Multi- Level Security Mechanism for Audio Steganography

[I]Sakshi Gupta, [II]Deepti Dhingra, [III]S.C.Gupta, [IV]Vikram Bali

[I,II,III,IV]Dept. of Computer Science, Panipat Institute of Engineering & Technology (PIET), Kurukshetra University, Kurukhetra (KUK), Haryana, India

Abstract

Today's Computer world ensures security, integrity, confidentiality of the organization's data to a very large extend. Cryptography is being used by organization in order to transmit a secret message successfully without being caught up by the enemies. Cryptography has evolved rapidly from the ancient times to the modern world. The information which is being transmitted from one place to another is vulnerable to various types of active and passive attacks. Therefore, the motive to secure information is considered a major challenging aspects of communication in today' time. A hybrid method for audio steganography (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications) has been proposed in this paper.

Keywords

Spatial Domain, Frequency Domain, Patchwork, Spread Spectrum

I. Introduction

Before inventing the steganography and cryptography, it was a major challenge for secure transmission of information and, also for achieving secure environment for communication. There were various methods used in the earlier days for securely transmitting messages. Some include using invisible ink for writing purpose, making small modifications in a standard painting, creating a new image by joining two images, forming a message on a messenger's head with the help of a suitable shave, making tattoos for messages on scalp and so on [12].

It is common that an application used by many people, is mostly built by a small group. Some people tend to modify the original application or use them as they are without providing proper credits to the real possessor to make more profits, such people are termed Hackers. It is also an evident fact that the hackers outnumber the creators. Hence, the application protection should be given a remarkable priority. Thus to ensure restriction of mischievous users robust, efficient and distinctive techniques must be employed to protect them. The technological development has grown the horizon of steganography and has lowered its efficiency at the same instant for the medium being unprotected. This thus gives way to a new technology being developed called "Watermarking". Some of its applications consist of protecting possession, evidence for authentication, to monitor air traffic, medical implementations etc [9, 17]. Being among major businesses of the world, music industry takes great advantage from the audio signal watermarks.

Replacement of non-useful data in various computer files like audio, video or text or graphics with different invisible data bits is the working principle of Steganography. Plain or cipher text or images are the hidden data. The Audio Steganography used in computer systems embed the secret memo in the digital audio signals. The commonly used audio format files AU, WAV and MP3 are used to insert the classified data as the implementation of current audio steganography softwares. The message embedding in the digital audio signals is comparatively a difficult task than the processes using other media file like images. The audio steganography covers the ground of fundamental algorithms of inserting data as the noise signals and also the influential ways of usage of authentic signal processing methods for hiding data.

In this paper we propose a hybrid approach for audio steganography (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications).

II. Overview of Work

The techniques for watermarking of audio is distributed to two groups focused on their sphere of operation. The techniques divided are **time domain** and the **transformation based techniques**. The time domain method consists of ways where no transformation is used for embedding. Watermarking is employed on the original samples of the audio signal. One example of such technique includes the **LSB** method. In this method, the host signal's least significant bits are used to embed the watermark. In contrast to this technique, transformation domain is used to watermark in the transformation based watermarking technique.

Normally, simple low pass filter can be used to remove the watermarking, so the time domain techniques give the least robustness [5]. Hence application including protection of copyright and airline traffic monitoring do not use the time domain techniques; however, applications such as ownership proof and medical applications can use it.

A. LSB Coding

This is a very commonly used techniques employed in applications used to process signal. This technique consists of substituting the carrier signal's LSB with the bit pattern obtained via the watermark noise [17]. The number of bits in the host signal that are being substituted defines the robustness. This technique is commonly helpful for watermarks used in images as integers are used for representation of pixels making the bits easily replaceable. The conversion of samples to integers leads to degradation of the signal quality very much; hence the audio signal contains real values. The 2-bit LSB coding is shown in Figure 3 below.

