UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

Effective Security Mechanism for Audio Steganography

Garima Malik

Department of Computer Science & Engineering, B.P.S Women University, Sonepat

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 security of the information is one of the most 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 the invention of steganography and cryptography, it was challenging to transfer secure information and, thus, to achieve secure communication environment. Some of the techniques employed in early days are writing with an invisible ink, drawing a standard painting with some small modifications, combining two images to create a new image, shaving the head of the messenger in the form of a message, tattooing the message on the scalp and so on [12]. Normally an application is developed by a person or a small group of people and used by many. Hackers are the people who tend to change the original application by modifying it or use the same application to make profits without giving credit to the owner. It is obvious that hackers are more in number compared to those who create. Hence, protecting an application should have the significant priority. Protection techniques have to be efficient, robust and unique to restrict malicious users. The development of technology has increased the scope of steganography and at the same time decreased its efficiency since the medium is relatively insecure. This lead to the development of the new but related technology called "Watermarking". Some of the applications of watermarking include ownership protection, proof for authentication, air traffic monitoring, medical applications etc [9, 17]. Watermarking for audio signal has greater importance because the music industry is one of the leading businesses in the world. Steganography works by replacing bits of useless or unused data in regular computer files such as graphics, sound, text, HTML, or even video with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. In this paper we propose a hybrid approach for audio steganography (using modified Direct Sequence Spread spectrum) cryptography (using advanced random permutation with multiple key applications).

II. OVERVIEW OF WORK

An audio watermarking technique can be classified into two groups based on the domain of operation. One type is **time domain** technique and the other is **transformation based method**. The time domain techniques include methods where the embedding is performed without any transformation. Watermarking is employed on the original samples of the audio signal. One of the examples of time domain watermarking technique is **the least significant bit** (LSB) method. In LSB method the watermark is embedded into the least significant bits of the host signal. As against these techniques, the transformation based watermarking methods perform watermarking in the transformation domain.

In general, the time domain techniques provide least robustness as a simple low pass filtering can remove the watermark [5]. Hence time domain techniques are not advisable for the applications such as copyright protection and airline traffic monitoring; however, it can be used in applications like proving ownership and medical applications.

A. LSB Coding

This technique is one of the common techniques employed in signal processing applications. It is based on the substitution of the LSB of the carrier signal with the bit pattern from the watermark noise [17]. The robustness depends

DOI10.17148/IARJSET.2017.4717

on the number of bits that are being replaced in the host signal. This type of technique is commonly used in image watermarking because, each pixel is represented as an integer hence it will be easy to replace the bits. The audio signal has real values as samples, if converted to an integer will degrade the quality of the signal to a great extent. The operation of the 2-bit LSB coding is shown in Figure 1 below.

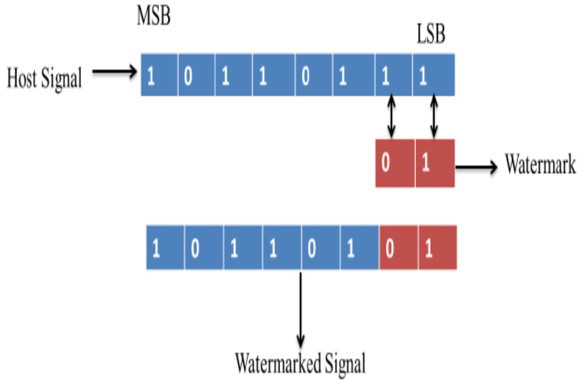

Figure 1: LSB Coding

B. Spread Spectrum Technique

These techniques are derived from the concepts used in spread spectrum communication [17]. The basic approach is that a narrow band signal is transmitted over the large bandwidth signal which makes them undetectable as the energy of the signal is overlapped. In the similar way the watermark is spread over multiple frequency bins so that the energy in any one bin is very small and certainly undetectable [18].

