Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Multi-level Secure Mechanism For Audio Watermarking

Supiksha Jain
M.TECH Scholar,CSE Dept.
DCRUST Murthal, India

Er. Sanjeev Indora
Asst. Prof, CSE Dept.
DCRUST Murthal, India

Abstract: The information which is being transmitted from one place to another is vulnerable to various types of active and passive attacks. The security of the data and information is one of the most challenging aspects of computer communication in today' time. Steganography & watermarking are the process of hiding information which are needed to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. Audio Watermarking is the popular technique used to hide copyright information in original audio file. This technique helps to determine ownership of original creator of audio file. A hybrid method for audio watermarking (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications) has been proposed in the current research article. The effect of cryptography is that watermark audio is encrypted so that no one understood the meaning of audio.

Keywords: Audio Watermarking, Spread Spectrum, Encryption coding

1. INTRODUCTION

Both cryptography and steganography ensure secret transfer of data and information over the insecure communication medium. This method of secret communication is also prevalent in ancient time where messages are written with some special ink etc. The modern Steganography uses different mediums for hiding secret information such as image, text, audio and video. [1].
Generally applications are developed by teams of limited members but they are used by large group of users. There are some persons called hackers that modify by original applications a little bit & make profit without giving any benefits to their original creators. The numbers of hackers are increasing day by day. Therefore we must assign high priority for protection of applications. One of the latest method for providing copyright information to our work is using watermarking [2].
Steganography [3] is the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. As the message is not visible so it does not get any attention of unauthorized users which safeguard the secret message. This method of secret communication is also prevalent in ancient time where messages are written with some special ink etc. The modern Steganography uses different mediums for hiding secret information such as image, text, audio and video.
Watermarking is the popular technique used to hide copyright information. In an audio Watermarking some secret image or text are embedded in the sound of audio file. This can be done by modifying the sound file in their binary sequence. There are multiple audio formats that help in audio watermarking such as au format, wav format and mp3 format. There are simple to most powerful methods for performing audio watermarking. This technique helps to determine ownership & authentication proof of original creator of audio file.
In this paper we propose a hybrid approach for audio watermarking (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications).

2. OVERVIEW OF WORK

Depending upon domain of operation the audio watermarking technique [2] can be divided into two groups' viz. 'Time Domain method' and 'Transformation based technique'. With Time domain method embedding of secret data is done with alteration without any transformation. This technique is applied on original sound signal of the audio file. One popular method used with this technique is LSB (Least Significant Bit). As the name suggests watermark image is inserted into the lowest bit of the cover audio.
The Time domain method is not very rigid because low pass filtering of audio signal can lost the watermark image or data. Therefore this technique is applicable in the application areas where less security is required for example ownership applications.
The Transformation based watermarking uses transformation of cover audio signal to provide more robust and rigid security of hidden data. One popular method using transformation based watermarking concept is 'Spread Spectrum Technique'. In this method the original signal is transformed in some another domain then watermark information is placed in the transformation domain. Due to robust security this technique is used in applications such as copyright of original work [4][5].

A. LSB Coding

LSB coding [13] is the oldest and popular technique for steganography and watermarking. It is the process of modifying the least significant bits of cover signal with the bits of watermark image or data. It is the best technique for hiding text data in image file because it is easy to represent image file in the form of bits. Large the number of bits substituted in the cover signal largest the robustness of the secret data. Figure 1 below shows the insertion of two bits of watermark in the host signal of eight bits [6][7].

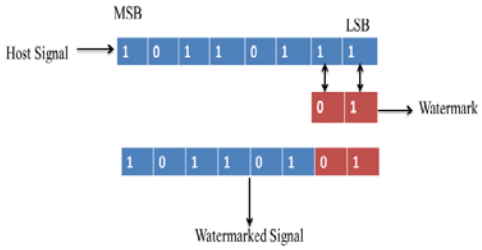

Figure 1: LSB Coding

B. Spread Spectrum Technique

With this technique on high bandwidth signal we transmit the low bandwidth signal so that signal is not detectable. In audio watermarking using spread spectrum technique the watermark data is spread over the different frequencies of audio signal such that there is negligible change in audio quality [8].