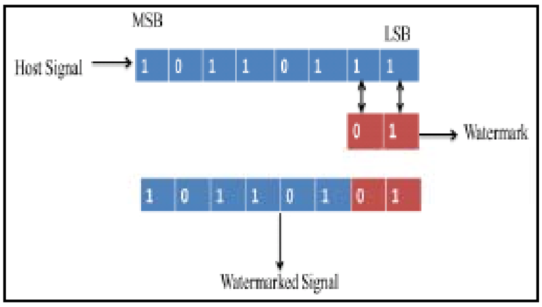


Fig. 3: LSB Coding

B. Spread Spectrum Technique

The communication via spread spectrum is used to derive the above techniques [17]. The basic principle is the use of large bandwidth signal to transmit a narrow band signal because the overlapped signal energy makes it undetectable. Similarly multiple frequency bins are used to distribute the watermark over them such that each of them has very less energy making them undetectable [18].

In this technique, domain transformation method is used to transform the original signal to some other domain [17]. Any approach can be used for the techniques used to embed such as quantization. Zhou *et al.* proposed an algorithm which applies the DCT technique to the original signal. It then uses 0th and 4th coefficients obtained from DCT to embed the watermark. Figure 4 interprets the embedding and extracting procedure. DCT is used to transform the original signal to frequency domain. After that sample values of that domain are used for embedding the watermark. Similarly to extract the signal back which is watermarked, the reverse procedure is executed [19]. This embedding procedure to generate the signals is shown in Figure 4 below.

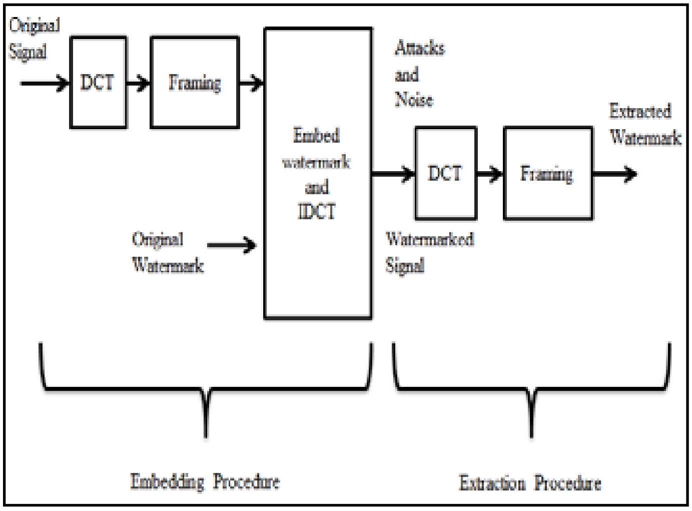


Fig. 4: Example for spread spectrum technique

III. Proposed Work

When the audio steganography is concerned, the spread spectrum technique works on the principle to use the information to be hidden to stretch it across the frequency spectrum of audio signal as greater as possible. This technique shows analogy to a system which uses the LSB coding that scatters the bits of required message entirely over the sound file. However, in contrast to LSB coding, the spread spectrum technique uses the frequency spectrum of the sound file to spread the hidden message, and the code used is not dependent of the original signal. Thus, a bandwidth greater than the actual requirement for transmission is occupied by the final signal.

Direct-sequence and frequency-hopping are the two versions of spread spectrum that are useful in audio steganography. In DSSS, a constant known as chip rate is used to scatter the hidden message which is then modulated further with a pseudorandom signal. It is then interleaved with the cover-signal. In FHSS, the alteration of frequency spectrum of sound file is carried out such that rapidly hopping between frequencies could be possible.

The steps for implementation of proposed method are as follows:

A. Audio Steganography

A1. 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. Conversion of row vector audio to column vector audio.
5. Calculation of size of column vector.
6. Generation of 1st random row vector of a fixed length and seed value.
7. Generation of 2nd random row vector according to number of elements of audio column vector.
8. Generation of 3rd random row vector according to number of elements of audio column vector.
9. Random permutation of audio or rearrangement of elements of audio matrix according to 3rd random row vector.
10. Updation and modification of 1st random row vector.
11. Generation of empty row cell according to the seed value.
12. Allotment and division of random permuted audio into empty cells with fast Fourier transform of each elements.
13. Allotment of rest of the audio part into last cell.
14. Conversion of cell into matrix.
15. Again application of random permutation on updated audio matrix according to 2nd random row vector.
16. Normalization of updated and permuted audio matrix elements (real and imaginary separately).
17. Saving of all 3 random vector and maximum value of real and imaginary parts as key for decryption.
18. Joining of both part (real and imaginary) of normalized audio.
19. Saving of the new encrypted audio.

