ISSN 2320 -2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.11, Pages : 26-31 (2014)
Special Issue of ICCAAC 2014 - Held on December 08,2014,Hyderbad, India

Analysis of wavelet families on Audio steganography using AES

Mirza Tabinda [1], Vijaya Ahire [2]

[1] Jawarharlal Nehru College of Engineering, Aurangabad, India, mtabinda@gmail.com ,

[2] Faculty, Jawarharlal Nehru College of Engineering, Aurangabad, India Maharashtra

Abstract*:* With the growing trends in wireless network in this modern era, more and more multimedia data are generated and transmitted. So the effective ways to ensure their security are increased. This can be achieved by implementing steganography techniques. Audio steganography is more challenging compared to image or video steganography. There are number of audio steganography methods. In this paper we focus on different wavelet families for embedding secret message in audio file. The advantage of wavelet is due to its reconstruction property and its capacity of capturing the low frequency component. The wavelet families which are taken for the analysis for audio stegnography are daubechies, symlet, coiflet, biorthogonal, stationary and dmer. In addition to this secured data transfer between two parties is achieved by combining steganography with cryptography. In the proposed system first the sender encrypts the secret message by AES algorithm and secondly encrypted secret message is embedded using Wavelet families. Then the receiver performs the reverse process to get the original secret message. Here we review current and novel wavelet audio steganographic techniques and evaluate their performance based on PSNR, MSE and Entropy. This method also results in increased robustness against noise addition, random cropping and deletion of samples. In addition, listening tests showed that stego audio and original audio are imperceptible to each other.

Keywords: Audio Steganography, Wavelet families, Cryptography, Advanced Encryption Standard.

INTRODUCTION

In the today's age, digital communication plays a vital role which is distributed over internet. At the same time, data over internet has become susceptible to copyright infringement, eavesdropping, hacking etc and thus need to secure communication. For this steganogrphy is technique that hide information inside another media. The word "Steganography" is derived from Greek "Steganos" meaning hidden or concealed [1]. Thus Steganography stands for concealed [1]. Thus Steganography stands for concealed writing. Steganography is an art of hidden data or secret messages over public channel so that third party cannot detect the presence of secret messages.

Audio steganography hides data in cover speech which is imperceptible from the original audio, by the people in such a way that eavesdropper cannot detect the presence of original message. Another technique which can be implemented side by side to steganography is cryptography. Cryptography protect the information by transforming it into unreadable format in which a message can be concealed from casual reader and only the intended recipient will be able to convert it into original text [2]. Cryptography scrambles the content of data like text, images, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep data secure from unauthorized access. Steganography assures secrecy whereas cryptography assures privacy. Steganography and cryptography are both used to ensure data confidence.

Audio steganography is a challenging technique than image or video steganography due to wider dynamics range of Human Auditory System when compared to Human Visual System. In this system, steganography is compared with cryptography for better security [3].

Many techniques have been developed for hiding secret signals into other cover signals. [4] Fatiha Djebbar et al has discussed about different audio steganography techniques avalaible in different domain. In temporal domain also called as subsituition technique, LSB method is widely used. It is one of the earliest and easiest methods used in information hiding. It allows high embedding capacity for data hiding but when it comes to robustness part, reduces its performance hence vulnerable to simple attack. Rohit Tanwar et al. improves LSB method by making this substuition technique robust to various intentional that try to reveal hidden message as well as unintentional attacks like distortions with high average power [5].

ISSN 2320 -2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.11, Pages : 26-31 (2014)
Special Issue of ICCAAC 2014 - Held on December 08,2014,Hyderbad, India

The transform domain is another domain which exploits the frequency of the HAS directly by modifying only masked regions or indirectly by altering slightly the audio signals samples. Phase coding is one of the methods of temporal domain. [6] Samir Kumar el at. discuss about two methods modified LSB and Phase coding. The basic idea of phase coding is to split the original audio stream into blocks and embed the whole message data sequence into the phase spectrum of the first block. Phase coding provides with low data transmission rate as secret message is encoded in the first signal segment only and to extract the secret message from the sound file, the receiver must know the segment length. Thus it can be used when only a small amount of data needs to be concealed.

