Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Designing and Evaluation of Performance of a Spread Spectrum Technique for Audio Steganography

Heena Malik[*], **Sandeep Singh Kang**

Department of Computer Science
Punjab Technical University
India

Abstract— Steganography is the art and science of hiding that a communication is taken place. It embeds the secret file (text, audio or image) in other carrier file. Audio information hiding has attracted more attentions recently. Spread spectrum (SS) technique has developed rapidly in this area due to the advantages of good robustness and immunity to noise attack. Spread spectrum techniques really of digital communications systems. Two commonly spread spectrum techniques are used direct sequence spread spectrum (DSSS) and frequency hopped spread spectrum (FHSS). Implementation of steganography in audio data using Direct Sequence Spread Spectrum method has been presented in this thesis. The message is transmitted through noise-like wave. This method can be applied to embed messages in audio data. The embedded audio data will be heard as noise. In this thesis Direct Sequence Spread Spectrum method is used. A key is needed to embed messages into noise , this key is used to generate pseudo-random key sequence. The information to be embedded must first modulated using the pseudo- random key sequence. Also, Random location selection to embed the data within the cover image pixels is also proposed in the work. These modifications give a more secure stegno-graphic system, making guesses about the bit-rate or message length less feasible. The proposed stego and extraction system uses DSSS technique. These are used to increase the security and robustness of the system. Improvement has been achieved in robustness on the expense of reducing the capacity of hiding. The imperceptibility of the stego audio and extracted image is assessed by using peak signal-to-noise ratio (PSNR) and normalized correlation measure.

Keywords— Audio Steganography; Cryptography Spread Spectrum (SS) technique; Information Security, secret Key

I. Introduction

Before the invention of steganography and cryptography, it was challenging to transfer secure information and, thus, to achieve secure communication environment [1]

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. [1] [5] [8].

A. Steganography and Watermarking

- *Steganography*

Steganography is evolved from the ancient technique known as the "Cryptography". Cryptography protects the contents of the message [13]. On the other hand, steganography is a technique to send information by writing on the cover object invisibly. Steganography comes from the Greek word that means covered writing (stego = covered and graphy = writing) [3]. Here the authorized party is only aware of the existence of the hidden message. An ideal steganographic technique conceals large amount of information ensuring that the modified object is not visually or audibly distinguishable from the original object.

The steganography technique needs a cover object and message that is to be transported. It also requires a stego key to recover the embedded message. Users having the stego key can only access the secret message. Another important requirement for efficient steganographic techniques is that, the cover object is modified in a way that the quality is not lost after embedding the message.

- *Watermarking*

Watermarking is a technique through which the secure information is carried without degrading the quality of the original signal. The technique consists of two blocks:

(i) Embedding block
(ii) Extraction block

The system has an embedded key as in case of a steganography. The key is used to increase security, which does not allow any unauthorized users to manipulate or extract data. The embedded object is known as watermark, the watermark embedding medium is termed as the original signal or cover object and the modified object is termed as embedded signal or watermarked data [13].

B. Image and Audio Watermarking

Watermarking technique has evolved considerably from its origin [8]. Due to evolution of technology the medium of transmission has been changed. Watermarking is employed in digital media such as image and audio. The watermarking technique, in which the cover objects as discussed in Section 1.1.2, is image (audio) then the process is termed as Image (Audio) Watermarking. Audio watermarking is quite challenging than image watermarking due to the dynamic supremacy of human auditory system (HAS) over human visual system (HVS) [12].

C. Requirements of efficient watermarking techniques

*Ac*cording to IFPI (International Federation of the Phonographic Industry) [4], audio watermarking algorithms should meet certain requirements. The most significant requirements are perceptibility, reliability, capacity, and speed performance [9].

Perceptibility: One of the important features of the watermarking technique is that the watermarked signal should not lose the quality of the original signal. The signal to noise ratio (SNR) of the watermarked signal to the original signal should be maintained greater than 20dB [4]. In addition, the technique should make the modified signal not perceivable by human ear.

Reliability: Reliability covers the features like the robustness of the signal against the malicious attacks and signal processing techniques. The watermark should be made in a way that they provide high robustness against attacks. In addition, the watermark detection rate should be high under any types of attacks in the situations of proving ownership. Some of the other attacks summarized by Secure Digital Music Initiative (SDMI), an online forum for digital music copyright protection, are digital-to-analog and analog-to-digital conversions, noise addition, band-pass filtering, time-scale modification, echo addition, and sample rate conversion [10].

Capacity: The efficient watermarking technique should be able to carry more information but should not degrade the quality of the audio signal. It is also important to know if the watermark is completely distributed over the host signal because, it is possible that near the extraction process a part of the signal is only available. Hence, capacity is also a primary concern in the real time situations [4].

