International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 217-222 June 2018-Dec 2018 www.csjournals.com

Secure Mechanism for Voice Watermarking

Supiksha Jain[1], Er. Sanjeev Indora[2]
M.TECH Scholar[1], Asst. Professor[2]
CSE Dept., DCRUST Murthal, India
supikshajain04@gmail.com, sanjeev.cse@dcrustm.org

Abstract: The details 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 details,is one of the most challenging aspects of computer communication in today's time. Steganography & watermarking are the process of hiding details 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 details.Voice Watermarking is one of the popular technique used to hide copyright details in original voice file. This technique helps to determine ownership of original creator of voice 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 voice is encrypted so that no one understood the meaning of voice.
Keywords: Voice Watermarking, Spread Spectrum, Encryption coding.

I. INTRODUCTION

Both cryptography and steganography ensure secret transfer of data and details over the insecure communication medium. This method of secret communication is also prevalent in ancient time where text messages are written with some special ink etc. The modern Steganography uses different mediums for hiding secret details such as image, text, voice 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 termed as hackers that modify original applications a little bit & make gain 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 details to our work is using watermarking [2].

Steganography [3] is the process of hiding details 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 details. 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 details such as image, text, voice and video.

Watermarking is the popular technique used to hide copyright details. In a Voice Watermarking some secret image or text are embedded in the sound of voice file. This can be done by modifying the sound file in their binary sequence. There are multiple voice formats that help in voice watermarking such as au format, wav format and mp3 format. There are simple to most powerful methods for performing voice watermarking. This technique helps to determine ownership & authentication proof of original creator of voice 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).

II. OVERVIEW OF WORK

Depending upon domain of operation the voice 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 voice 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 voice.

The Time domain method is not very rigid because low pass filtering of voice 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.

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 217-222 June 2018-Dec 2018 www.csjournals.com

The Transformation based watermarking uses transformation of cover voice 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].

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].

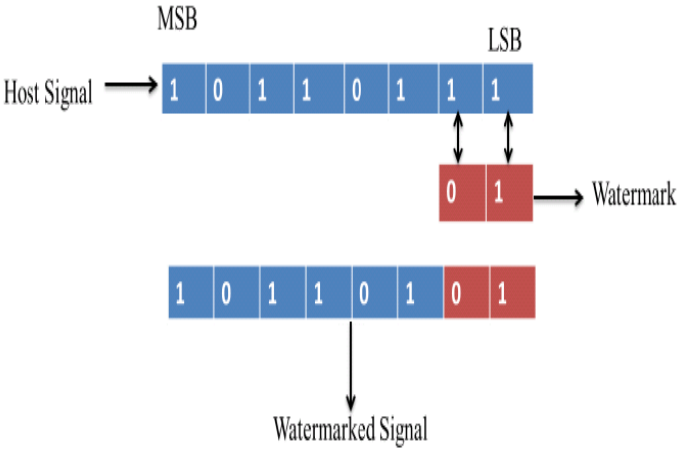

Figure 1: LSB Coding

A. Spread Spectrum Technique

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

In spread spectrum technique [9] method the original signal is transformed in some another domain then watermark details 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 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.

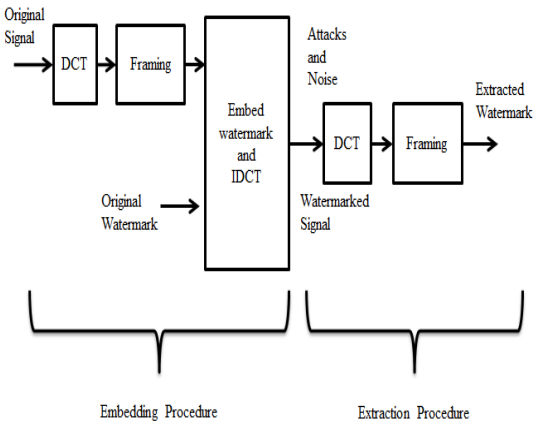

Figure 2: Embedding & Extraction using spread spectrum technique

III. PROPOSED WORK

A hybrid method for voice 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 is kept inside a voice with encryption of watermark image using modified Direct Sequence Spread spectrum method [12][13]. After that, Watermarked Voice [14] is encrypted using advanced random permutation method and then decrypted using reverse process. Then, watermark is extracted from decrypted watermarked voice PSNR, MSE and Cross-correlation are calculated as performance evaluation parameters for proposed method. MATLAB 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:

A. AUDIO WATERMARKING

A1. EMBEDDING OF WATERMARK

- First of all read audio signal and image file from the disk.
- Convert both image files into audio files into row and column format using MATLAB function.
- Convert watermark matrix into binary matrix and reshape binary matrix into row matrix.
- Now use the 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.

