Audio Steganography by Direct Sequence Spread Spectrum

Rupanshi , Preeti , Vandana

Department of Computer Science and Technology
Hindu College of Enginnering,Sonipat,Haryana

Abstract-**Image steganography has widely developed. There are also many algorithm developed for it. Meanwhile, the interest in using audio data as cover object in steganography can be spelled out late emergence than image data. This paper discusses the implementation of steganography in audio data using Direct Sequence Spread Spectrum method. Spread Spectrum method is often used to send hidden message through radio waves. This message is transmitted through noise-like wave. Spread spectrum (SS) technique has developed rapidly in this area due to the advantages of good robustness and immunity to noise attack. Accordingly steganalysis of the SS hiding effectively verify the presence of the secrete message in an important issue. It embeds the secret file (text, audio or image) in other carrier file.**
Keyword-**Audio steganography, Direct sequence spread spectrum, Security key, DCT(direct cosine transfor)**

Text in image steganography is considered in this work. The proposed stegosystem uses Spread Spectrum technique which is applied in spatial domain together with error correction coding. These are used to increase the security and robustness of the system. Random location selection within the cover image pixels is also proposed in the work. Improvement has been achieved in robustness on the expense of reducing the capacity of hiding. The imperceptibility of the stego image is assessed by using peak signal-to-noise ratio (PSNR) measure. Attacks in the form of lossy compression and additive noise are considered. The performance of the proposed system has shown good immunity to moderate levels of channel noise and lossy compression ratios.

I.INTRODUCTION

A.Steganography

It is the science which deals with hidden information exchange. In a communication, only the sender and the intended recipient are supposed to know about, and extract, the secret message [1].
In steganography we have two parts. One part is the embedding and second part is extractging of the data. As we have shown in figure 1 that for embedding and extraction we need a cover medium and a stego key.

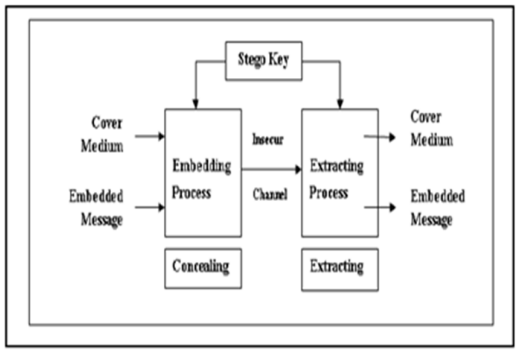


Figure1:- steganography

In technical steganography, the use of different cover media, like digital audio and video files or digital images, is possible [2]. Steganography is often mixed up with cryptography. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message.
The purpose of steganographic techniques is to transmit data secretly and to identify or protect the owner of information. Steganographic algorithms are an important field of research, as numerous applications do exist. These range from copyright protection of digital media to tamper proving, authentication, integrity proving and secure data transmission [3]. The key requirements for steganography are imperceptibility, robustness against destruction and a high data rate [4]. The latter is quite contrary to the invisibility of hidden information, because the more it is embedded, the easier it is for an observer to detect parts of the secret message. Various steganographic algorithms have been proposed, including echo-hiding, phase-coding, patchwork technique and spread spectrum [5]. Our research focuses on auditive data as cover media, such as voice calls or compressed and uncompressed digital sound files. To embed messages in digit To embed messages in digital audio data, the spread spectrum technique seems to be the most promising field of research.

B.Watermarking

Watermarking and data hiding have become a vibrant research area. Various kinds of multimedia files can be downloaded freely from the Internet. Watermarking is a technique through which the

secure information is carried without degrading the quality of the original signal. 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 [15] The embedding block consists of watermark, original signal (or cover object), and watermarking key as the inputs (creates the embedded signal or watermarked data) [15]. Whereas, the inputs for the extraction block is embedded object, key and sometimes watermark.

II.RELATED WORK

A.Direct sequence spread spectrum

A lot of work has been done in the field of information hiding in the context of the spread spectrum technology. In a DSSS system, a signal of low bandwidth is spread over a broad frequency range. Hence the power of the signal is decreased and thus the signal vanishes in the noise of the cover media. To extract an embedded signal from the cover, the receiver needs knowledge about the spreading process. This knowledge can therefore be described as a kind of secret key, needed as input to the system.