Another method for audio steganography is Discrete Wavelet Transform (DWT). Satish Singh Verma et al. proposed a high capacity and high stego-signal quality method based on samples comparison in DWT domain where selected coefficient of a segment value is changed by a threshold value depending upon the embedding cipher text bit [7].

Siwar Rekik et al. presented a new approach where DWT separates high frequency and low frequency components. In the next stage low amplitude of the high frequency component is used to hide another audio signal. This increases the complexity hiding so that any eavesdropper cannot extract the hidden information even after suspecting the existence of a secret message [8].

Neha Gupta et al. proposed a new method by combining LSB and DWT. DWT is applied on audio files for extracting higher frequency. Then LSB is used for hiding secret message in higher frequency components. This improves the simple LSB algorithm so that the malicious people cannot easily try to extract the message from the beginning of the audio file [9].

B. Geetha vani et al. proposed a hybrid method by integrating cryptography and steganography. HCNN (Hopfield Chaotic Neural Network) is adopted for encrypting text characters which enhances the level of security [10].

In the proposed system, wavelet families are used to embed text in the cover audio file. For better security AES algorithm is used. The rest of the paper is organized as follow. In section 2, literature review is described, in section 3 proposed system is explained, in section 4 results are shown and in section 5 comprises of conclusion.

PROPOSED METHOD

In the proposed method steganography is combined with cryptography for secure transmission of information. Here information is in the form of text. For high security AES algorithm is used while for embedding data in audio file, Wavelet families had been used.

Hence this method is formulated as follows:

A. AES Algorithm:

In our method we are using 16 bit key while the data which is going to encrypt is of length 16 and 32. The length of cipher key is also 16.

For both cipher and inverse cipher, AES algorithm is broken down to following functions:

1) Add Round Key
2) Sub Byte
3) Shift Rows
4) Mix Columns

1) Add Round Key: Each 16 bytes of the state is XORed against each 16 bytes of the portion of expanded key.

2) Sub Byte: During encryption each valus of the state is replaced with corresponding SBOX value.

3) Shift Rows: Arranges he state in a matrix form and then performs a circular shift for each row. The circular shift moves each byte one space over.

4) Mix Columns: This step will mix data within each column of the state array.

B. Wavelet Transformtion:

Wavelet theory is a combination of low pass and high pass filter. In this method different wavelet families like daubechies, symlet, coiflet, biorthogonal, stationary and dmer are used for embedding data in audio signal. On applying these wavelet families to audio signal will split component into numerous frequency bands called sub bands known as

Approximation – LL – Horizontally and vertically low pass
Vertical – LH – Horizontally low pass and vertically high pass
Horizontal – HL - Horizontally high pass and vertically low pass
Diagonal – HH – Horizontally and vertically high pass

Thus these wavelet sub bands or coefficient are used for further processing.

HAS (Human Auditory System) had wider dynamic range compare to HVS (Human Visual System). HAS contains fairly small differential range i.e loud sounds generally tend to mash out weaker sounds. Thus HAS is sensitive to high frequency parts compared to low frequency. Hence hiding

ISSN 2320 -2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.11, Pages : 26-31 (2014)
Special Issue of ICCAAC 2014 - Held on December 08,2014,Hyderbad, India

secret message in low frequency i.e LL – approximation sub band will be more appropriate. As hiding secret data in approximate sub band doesn't distort much sound quality of the audio signal.

Wavelet Families:
Many Wavelet Families have been developed with different properties. Here the performance analysis is done for DWT's different wavelets.

1. Daubechies Wavelets: dbN

The dbN wavelets are the Daubechies extremal phase wavelets and having highest N number of vanishing moments for a given support width. The db1 wavelet is also known as the Haar wavelet. The Haar wavelet is one of the oldest and simplest wavelet. It is the only orthogonal wavelet with linear phase. The Haar wavelet is a sequence of rescaled "square-shaped" functions which together form a wavelet family or basis. The Haar wavelet transform has a number of advantages such as it is conceptually fast, simple, memory efficient. This property can be an advantage for the analysis of signals with sudden transitions including monitoring of tool failure in machines.