Speed: Speed of embedding is one of the criteria for efficient watermarking technique. The speed of embedding of watermark is important in real time applications where the embedding is done on continuous signals such as, speech of an official or conversation between airplane pilot and ground control staff. Some of the possible applications where speed is a constraint are audio streaming and airline traffic monitoring. Both embedding and extraction process need to be made as fast as possible with greater efficiency [4].

Asymmetry: If for the entire set of cover objects the watermark remains same; then, extracting for one file will cause damage watermark of all the files. Thus, asymmetry is also a noticeable concern. It is recommended to have unique watermarks to different files to help make the technique more useful [4].

D. Applications of Watermarking

Ownership protection and proof of ownership: In ownership protection application, the watermark embedded contains a unique proof of ownership. The embedded information is robust and secure against attacks and can be demonstrated in a case of dispute of ownership. There can be the situations where some other person modifies the embedded watermark and claims that it is his own. In such cases the actual owner can use the watermark to show the actual proof of ownership [5] [11] [4].

Authentication and tampering detection: In this application additional secondary information is embedded in the host signal and can be used to check if the host signal is tampered. This situation is important because it is necessary to know about the tampering caused to the media signal. The tampering is sometime a cause of forging of the watermark which has to be avoided [5] [11] [4].

Finger printing: Additional data embedded by a watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of a multimedia file. The usage of an audio file can be recorded by a fingerprinting system. When a file is accessed by a user, a watermark, or called fingerprint in this case, is embedded into the file thus creating a mark on the audio. The usage history can be traced by extracting all the watermarks that were embedded into the file [7].

Broadcast monitoring: Watermarking is used in code identification information for an active broadcast monitoring. No separate broadcast channel is required as the data is embedded in the host signal itself which is one of the main advantages of the technique [4].

Copy control and access control: A watermark detector is usually integrated in a recording or playback system, like in the DVD copy control algorithm [8] or during the development of Secure Digital Music Initiative (SDMI) [7]. The copy control and access control policy detects the watermark and it enforces the operation of particular hardware or software in the recording set [11].

Information carrier: The blind watermarking technique can be used in this sort of applications. These applications can transfer a lot of information and the robustness of the algorithm is traded with the size of content [13]. *Medical applications:* Watermarking can be used to write the unique name of the patient on the X-ray reports or MRI scan reports. This application is important because it is highly advisable to have the patients name entered on reports, and reduces the misplacements of reports which are very important during treatment [4].

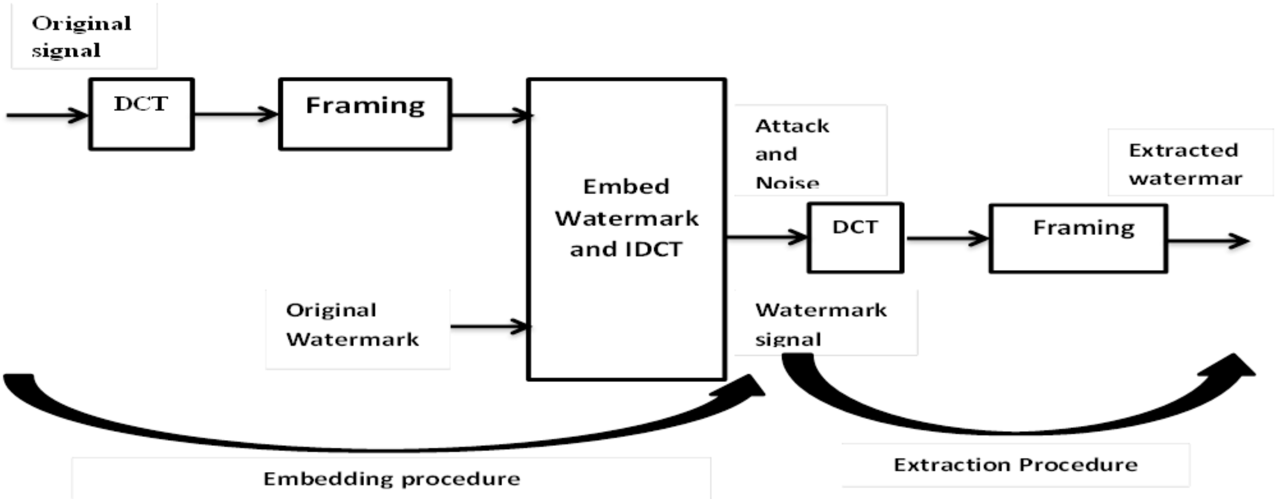

Fig 1. Example for spread spectrum technique[4]

II. RELATED WORK

Spread Spectrum Technique

These techniques are derived from the concepts used in spread spectrum communication [8]. 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 bits so that the energy in any one bit is very small and certainly undetectable [6].