For embedding we used many technique.nFor example As explained by Rizky M. Nugraha et. Al. [8] Image steganography has widely developed. There are also many algorithm developed for it. Meanwhile, the interest in using audio data as cover object in steganography can be spelled out late emergence than image data. This paper discusses the implementation of steganography in audio data using Direct Sequence Spread Spectrum method. Spread Spectrum method is often used to send hidden message through radio waves. This message is transmitted through noise-like wave. The same method can be applied to embed message in audio data. The embedded audio data will be heard as noise. The Spred Spectrum method used in this paper is Direct Sequence Spread Spectrum. A key is needed to embed messages into noise, this key is used to generate pseudo-noise wave. The information to be embedded must first modulated using the pseudo-noise. This paper discusses implementation of the method in audio data to hide text message. Spread Spectrum method is known to be very robust, but as a consequence the cost is very large, the implementation is relatively complex, and the information capacity is very limited. This problem will also be discussed in this paper. Based on the test results, the author conclude that the implementation of Direct-sequence Spread Spectrum steganography on audio cover object is possible and practical to use. At least for the duration of the first 15 seconds of data. This method proved very robust against audio manipulation and very safe with the resulting noise is quite small. But the cost that it takes far more xpensice than the LSB method. The author is still planning further development of this method.

Xu Anying et. Al. [2] describes that Spread spectrum techniques were invented in the1950's as a means of improving the security and reality of digital communications systems, and they are regularly employed in wireless systems today. A narrowband data signal, such as a frequency shift keying (FSK) signal for example, is converted into a spread signal by modulating it with a wideband spreading signal that is independent of the data signal. This process caused the spread signal to occupy a spectral bandwidth far in excess of the bandwidth of the original data signal. The data signal at the decoder is recovered by correlating the spread signal with a synchronized copy of the spreading signal, also known as dispreading. The spread spectrum techniques for watermarking are very popular nowadays. Two commonly spread spectrum techniques are used direct sequence spread spectrum (DSSS) and frequency hopped spread spectrum (FHSS).

III.PROBLEM FORMULATION

From the previous work the conclusion comes out that, steganography does in fact have a number of disadvantages . In some cases it has been high overhead for hiding a few bits of information. This disadvantage can be overcome easily. There is an Another problem is that a steganographic system has security issues. This 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 very complex, less secure and the data storage is very less. spread spectrum stegano-graphic applications are used with audio media are primarily limited to providing proof of copyright and assurance of content integrity. There is also a disvantage so there is a need to expand the applications to include the embedding of communicationsIn main method we have two steps one is embedding method and second is extraction method.

A.Embedding method

B.Extraction method

In figure2 we have explained the embedding and extraction technique and a algorithm for it which is shown on page number 5. In this method main focus is on security level as the security level is increases at each step of the algorithm.

V. PERFORMANCE EVALUATION

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.

As shown in figure2 and figure3 we take a music WAV file and a image PAN file. In figure 2 the watermark is embedded behind the audio file. In figure3 the watermark has been extracted only some noise element are present in the extracted figure.

It can be easily seen that both input and output signals have almost characteristic and almost similar, which can be proved by Normalized correlation value i.e. 0.9227.As a measure of the quality of a watermarked audio, the peak signal to noise ratio (PSNR) is typically used.

