[23]	7–30	Not reported	Not reported
[5]	3 k	30.55	–0.6
[6]	2 k – 6 k	Not reported	–0.6 < ODG < –1.7
[10]	11 k	30	–0.7
Proposed	683 to 3 k	35 to 61	–0.3 < ODG < –1.1

Note: The above tables are constructed with reference to [27]

Here all audio clips are sampled at 44.1 KHz with 16 bits per sample and the audio attacks mentioned above are provided by Stirmark Benchmark for Audio (SMBA)

V. CONCLUSION:

In this paper a high security, high capacity, robust, transparent, algorithm to encrypt watermark into audio is presented. The image is encrypted by generating bit stream of sum of XOR of pixel values and pseudo random sequence (generated by PRNG) and this method is blind as we do not require original signal during decryption. By using XOR sum for encryption the payload capacity is drastically increased. The two deciding factors to change the above parameters are the frame size and frequency bandwidth This paper provided proof that the maximum change of FFT samples is less than 61% but average change of a single FFT sample is just below 25%.Experimental proofs shows that this algorithm can handle capacity ranging from 700bps to 3kbps and is robust against all common signal processing attacks.

REFERENCES:

[1] M. Fallahpour and D. Megías, "Robust high-capacity audio watermarking based on FFT amplitude modification," *IEICE Trans. Inf.Syst.*, vol. E93-D, no. 01, pp. 87–93, Jan. 2010. 1282 IEEE/ACM TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING, VOL. 23, NO. 8, AUGUST 2015

[2] M. Fallahpour and D. Megías, "Secure logarithmic audio watermarking scheme based on the human auditory system," *Multimedia Syst.*, 2013, DOI: 10.1007/s00530-013-0325-1, ISSN.0942-4962.

[3] S. T. Chen, G. D. Wu, and H. N. Huang, "Wavelet-domain audio watermarking scheme using optimisation-based quantisation," *IET SignalProcess.*, vol. 4, no. 6, pp. 720–727, 2010.

[4] No, Really, "Rust," [Online]. Available: http://www.jamendo.com/en/album/7365 Jul. 17, 2014

[5] T. Thiede, W. C. Treurniet, R. Bitto, C. Schmidmer, T. Sporer, J. G.
Beerens, C. Colomes, M. Keyhl, G. Stoll, K. Brandenburg, and B. Feiten, "PEAQ - The ITU standard for objective measurement of perceived audio quality," *J. AES*, vol. 48, no. 1/2, pp. 3–29, 2000.

[6] S. T. Chen, H. N. Huang, C. J. Chen, and G. D. Wu, "Energy-proportion based scheme for audio watermarking," *IET Signal Process.*, vol. 4, no. 5, pp. 576–587, 2010.

[7] G. Hua, J. Goh, and V. L. L. Thing, "Time-spread echo-based audio watermarking with optimized imperceptibility and robustness," *IEEE/ACM Trans. Audio, Speech, Lang. Process.*, vol. 23, no. 2, pp. 227–239, Feb. 2015.

[8] R. A. Dunlap, *The golden ratio and fibonacci numbers*. Hackensack,

[9] J. Katz and Y. Lindell, "Introduction to modern cryptography: Principles and protocols," in *Chapman & Hall/CRC Cryptography and NetworkSecurity Series*. Boca Raton, FL, USA: CRC, 2007.

[10] H. J. Kim, "Audio watermarking techniques," in *Proc. Pacific Rim Workshop Digital Steganogr.*, 2005, pp. 1–17.

[11] S. Xiang, H. J. Kim, and J. Huang, "Audio watermarking robust againsttime-scale modification and MP3 compression," *Signal Process.*, vol. 88, no. 10, pp. 2372–2387, Oct. 2008.

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

[13] J. J. Garcia-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Data hiding in audio signal using rational dither modulation," *IEICEElectron. Express*, vol. 5, no. 7, pp. 217–222, 2008.

[14] M. Fallahpour and D. Megías, "High capacity audio watermarking using FFT amplitude interpolation," *IEICE Electron. Express*, vol. 6, no. 14, pp. 1057–1063, 2009.

[15] M. Fallahpour and D. Megías, "High capacity method for real-time audio data hiding using the FFT transform," in *Advances in InformationSecurity and Its Application*. Berlin, Germany: Springer-Verlag,
2009, pp. 91–97.

[16] M. Fallahpour and D. Megías, "DWT–based high capacity audio watermarking," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E93-A, no. 01, pp. 331–335, Jan. 2010.

[17] W. Li and X. Xue, "Content based localized robust audio watermarking 8, no. 1, pp. 60–69, Feb. 2006.

[18] M. Fallahpour and D. Megías, “High capacity audio watermarking using the high frequency band of the wavelet domain,” in *Multimedia Tools and Applications*. New York, NY, USA: Springer, 2011, vol.
52, pp. 485–498.

[19] M. Fallahpour and D. Megías, “High capacity robust audio watermarking scheme based on FFT and linear regression,” *Int. J. InnovativeComput., Inf. Control*, vol. 8, no. 4, pp. 2477–2489, Apr. 2012.

[20] N. K. Kalantari, M. A. Akhaee, M. Ahadi, and H. Amindavar, “Robust multiplicative patchwork method for audio watermarking,” *IEEETrans. Audio, Speech, Lang. Process.*, vol. 17, no. 6, pp. 1133–1141, Aug. 2009.

[21] X. Kang, R. Yang, and J. Huang, “Geometric invariant audio watermarking based on an LCM feature,” *IEEE Trans. Multimedia*, vol. 13, no. 2, pp. 181–190, Apr. 2011.

[21] , G. E. Bergum, Ed. *et al.*, *Applications of Fibonacci Numbers*. New York, NY, USA: Springer, 1991, vol. 4.

[22] OPTICOM OPERA software site, [Online]. Available: http://www.opticom. de/products/opera.html

[23] Stirmark Benchmark for Audio, [Online]. Available: http://wwwiti.cs. uni-[22] M. Unoki and D. Hamada, “Method of digital-audio watermarking based on cochlear delay characteristics,” *Int. J. Innovat. Comput., Inf.Control*, vol. 6, no. 3(B), pp. 1325–1346, Mar. 2010.

[24] K. Kondo and K. Nakagawa, “A digital watermark for stereo audio signals using variable inter-channel delay in high-frequency bands and its evaluation,” *Int. J. Innovat. Comput., Inf. Control*, vol. 6, no. 3(B), pp. 1209–1220, Mar. 2010.

[25] A. Nishimura, “Audio data hiding that is robust with respect to aerial transmission and speech codecs,” *Int. J. Innovat. Comput., Inf. Control*, vol. 6, no. 3(B), pp. 1389–1400, Mar. 2010.

[26] Chen, Brian, and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 14231443, May 2001.

[27] Mehdi Fallahpour and David megias “Audio watermarking using fibonacci series*”, IEEE/ACM*trascations on audio speech and language processing vol 23 ,no 8,August 2015.

[28] X. Y. Wang and H. Zhao, “A novel synchronization invariant audio watermarking scheme based on DWT and DCT,” *IEEE Trans. SignalProcess.*, vol. 54, no. 12, pp. 4835–4840, Dec. 2006.

[29] Aparna S , Bajju P S , “Audio watermarking technique using Modified Discrete Cosine Transform “ 2016 *International Conference on Communication systems and networks(ComNet)* |21-23 July 2016| Trivandrum.

*[30]*IJEDR: Volume 2, Issue, ISSN: 2321-9939: “A Study of Audio Watermarking Technique in DCT Domain” by Tejash Lad,Kaushal Doshi