In spread spectrum technique [9] method the original signal is transformed in some another domain then watermark information is placed in the transformation domain. Due to robust security this technique is used in applications such as copyright of original work. Zhou *et al.* proposed following quoted algorithm "embedding watermark in 0th DCT coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal."

For embedding of watermark data [10] is done in the frequency domain transformation of original signal using Discrete Cosine Transformation (DCT). Now for extraction inverse Discrete Cosine Transformation (IDCT) concept is applied for obtaining embedded watermark data.

Figure 2 below shows the concepts of embedding and extraction of watermark data using DCT & IDCT.

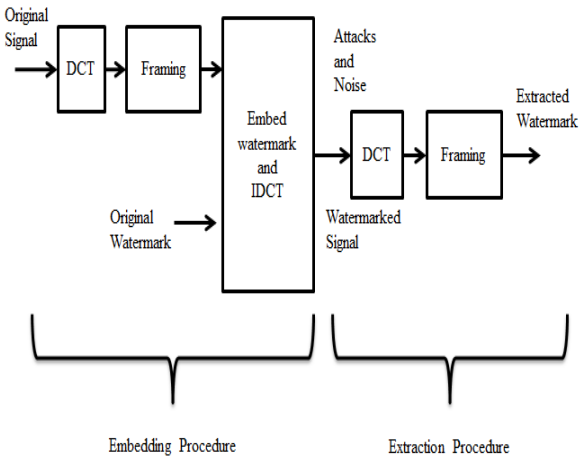

Figure 2: Embedding & Extraction using spread spectrum technique

3. PROPOSED WORK

A hybrid method for audio watermarking (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications) has been proposed in this work. Firstly, a secret watermark image [11] is kept inside an audio with encryption of watermark image using modified Direct Sequence Spread spectrum method [12][13]. After that, Watermarked Audio [14] is encrypted using advanced random permutation method and then decrypted using reverse process. Then, watermark is extracted from decrypted watermarked audio. PSNR, MSE and Cross-correlation are calculated as performance evaluation parameters for proposed method. MATLAB [15] has been used as an implementation platform using image processing toolbox and generalized toolbox.

MSE: Mean squared normalized error performance function

Perf = mse(net,t,y,ew)

mse is a network performance function. It measures the network's performance according to the mean of squared errors.

net	Neural Network
t	Matrix or cell array of targets
y	Matrix or cell array of outputs
ew	Error weights(optional)

PSNR: Peak Signal-to-Noise Ratio

The psnr function implements the following equations to calculate the Peak Signal-to-Noise Ratio (PSNR):

PSNR= 10log10(peakval2/MSE)

Where peakval is either specified by the user or taken from the range of the image datatype.

Cross-Correlation: Cross-correlation is a measure of similarity of two series as a function of the displacement of one relative to the other.

For continuous functions f and g , the cross-correlation is defined as:

$$(f \star g)(\tau) \stackrel{\text{def}}{=} \int_{-\infty}^{\infty} f^*(t)\, g(t+\tau)\, dt,$$

Where **f*** denotes the complex conjugate of **f**,and **τ** is the displacement, also known as lag, although a positive value of τ actually means that g(t+τ) leads g(t).

Similarly, for discrete functions, the cross-correlation is defined as:

$$(f \star g)[n] \stackrel{\text{def}}{=} \sum_{m=-\infty}^{\infty} f^*[m]\, g[m+n].$$

The steps for implementation of proposed method are as follows:

AUDIO WATERMARKING

A1. EMBEDDING OF WATERMARK

- First of all read audio signal and image file from the disk.
- Convert both audio and image files into rows and columns format (Matrix) using MATLAB functions.
- Convert watermark matrix into binary matrix & reshape binary matrix into row matrix.
- Now using concept of spread spectrum technique embed the watermark image into cover audio.
- Divide the watermark image into parts if size of image is large.