While the other Daubechies wavelet transforms are defined in the same way as the Haar wavelet transform by computing the running averages and differences via scalar products with scaling signals and wavelets, the only difference between them consists in how these scaling signals and wavelets are defined. They represent the foundations of wavelet signal processing and are used in various applications. For analyzing daubechies wavelet we have taken db1, db2, db4, db16 in the proposed algorithm.

2. Symlet Wavelets: symN
The symN wavelets are also known as least-asymmetric wavelets. They are a modified version of Daubechies wavelets with increased symmetry. The symlets are more symmetric than the extremal phase wavelets but not perfectly symmetrical. SymN has N is the number of vanishing moments. The symlet wavelets are near symmetric, orthogonal and biorthogonal. Here sym1, sym5 and sym8 are analyzed.

3. Coiflet Wavelet: coifN
This wavelet function has 2N moments equal to 0 and its scaling function has 2N-1 moments equal to 0. The two functions have support of length 6N-1. The coiflets wavelets have nearly symmetric graphs and they are similar to daubechies wavelet as they have a maximum number of vanishing moments. For analysis purpose coif1 and coif5 is considered.

4. Biorthogonal Wavelet
A biorthogonal wavelet is a wavelet where the associated wavelet transform is invertible but not surely orthogonal. Designing biorthogonal wavelets allows more degrees of freedom than orthogonal wavelets. One extra degree of freedom is the possibility to produce symmetric wavelet functions. Biorthogonal wavelets are linear phase, which is required for signal and image reconstruction.

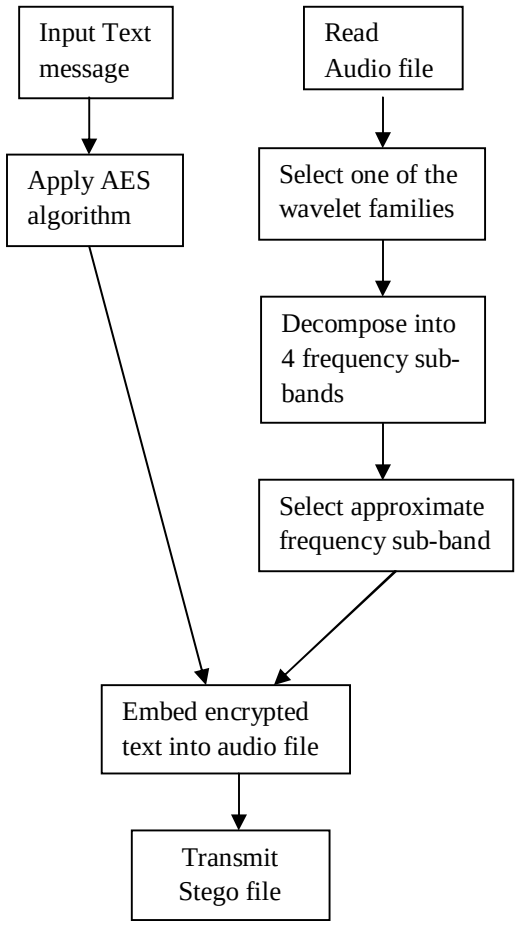

Fig 1: Block Diagram for Data Embedding

Implementation of Data Embedding:

The embedding process is summarized in the fig 1, and the implementation process of data embedding is explained in the following steps:

1. Input data and key.
2. Input data is encrypted using AES algorithm to obtain cipher text.
3. Audio signal will be read and separate into low frequency and high frequency

ISSN 2320 -2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.11, Pages : 26-31 (2014)
Special Issue of ICCAAC 2014 - Held on December 08,2014,Hyderbad, India

component using one of the wavelet transformations.

4. Cipher text is processed by adjusting according to the decomposition of the audio signal.
5. Then cipher text from the above step is added to low frequency of audio signal by using different wavelet families like daubechies, symlet, coiflet, biorthogonal, stationary and dmer.