A2. Decryption Part

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

A. Embedding of Watermark

- First of all read cover sound signal and get equivalent 2D matrix and size of matrix i.e. rows and column is calculated. Read image of watermark and get equivalent 2D matrix and compute size of matrix i.e. rows and column. Convert watermark matrix into binary matrix & reshape binary matrix into row matrix.
- A spreading factor 2 is multiplied with the added complete

number of elements in the binary matrix of watermark to obtain the spreading size. After that a random sequence for binary key is generated in accordance with the spreading size, so that security can be provided. Binary XOR the row vector of watermark matrix using the key sequence to generate the encoded watermark matrix. This results in a double sized encoded watermark matrix in comparison to the original one.

- In case cover image turns out to be too big then it is divided into two parts of matrix. The part of the cover image matrix is selected such that the a block size is selected which is suitable for that part. After that two parts are created for the matrix.
- The first part matrix is segmented to a sub-matrix array which is given below. Each of this sub-matrix contains a certain number of elements which depends upon block size. Application of Discrete Cosine Transform (DCT) on each element of all the sub-matrices. Embedding of watermark by multiplication of encoded watermark matrix with cosine transform matrix. Join reconstructed matrix with second part of cover image matrix and getting of embedded image and resize embedded image according to original audio cover signal. Plot frequency coefficients of both audio cover signals, so as to make comparison.

A. Extraction of Watermark

- Read audio cover signal and audio watermarked signal & calculate size of cover audio signal. Read watermark image and compute size of watermark image. Also calculate number of elements in watermark image.
- For increasing the spreading, block size of 10 are selected and after that cover and marked audio images are then divided in two parts. Empty cell containing the empty matrices arrays are declared which are then filled with the former part of both matrix.
- To limit the filling of empty cells to a certain value, a threshold value is declared. DCT is then applied on both the cells. After that the real sound cover signal is used to divide third element of every watermarked signal matrix.
- Removing the key sequence or the watermark components being decoded. Reconstructing the fetched watermark in accordance with the image size of real watermark. After that the two images of watermark, that are the real one and the extracted one, are plotted.

IV. Results

Figure 5 is the snapshot of original audio, binary watermark and watermarked audio. Figure 6 is the snapshot of watermarked audio and encrypted watermarked audio. Figure 7 is the snapshot of Encrypted watermarked audio and recovered watermarked audio. On analytical comparison of both watermark, we found almost no difference between them, which enhances the efficiency and robustness of proposed method.