A2. EXTRACTION OF WATERMARK

- For extraction of watermark image read the original audio file and watermark audio file.
- Select the image of original watermark & compute its size.
- Using spread spectrum technique extract the hidden watermark from the watermark audio.
- Display original as well as extracted image of watermark.

A. AUDIO CRYPTOGRAPHY

B1. ENCRYPTION PART

1. Inputting and reading of secret audio data.
2. Checking of length and sampling frequency of audio data
3. If sampling frequency > 44100 than cut down the length and sampling frequency of secret audio.
4. Calculation of size of row vector.
5. Generation of 1st random row vector of a fixed length and seed value.
6. Generation of 2nd random row vector according to number of elements of audio row vector.
7. Generation of 3rd random row vector according to number of elements of audio row vector.
8. Random permutation of audio or rearrangement of elements of audio matrix according to 3rd random row vector.
9. Updation and modification of 1st random row vector.
10. Generation of empty row cell according to the seed value.
11. Allotment and division of random permuted audio into empty cells with fast Fourier transform of each elements.
12. Allotment of rest of the audio part into last cell.
13. Conversion of cell into matrix.
14. Again application of random permutation on updated audio matrix according to 2nd random row vector.
15. Normalization of updated and permuted audio matrix elements (real and imaginary separately).
16. Saving of all 3 random vector and maximum value of real and imaginary parts as key for decryption.
17. Joining of both part (real and imaginary) of normalized audio.
18. Saving of the new encrypted audio.

B2. DECRYPTION PART

1. Reading of encrypted audio file.
2. Calculation of size of row vector audio.
3. Loading of key matrix.
4. Estimation of all 3 random vectors and maximum values of real and imaginary parts.
5. Estimation of seed value.
6. Combining of real and imaginary parts of encrypted audio with their maximum values.
7. Rearranging of encrypted audio according to 2nd random vector.
8. Generation of empty row cell according to the seed value.
9. Allotment and division of encrypted audio into empty cells with inverse fast Fourier transform of each elements.
10. Conversion of cell into matrix.
11. Rearranging of encrypted audio according to 3rd random vector.
12. Saving of new decrypted audio.

B. RESULTS

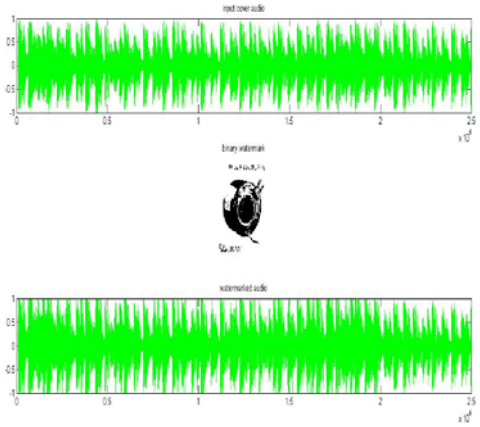

Figure 3: The original audio, binary watermark and watermarked audio

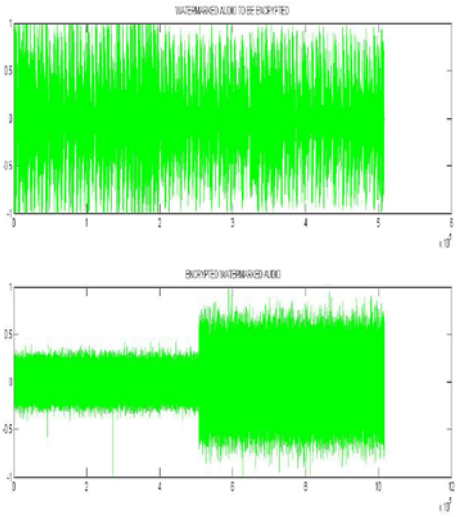

Figure 4: Watermarked audio and encrypted watermarked audio.