In spread spectrum technique, the original signal is first transformed to another domain using domain transformation techniques [8]. 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 [7]. Both embedding and extraction procedure can be interpreted using Figure 1.1. 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. This process of generating embedded signal is shown as embedding procedure in Fig 1. Embedded signal will undergo some attacks, thus, noise is added to the signal. To extract the watermark the attacked signal is fed through extraction procedure. The procedure for extractions follows the same steps as that in embedding procedure as shown in Fig 1. The extraction process involves taking the attacked signal and applying DCT, framing the obtained components. And they obtained frames are used to obtain the watermark. Care is taken to replicate the procedure used for embedding process.

III. SPREAD SPECTRUM METHOD

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 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 math theory behind SS is quite complicated and goes beyond the scope of this project. However, Katzenbeisser and Petitcolas write about a generic steganography system that uses direct-sequence SS in Information Hiding Techniques for Steganography and Digital Watermarking. The following procedural diagram illustrates the design of that system when applied to our specific topic of audio steganography.

IV. PROBLEM FORMULATION

It can be concluded from the literature survey that, steganography does in fact have a number of disadvantages i.e. it has high overhead for hiding a few bits of information. This disadvantage can be overcome relatively easily. Another problem is that a steganographic system is rendered useless once it has been discovered. This also can be overcome by utilizing a key for the insertion and extraction of the hidden data. Also, Spread Spectrum method is known to be very robust, but as a consequence the cost is very large, the implementation is relatively complex, less secure and the information capacity is very limited. Current spread spectrum stegano-graphic applications with audio media are primarily limited to providing proof of copyright and assurance of content integrity. There is the potential to expand the applications to include the embedding of covert communications. Above mentioned problems related to spread spectrum can be overcome by using proposed methodology.

V. EMBEDDING AND EXTRACTION ALGORITHM

A. *Embedding of Watermark*

1. Reading of cover audio signal and getting of equivalent 2D matrix and calculate size.
2. Reading of watermark image and getting of equivalent 2D matrix and Calculate size of matrix.
3. Conversion of watermark matrix into binary matrix.
4. Getting of spreading size by multiplying spreading factor with total number of elements of binary watermark matrix.
5. Generation of a random binary key sequence according to spreading size, so as to provide security.
6. Encoding of watermark matrix by Binary XOR-ing of row vector watermark matrix with key sequence.
7. Now, encoded watermark matrix has a double size as compared to that of original.
8. If cover image is too big than division of cover image matrix into two parts.
9. Selection of a block size, which must be suitable to the size of first part of cover image matrix.
10. Division of cover image matrix into first and second part.
11. Segmentation of first part matrix into an array of sub-matrix.
12. Each sub-matrix has a specific number of elements which depends upon block size.
13. Application of Discrete Cosine Transform (DCT) on each element of all the sub-matrices.
14. Embedding of watermark by multiplication of encoded watermark matrix with cosine transform matrix.
15. Reconstruction of matrix by application of inverse discrete cosine transform on resultant matrix.
16. Joining of reconstructed matrix with second part of cover image matrix and Resizing of embedded image according to original audio cover signal
17. Plotting of frequency coefficients of both audio cover signals, so as to make comparison.

B. *Extraction of Watermark*

1. Reading of audio cover signal.
2. Reading of audio watermarked signal and Calculation of size of cover audio signal.
3. Reading of watermark image and Calculate size of watermark image.
4. Selection of block size, so as to increase the spreading.
5. Division of both images i.e. cover and marked audio into two parts.
6. Declaration of empty cell having array of empty matrices so as to fill these with first part of both matrices.
7. Declaration of threshold value so as to fill the empty cell up to a certain limit.
8. Application of discrete cosine transform on both cell.
9. Division of 3rd element of each matrix of watermarked signal by that of original audio cover signal.
10. Decoding of watermark components or removal of key sequence.
11. Reconstruction of extracted watermark according to size of original watermark image
12. Plotting of both watermark images i.e. original and extracted.