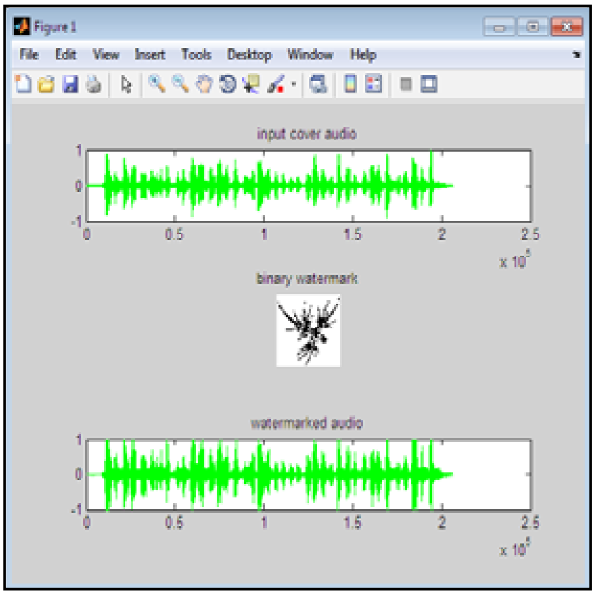


Fig. 5: The original audio, binary watermark and watermarked audio

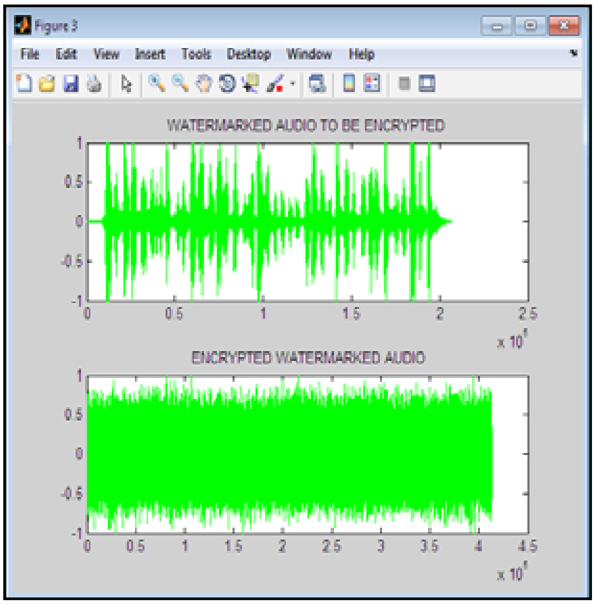


Figure 3
File Edit View Insert Tools Desktop Window Help
WATERMARKED AUDIO TO BE ENCRYPTED
1
0.5
0
-0.5
-1
0 0.5 1 1.5 2 2.5
x 10^5
ENCRYPTED WATERMARKED AUDIO
1
0.5
0
-0.5
-1
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5
x 10^5

Fig. 6: Watermarked audio and encrypted watermarked audio.

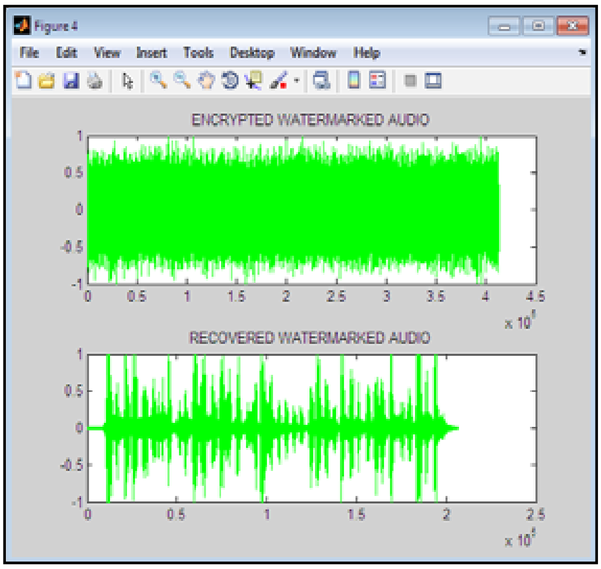
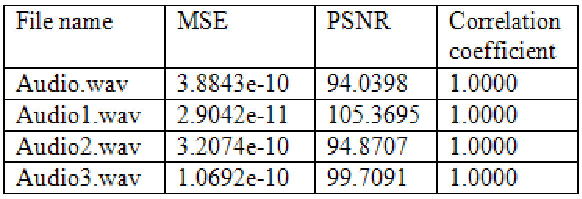


Figure 4
File Edit View Insert Tools Desktop Window Help
ENCRYPTED WATERMARKED AUDIO
1
0.5
0
-0.5
-1
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5
x 10^5
RECOVERED WATERMARKED AUDIO
1
0.5
0
-0.5
-1
0 0.5 1 1.5 2 2.5
x 10^5

Fig. 7: Encrypted watermarked audio and recovered watermarked audio.

Figure 8 below shows the Comparison of watermarked audio and recovered watermarked audio



File name	MSE	PSNR	Correlation coefficient
Audio.wav	3.8843e-10	94.0398	1.0000
Audio1.wav	2.9042e-11	105.3695	1.0000
Audio2.wav	3.2074e-10	94.8707	1.0000
Audio3.wav	1.0692e-10	99.7091	1.0000

Fig. 8: The Comparison of watermarked audio and recovered watermarked audio

From all the results derived above it can be concluded that proposed methodology is much efficient in terms of PSNR, correlation with original watermark, computational time, complexity and invisibility as compared to existing other methods for the same. Proposed method is more imperceptible and a robust combined algorithm of digital watermarking, which is based on advanced spread spectrum methodology.