B. AUDIO CRYPTOGRAPHY

B1. ENCRYPTION PART

- Inputting & reading of secret audio data.
- Checking of length & sampling frequency of audio data.
- If sampling frequency > 44100 than cut down the length and sampling frequency of secret audio.
- Calculation of size of row vector.
- Generation of 1st random row vector of a fixed length and seed value.
- Generation of 2nd random row vector according to number of elements of audio row vector.
- Generation of 3rd random row vector according to number of elements of audio row vector.
- Random permutation of audio or rearrangement of elements of audio matrix according to 3rd random row vector.
- Updation & modification of 1st random row vector.
- Generation of empty row cells according to the seed value.
- Allotment & revision of random permuted audio into empty cells with fast fourier transform of each elements.
- Allotment of rest of audio part into last cell.
- Conversion of cell into matrix.
- Again application of random permutation on updated audio matrix according to 2nd random row vector.
- Normalization of updated & permuted audio matrix elements.

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 217-222 June 2018-Dec 2018 www.csjournals.com

- Saving all 3 random vector & maximum value of real & imaginary parts as key for decryption.
- Joining of both part (real & imaginary) of normalized audio.
- Saving of the new encrypted audio.

B2. DECRYPTION PART

- Reading of encrypted audio file.
- Calculation of size of row vector audio.
- Loading of key matrix.
- Estimation of all 3 random vectors & maximum values of real & imaginary parts.
- Estimation of seed value.
- Combining of real & imaginary parts of encrypted audio with their maximum values.
- Rearranging of encrypted audio according to 2nd random vector.
- Generation of empty row cells according to the seed value.
- Allotment & division of encrypted audio into empty cells with inverse fast fourier transform of each elements.
- Conversion of cell into matrix.
- Rearranging of encrypted audio according to 3rd random vector.
- Saving of new decrypted audio.

C. RESULTS

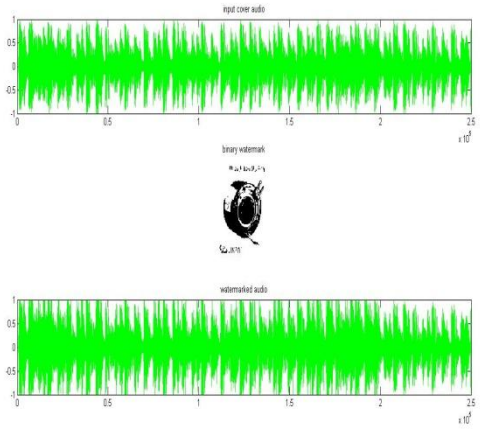

Figure 3: The original audio, binary watermark and watermarked audio

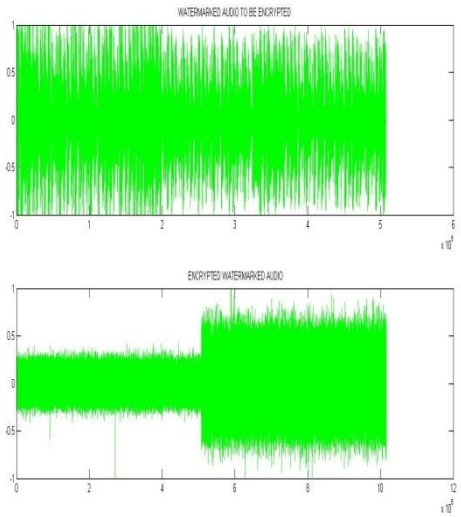

Figure 4: Watermarked audio and encrypted watermarked audio.