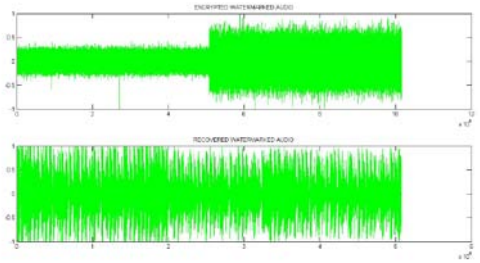

Figure 5: Encrypted watermarked audio and recovered watermarked audio.

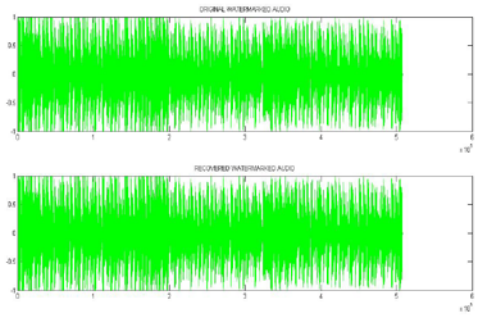

Figure 6: Orignal watermarked audio and Recovered watermark audio.

Figure 7: Orignal Watermark

Figure 8: Extracted Watermark

On analytical comparison of both watermark, we found almost no difference between them, which enhances the efficiency and robustness of proposed method.

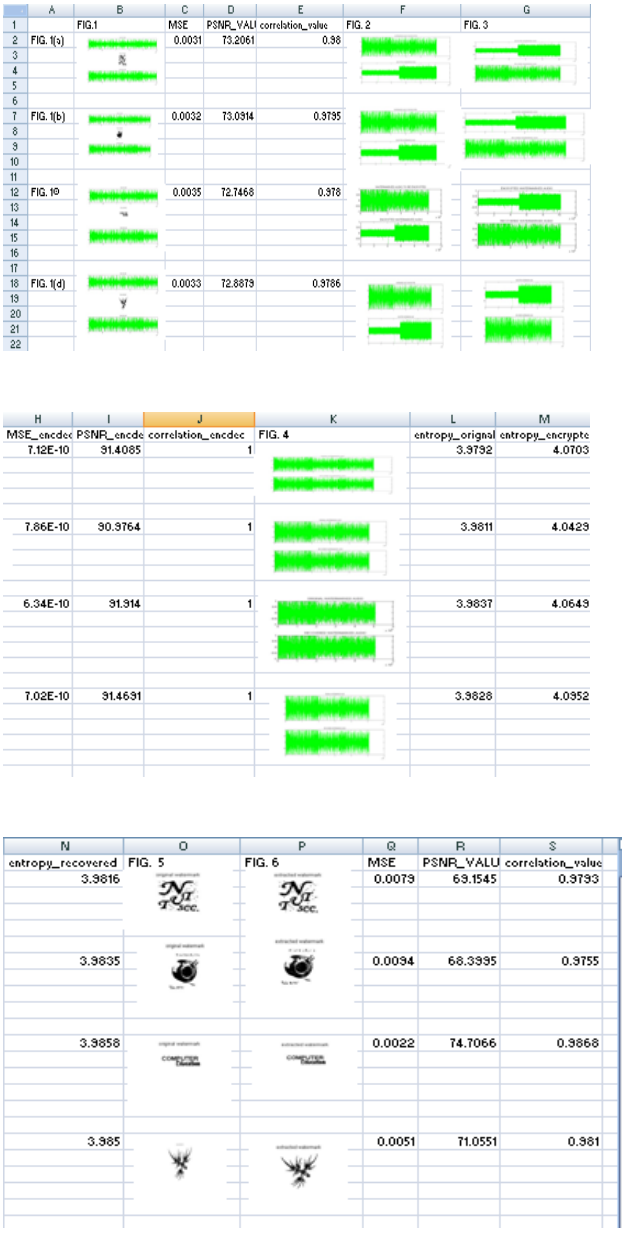

	FIG.1	MSE	PSNR_VALU	correlation_value	FIG. 2	FIG. 3
FIG. 1(a)		0.0031	73.2061	0.98		
FIG. 1(b)		0.0032	73.0914	0.9795		
FIG. 1©		0.0035	72.7468	0.978		
FIG. 1(d)		0.0033	72.8879	0.9786		