In spread spectrum technique, the original signal is first transformed to another domain using domain transformation techniques [17]. The embedding technique can use any type of approach for example quantization. Zhou et al. proposed an algorithm embedding watermark in 0th DCT coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal. Both embedding and extraction procedure can be interpreted using Figure 4. The original signal is transformed into frequency domain using DCT. Then watermark is embedded to the sample values in that domain. Reverse procedure is followed to obtain the watermarked signal [19]. This process of generating embedded signal is shown as embedding procedure in Figure 2 below.

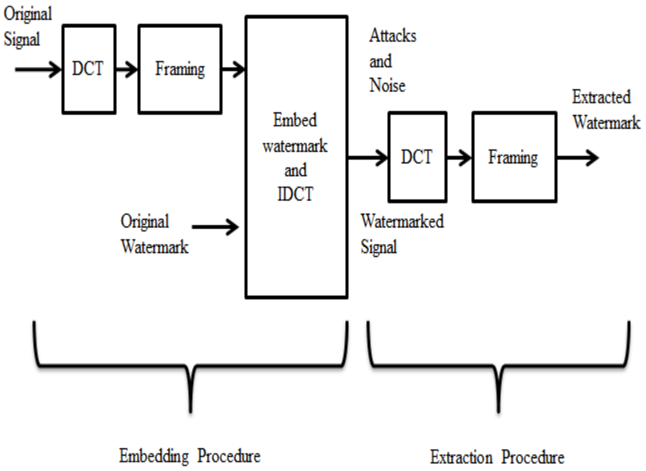

Figure 2: Example for spread spectrum technique

III. PROPOSED WORK

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Two versions of SS can be used in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated

DOI10.17148/IARJSET.2017.4717

with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.
The steps for implementation of proposed method are as follows:

A. AUDIO WATERMARKING

A1. EMBEDDING OF WATERMARK

- First of all read cover audio signal and get equivalent 2D matrix & calculate size of matrix i.e. rows and column. Read watermark image and get equivalent 2D matrix & calculate size of matrix i.e. rows and column. Convert watermark matrix into binary matrix & reshape binary matrix into row matrix.
- Get spreading size by multiplying spreading factor i.e. 2 with total number of elements of binary watermark matrix and generate a random binary key sequence according to spreading size, so as to provide security. Encode watermark matrix by Binary XOR-ing of row vector watermark matrix with key sequence. Now, encoded watermark matrix has a double size as compared to that of original.
- If cover image is too big then divide cover image matrix into two parts. Select a block size, which must be suitable to the size of first part of cover image matrix & divide cover image matrix into first and second part.
- Segmentation of first part matrix into an array of sub-matrix is given below. Each sub-matrix has a specific 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.

A2. EXTRACTION OF WATERMARK

- Read audio cover signal and audio watermarked signal & calculate size of cover audio signal. Read watermark image and calculate size of watermark image. Also calculate number of elements in watermark image.
- Select block size of 10 so as to increase the spreading and divide both images i.e. cover and marked audio into two parts. Declare empty cell having array of empty matrices so as to fill these with first part of both matrices.
- Also declare threshold value so as to fill the empty cell up to a certain limit. Application of discrete cosine transform on both cell. Division of 3rd element of each matrix of watermarked signal by that of original audio cover signal.
- Decoding of watermark components or removal of key sequence. Reconstruction of extracted watermark according to size of original watermark image .Plotting of both watermark images i.e. original and extracted.

B. AUDIO STEGANOGRAPHY

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. 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 parts (real and imaginary) of normalized audio.
19. Saving of the new encrypted audio.

B2. 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.

IV. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography is not a new form of science. Steganography works by replacing bits of useless or unused data in regular computer file such as graphics, sound, text, HTML, or even video with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. The information which is being transmitted from one place to another is vulnerable to various types of active and passive attacks. Therefore, the security of the information is one of the most 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.

DOI10.17148/IARJSET.2017.4717