VI. PERFORMANCE METRIC

All the simulations have been performed in MATLAB R2012a. After simulation of program some results or output parameters i.e. value of PSNR, computational time and value of normalized correlation has been driven along with some figures, representing input and output from the simulation. First two figures are derived from simulation for embedding of watermark image in cover audio signal Fig.4.1 has been divided into two parts 1st part shows the plot of frequency coefficients of cover audio signal and 2nd part shows the plot of frequency coefficients of watermarked audio signal, so as to compare cover and watermarked audio signal. It can be easily seen that both have almost characteristic and almost similar, which can be proved by Normalized correlation value i.e. 0.9995.As a measure of the quality of a watermarked audio, the peak signal to noise ratio (PSNR) is typically used. PSNR in decibels (dB) is given below

```
psnr_den= (sum ((watermarked_audio-cover_mat).^2))
ww=(sum (watermarked_audio.^2))
PSNR=ceil(10*log10(ww/psnr_den))
```

The performance/ imperceptibility of the given digital watermarking algorithm is evaluated by calculating PSNR The PSNR value of embedded audio signal is 103.8254 dB. Digital watermarking, which is based on advanced spread spectrum methodology, PSNR (i.e. 103.8254 dB and 64.4317dB) and normalized correlation (i.e. 0.9995 and 0.8642) values are very high whereas, computational time (i.e. 2.708s and 1.6692s) is very low. Performance evaluation results shows that advancement of spread spectrum methodology improved the performance of the already existed watermarking algorithms that are based solely on the normal spread spectrum methodology. The simulation result shows that this algorithm is much better for invisible watermarking and has good robustness for some common signal processing operations.

VII. CONCLUSIONS

This is work can be extended by improving the performance of methodology by making it more robust and less complex for low frequency audio signal. Also, time consumption for embedding as well as for extraction of watermark can be reduced.

REFERENCES

[1] Youail, R.S., Samawi, V.W. and Kadhim, A-R. A- K. (2008) "Combining a Spread Spectrum Technique with Error-Correction Code to Design an Immune Stegosystem", Anti counterfeiting, Security and Identification (ASID 2008), IEEE, pp. 245-248.

[2] RU, X.M., ZHANG, H.J. and HUANG, X (2005), "steganalysis of audio: attacking the steghide", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou (2005), IEEE, pp. 3937-3942.

[3] Kexin, Z. (2010), "Audio Steganalysis of Spread Spectrum Hiding Based on Statistical Moment", 2nd International Conference on Signal Processing Systems (ICSPS-2010), IEEE, vol. 3, pp. 381-384.

[4] Gupta, A., Barr, D.K. and Sharma, D. (2009), *"Mitigating the Degenerations in Microsoft Word Documents: An Improved Steganographic Method"*, 2nd International Conference on Computer, Control and Communication (IC4-2009), IEEE, pp.1-6.

[5] Nutzinger, M., Fabian, C. and Marschalek, M. (2010), *"Secure Hybrid Spread Spectrum System for Steganography in Auditive Media",* Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2010), IEEE, pp. 78-81.

[6] Gao, S.; Hu, R.M.; Zeng, W.; Ai, H.J. and Li, C.R. (2008), *"A Detection Algorithm of Audio Spread Spectrum Data Hiding"*, International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM-2008), IEEE, pp. 1-4.

[7] Garay,S.H.; Medina, R.V.; Rivera, L. N. and Ponomaryov, V. (2008),*"steganographic communication channel using audio signals"*, International Conference on Mathematical Methods in Electromagnetic Theory (2008), IEEE, Odesa, Ukraine,

[8] Shah, P.; Choudhari, P. and Sivaraman, S. (2008), *"Adaptive Wavelet Packet Based Audio Steganography using Data History"*, Region 10 Colloquium and the Third ICIIS, Kharagpur, (2008), IEEE.

[9] Li, M., Kulhandjian, M., Pados, D.A., Batalama, S.N., Medley, M.J. and Matyjas, J.D. (2012), *"On the Extraction of Spread-Spectrum Hidden Data in Digital Media",* Communication and Information Systems Security Symposium, IEEE (ICC- 2012), pp. 1031-1035.

[10] Ghosh, S., De, D. and Kandar, D. (2012), *"A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network",* International Conference on Radar, Communication and Computing (ICRCC-2012), IEEE, SKP Engineering College, Tiruvannamalai, pp. 29-33.

[11] Skopin, D.E. ; El-Emary, I.M.M. ; Rasras R.J. and Diab R.S.(2010),*"Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal"*, International Conference on Advanced Computer Control (ICACC- 2010) , IEEE, vol. 5, pp. 29-32.

[12] Kumar, H. and Anuradha (2012), *"Enhanced LSB technique for Audio Steganography",* International Conference on Computing, Communication & Networking Technology (ICCCNT-2012), IEEE-20180, Coimbatore.

[13] Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B. and Su, J (2011), "Thwarting Audio Steganography Attacks in Cloud Storage Systems", International Conference on Cloud and Service Computing (2011), IEEE, pp. 279-284.