MSE_encdec	PSNR_encde	correlation_encdec	FIG. 4	entropy_orignal	entropy_encrypte
7.12E-10	31.4085	1		3.9732	4.0703
7.86E-10	30.9764	1		3.9811	4.0429
6.34E-10	31.314	1		3.9837	4.0649
7.02E-10	31.4631	1		3.9828	4.0352

entropy_recovered	FIG. 5	FIG. 6	MSE	PSNR_VALU	correlation_value
3.9816			0.0079	69.1545	0.9793
3.9835			0.0034	68.3395	0.9755
3.9858			0.0022	74.7066	0.9868
3.985			0.0051	71.0551	0.981

Figure 9: Analysis on various images

4. CONCLUSION

Watermarking and Steganography is the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. As the message is not visible so it does not get any attention of unauthorized users which safeguard the secret message. In an audio Watermarking some secret image or text are embedded in the sound of audio file. This can be done by modifying the sound file in their binary sequence. In this work we uses combine approach of audio watermarking using modified Direct Sequence Spread spectrum and cryptography using advanced random permutation with multiple key applications. Audio watermarking is to provide copyright & ownership information and cryptography provides encryption of watermark audio so that no one understood the meaning of audio.

REFERENCES

[1]. P. Singh, S. Kaur and S. Singh , "Cryptography: An Art of Data Hiding", International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (1), 2015, 117-120.

[2]. D. Kirovski and H. S. Malvar, "Spread-Spectrum Watermarking of Audio Signals", IEEE Transactions On Signal Processing: Special Issue On Data Hiding, 2014.

[3]. P. Shah, P. Choudhari and S. Sivaraman, "Adaptive Wavelet Packet Based Audio Steganography using Data History", 2008 IEEE Region 10 Colloquium and the Third ICIIS, Kharagpur, INDIA December 8-10. 286.

[4]. J. Antony, S. C. Sherly, "Audio Steganography in Wavelet Domain – A Survey", International Journal of Computer Applications (0975 – 8887) Volume 52– No.13, August 2012.

[5]. C. Li, W. Zeng, H. Ai and R. Hu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM". International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.

[6]. B. A. Patil and V. A. Chakkarwar, "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34 www.iosrjournals.org.

[7]. M. Asad, J. Gilani, A. Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 978-1-61284-941-6/111$26.00 ©2011 IEEE.

[8]. M. Sterling, E. L. Titlebaum, X. Dong and Mark F. Bocko, "An Adaptive Spread Spectrum Data Hiding Technique For Digital Audio", 0-7803-8874-7/05/$20.00 ©2005 IEEE, V – 685, ICASSP 2005.

[9]. M. Li, M. K. Kulhandjian, D. A. Pados, *E*, S. N. Batalama and M. J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, JULY 2013.

[10]. P. P. Balgurgi and S. K. Jagtap, "Intelligent Processing : An Approach of Audio Steganography", International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 2012, 19-20.

[11] R. Kaur and A. Kaur, "Hiding Copyright Mark in Images using Watermarking Technique", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014.

[12]. S. Gao, R.M. Hu, W. Zeng, H.j. Ai, and C.R. Li , "A Detection Algorithm of Audio Spread Spectrum Data Hiding", National Engineering Research Center for Multimedia Software Wuhan University :XKDQ, China email_gs@126.com . 978-1-4244-2108-4/08/$25.00 © 2008 IEEE.

[13] Y. Kakde, P. Gonnade and P. Dahiwale, "Audio-Video steganography," in IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems [Online]. pp. 1-6. 2015. Available: http://ieeexplore. ieee. org/

[14] U. Chauhan, R. K. Singh, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.

[15]. MATLAB Primer, MathWorks Inc, 2014.