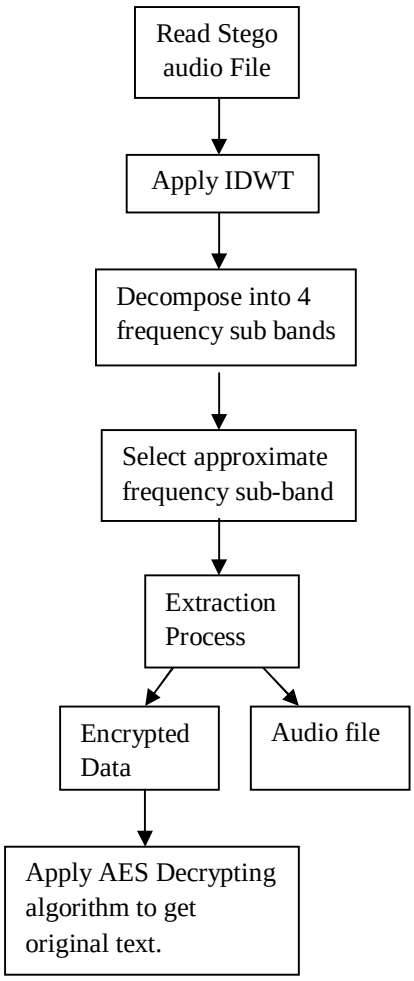

Fig 2: Block Diagram for Data Extraction

Implementation of Data Extraction:

The data extraction is the reverse process of data embedding summarized in fig 2. The following steps explain the data embedding:

1. Read the stego signal.
2. Apply inverse DWT on the stego audio signal to obtain audio signal into low frequency and high frequency.
3. Select approximate frequency sub band i.e low frequency
4. The stego signal is decomposed to obtain cipher text and audio signal.
5. The cipher text adjusts the values of the columns of the signal from decomposition.
6. The cipher text is converted into plain text using AES decryption algorithm.

PERFORMANCE VALUATION:

Steganographic approaches are evaluated in the literature using subjective and objective evaluation.

Subjective Evaluation:

Subjective listening tests are performed by human's auditory perception, the listeners are asked to play in random order the stego signal and ordinary audio clips. Each listener has to identify better quality audio file among original and stego signal. The maximum number of listener couldn't distinguish between two audio file.

Objective Evaluation:

The objective evaluation is mainly done to measure the distortion level in steganographic object. The evaluation of the stego audio done by objective measure demonstrates the possibility of any alteration to perceptual layout of the audio. The main parameters used for objective evaluations are PSNR, MSE and Entropy.

The table 1 shows only slight variation in the above parameters. This indicates that the embedding algorithm will modify the content of original audio by negligibly amount. The amount of noise added to cover file is calculated by using MSE and PSNR.

The data obtained for different wavelet families is tabulated in the table given below:

ISSN 2320 -2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.11, Pages : 26-31 (2014)
Special Issue of ICCAAC 2014 - Held on December 08,2014,Hyderbad, India

Table 1: Result of the proposed method.

Audio File	Types of Wavelet	Original audio file			Stego audio file		
		PSNR	MSE	Entropy	PSNR	MSE	Entropy
One.wav	Db1 (Haar)	62.2739	0.0385204	3.77812	44.1405	2.50629	3.78172
	Db16	62.2739	0.0385204	3.77812	62.268	0.0385726	3.78517
	Coif1	62.2739	0.0385204	3.77812	48.9591	0.8274	3.7829
	Sym8	62.2739	0.0385204	3.77812	62.2716	0.0385409	3.77838
	Bior3.7	62.2739	0.0385204	3.77812	62.2726	0.0385322	3.77838
Handel.wav	Db1 (Haar)	57.6707	0.111175	4.08073	53.768	0.273076	4.08073
	Db16	57.6707	0.111175	4.08073	57.6707	0.111175	4.08041
	Coif1	57.6707	0.111175	4.08073	43.5460	0.7864	3.1002
	Sym8	57.6707	0.111175	4.08073	57.6705	0.111173	4.08040
	Bior3.7	57.6707	0.111175	4.08073	57.6707	0.111174	4.08042
Trimhandel.wav	Db1 (Haar)	62.1862	0.0393058	3.78068	44.1911	2.47728	3.78436
	Db16	62.1862	0.0393058	3.78068	62.1859	0.0393092	3.78081
	Coif1	62.1862	0.0393058	3.78068	48.9585	0.8265	3.7819
	Sym8	62.1862	0.0393058	3.78068	62.1737	0.0394197	3.78081
	Bior3.7	62.1862	0.0393058	3.78068	62.1862	0.0393044	3.78052

Robustness:

Robustness is another measure used to evaluate the performance of the proposed method. The behavior of the typical attacks is experimented and result is shown. Normalized correlation coefficient value is calculated from stego and original audio file which determines whether the secret message embedded in the audio file withstands the attack or not. If the normalized correlation coefficient values are equal to 1 then stego file resist against the processing attacks.