V. Conclusion

The scientific art of scripting secret messages such that no one except the sender and the intentional receiver could guess the presence of the message is defined as the steganography. It is a type security via obscurity. Steganography is not a new form of science. Replacement of non-useful data in various computer files like audio, video or text or graphics with different invisible data bits is the working principle of Steganography. Plain or cipher text or images are the hidden data. The Audio Steganography used in computer systems embed the secret memo in the digital audio signals. The commonly used audio format files AU, WAV and MP3 are used to insert the classified data as the implementation of current audio steganography softwares. The information which is being transmitted from one place to another is vulnerable to various types of active and passive attacks. Therefore, the securing of the information is a very major challenging aspects of communication in today' time. A hybrid method for audio steganography (using modified Direct Sequence Spread spectrum) and cryptography (using advanced random permutation with multiple key applications) has been proposed in this paper.

References

[1]. *Rashid Ansari, Hafiz Malik, Ashfaq Khokhar," Data-Hiding in Audio Using Frequency-Selective Phase Alteration".0-7803-8484-9/04/$20.00, 4004 IEEE, V-389, ICASSP 2004.*

[2]. *Mark Sterling, Edward L. Titlebaum, Xiaoxiao Dong, 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.*

[3]. *Xue-Min RU, Hong-Juan Zhang , Xiao Huang, "Steganalysis of Audio: Attacking The Steghide". Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005.*

[4]. *Anand Gupta, Deepak Kumar Barr, Deepali Sharma, "Mitigating the Degenerations in Microsoft Word Documents : An Improved Steganographic Method". 978-1-4244-3314-809$25.00 2009 IEEE.*

[5]. *Cairong Li, Wei Zeng, Haojun Ai, Ruimin Hu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM". 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.*

[6]. *Zhiping Zhang Xihong Wu, " An Audio Covert Communication System for Anolog Channels". 2010 International Conference on Electrical and Control Engineering".*

[7]. *Kaliappan Gopalan, "Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding". 978-1-4244-7116-4/10/$26.00 ©2010 IEEE.*

[8]. *Dmitriy E. Skopin, Ibrahim M. M. El-Emary, Rashad J. Rasras, Ruba S. Diab, "Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal". 978-1-4244-5848-6/10/$26.00 ©2010 IEEE.*

[9]. *Marcus Nutzinger, Christian Fabian, Marion Marschalek, "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media". 2010 sixth International conference on Intelligent Information Hiding and Multimedia Signal Processing.*

[10]. *Rizky M. Nugraha, "Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data". 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.*

[11]. *Sarosh K. Dastoor, "Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices" 2011 IEEE.*

[12]. *Bo Liu, Erci Xu, Jin Wang, Ziling Wei, Liyang Xu, Baokang Zhao, Jinshu Su , "Thwarting Audio Steganography Attacks in Cloud Storage Systems". 2011 International Conference on Cloud and Service Computing.*

[13]. *Muhammad Asad, Junaid Gilani, Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography". ©2011 IEEE.*

[14]. *Saswati Ghosh, Debashis De, Debdatta Kandar, "A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network". 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.29-33.*

[15]. *Pooja P. Balgurgi, Prof. Sonal K. Jagtap, "Intelligent Processing: An Approach of Audio Steganography".2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.*

[16]. *Ming Li,, Michel K. Kulhandjian, Dimitris A. Pados, E, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, JULY 2013.*

[17]. *Parul Shah, Pranali Choudhari and Suresh 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.*

[18]. *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. © 2008 IEEE.*

[19]. *S. Hernández-Garay, R. Vázquez-Medina, L. Niño de Rivera and V. Ponomaryov, "Steganographic Communication Channel Using Audio Signals", National Polytechnic*

Institute, 12th International Conference on Mathematical Methods in Electromagnetic Theory June 29 – July 02, 2008, Odesa, Ukraine.

[21]. Jisna Antony, Sobin c. c,Sherly A. P, "Audio Steganography in Wavelet Domain – A Survey". International Journal of Computer Applications (0975 – 8887) Volume 52– No.13, August 2012.

[24]. Suvajit Dutta, Tanumay Das, SharadJash, DebasishPatra, Dr.Pranam Paul, "A Cryptography Algorithm Using the Operations of Genetic Algorithm &Pseudo Random Sequence Generating Functions". International Journal of Advances in Computer Science and Technology, Volume 3, No.5, May 2014.

[25]. Prabhsimran Singh, Sukhmanjit Kaur, SabiaSingh , "Cryptography: An Art of Data Hiding". Prabhsimran et al, / International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (1), 2015, 117-120. ISSN: 2312-7694