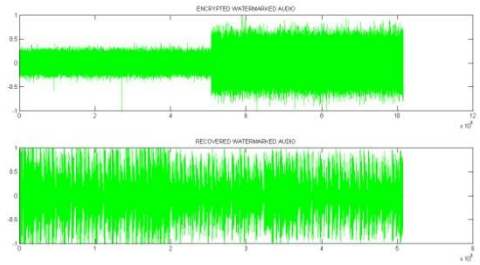

Figure 5: Encrypted watermarked audio and recovered watermarked audio.

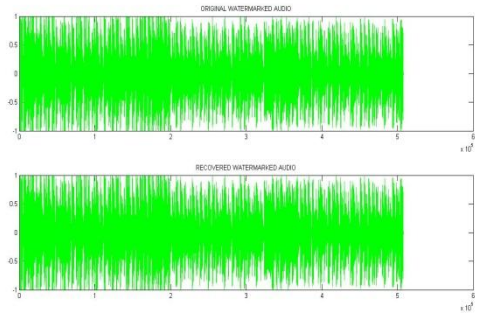

Figure 6: Orignal watermarked audio and Recovered watermark audio.

Figure 7: Original Watermark

International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 217-222 June 2018-Dec 2018 www.csjournals.com

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.

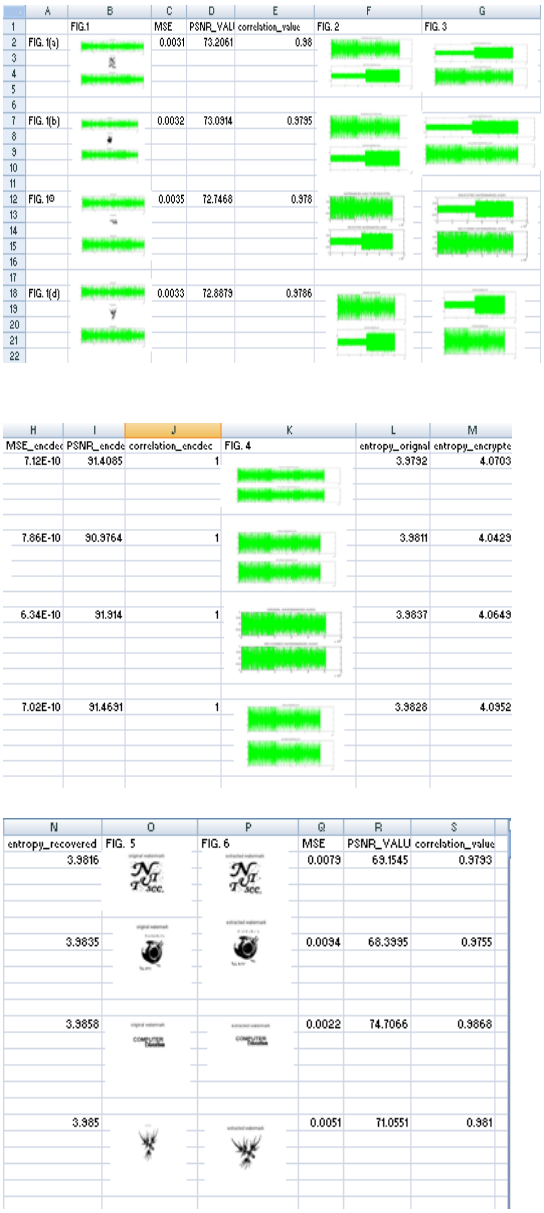

Figure 9: Analysis on various images

IV. Conclusion

Watermarking and Steganography is the process of hiding details 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 details. As the message is not visible so it does not get any attention of unauthorized users which safeguard the secret message. In an Voice Watermarking some secret image or text are embedded in the sound of voice file. This can be done by modifying the sound file in their binary sequence. In this work we uses combine approach of voice watermarking using modified Direct Sequence Spread spectrum and cryptography using advanced random permutation with multiple key applications. Voice Watermarking is to provide copyright & ownership details and cryptography provides encryption of watermark voice so that no one understood the meaning of voice.

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] K. Hossain and R. Parekh, "An Approach Towards Image, Audio and Video Steganography", Second International Conference on Research in Computational Intelligent and Communication Networks (ICRCICN), IEEE 2016.

[16] B. Ram,"Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancement in Research & Technology, Vol. 2(4), pp. 19-27, 2013.

[17] Y. Perwej, F. Parwej, & A. Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", International Journal of Multimedia & Its Applications, 4(2), pp. 21-38, 2012.