Adding noise:

First the proposed method is tested by applying noise and filtering technique.

Gaussian filtering technique is applied to the stego file and PSNR, MSE and Entropy is calculated. The noise is added to stego audio file by 25%, 40% and 50% and thus result is compared with the original one.

Removal of sample:

Similarly samples are removed and replaced by the vertical component to measure the robustness of the system. Around 1000 to 5000 samples are replaced. The result of both adding noise and removing samples are shown in the table 2.

Table 2: Result of proposed method after adding noise and removing samples

Audio file	SNR value/ Removed Samples	Stego Audio File			After adding noise and removing samples			Correlation coefficient
		PSNR	MSE	Entropy	PSNR	MSE	Entropy	
Track 1	SNR 50	58.5138	0.0915592	4.03347	58.5131	0.091573	4.53666	1
Track 2	SNR 75	57.6707	0.0111174	4.08037	57.6707	0.0111174	4.12623	1
Track 3	SNR 60	62.2756	0.038505	3.7776	62.2756	0.038505	4.07736	1
Track 4	Removed 1000	62.2285	0.038925	3.78097	62.2284	0.038925	3.78097	1
Track 5	Removed 5000	62.2726	0.0385315	3.77835	62.2720	0.0385311	3.77831	1

CONCLUSION

This paper illustrates some of the wavelet methods used for digital audio steganography. We have presented a high security and high stego-signal quality audio steganography scheme. We had observed larger PSNR indicates better perceptual quality. A perfect reproduction of original audio file will have an MSE equal to zero but stego audio file greatly differs from the original audio when MSE will have large value like in db1 i.e Haar wavelet. The db16, sym8 and bior3.7 produce the best result for audio steganography. Among these three wavelets bior3.7 is best. This is so, the wavelet coefficient should be even for the embedding as we are using the AES algorithm which produces the data in even (16, 32). In simple manner the embedding process of data should be done in lower no of rows extension for the best result using wavelet family in audio steganography. The proposed method is also resistant to different types of attack like adding noise and removing samples.

REFERENCES

[1] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath, “Evaluating Image Steganography Techniques: Future Research Challenges”, 978-1-4673-2088-7, 2013 IEEE

[2] Shamim Ahmed Laskar1 and Kattamanchi Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar, Neeraj Vishwakarma, “Audio Steganography And Security Using Cryptography” , International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.

[3] (Book style)

[4] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam, “Comparative study of digital audio steganography techniques”, EURASIP Journal on Audio, Speech, and Music Processing 2012, 2012:25

[5] Rohit Tanwar, Bhasker Sharma and Sona Malhotra" A Robust Substitution Technique to implement Audio Steganography", International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, February 6-8, 2014, Page(s):14.ISBN: 978-1-4799-2995-5 2014 IEEE.

[6] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik , "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" in International Journal of Advanced Research in Computer and Communication Engineering Vol. I, Issue 4, June 2012.

[7] Satish Singh Verma, Ravindra Gupta and Gaurav Shrivastava, “A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain”. 2014 Fourth International Conference on Communication Systems and Network Technologies. ISBN: 978-1-4799-3070-8 2014 IEEE.

[8] Siwar Rekik, Driss Guerchi, Sid-Ahmed Selouani and Habib Hamam, “Speech steganography using wavelet and Fourier transforms” EURASIP Journal on Audio, Speech, and Music Processing 2012, 2012:20 http://asmp.eurasipjournals.com/content/2012/1/20.

[9] NehaGupta, Ms. Nidhi Sharma, “Dwt and Lsb Based Audio Steganography”. 2014 International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, India, Feb 6-8 2014 ISBN: 978-1-4799-2995-5 2014 IEEE.

[10] B. Geetha vani, Prof. E. V. Prasad, “A Hybrid Model for Secure Data Transfer in Audio Signals using HCNN and DD DWT”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 2013.