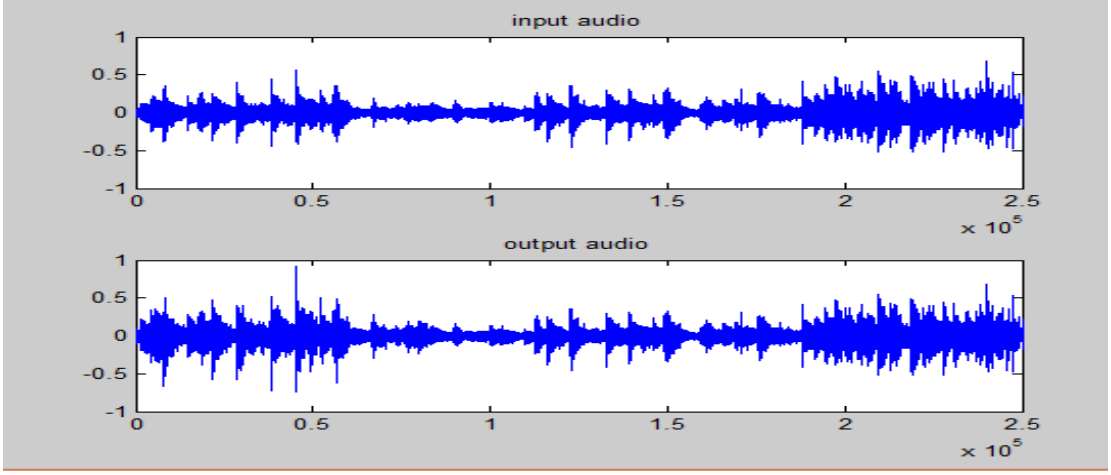


Figure 2:- Input and Output signals

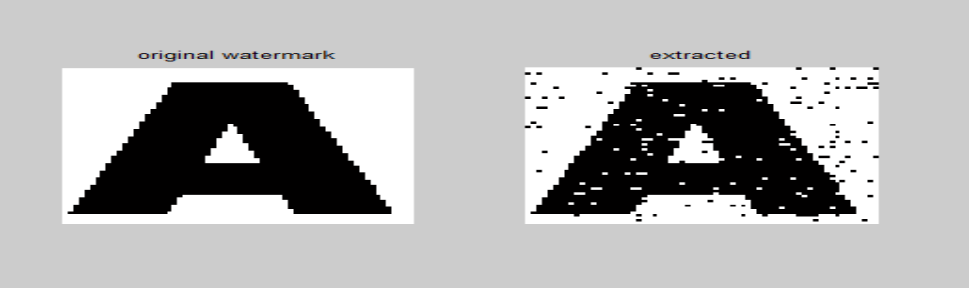
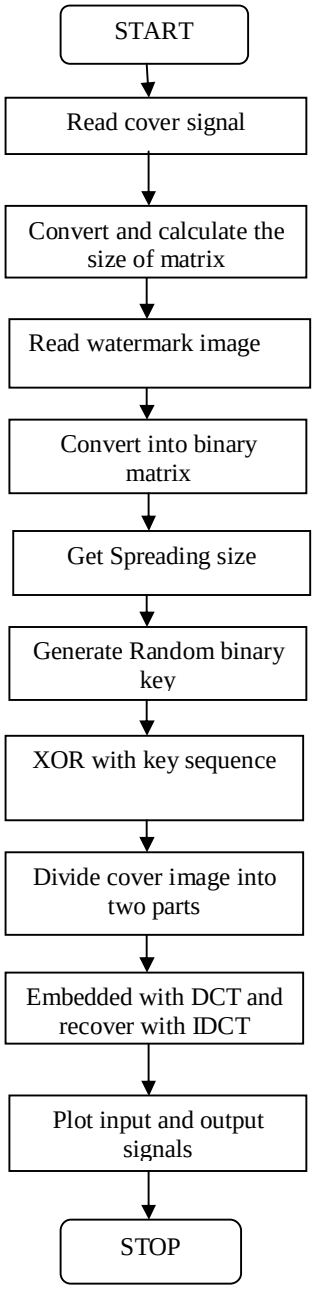


Figure3:- Original and extracted watermark

The performance/ imperceptibility of the given digital watermarking algorithm is evaluated by calculating PSNR The PSNR value of embedded audio signal is 87.3147 dB. Digital watermarking, which is based on advanced spread spectrum methodology, PSNR (i.e. 87.3147 dB and 62.2678dB) and normalized correlation (i.e. 0.9938 and 0.9227) values are very high whereas, computational time (i.e. 1.3594s and 0.8906s) 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.

VI.CONCLUSION

This work can be improved by using different steganography technique which are compatible for low frequency audio signal and more robust and easy to use. Time consumption can be less for embedding as well as for extraction of watermark.



REFERENCES

[1] H. Farid (2002) Detecting hidden messages using higher-order statistical models. In Proceedings of IEEE International Conference on Image Processing, pp. 905-908

[2] Harmsen J J, Pearlman W A (2003) Steganalysis of additive noise modelable information hiding. SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents. vol.5022, 21-24

[3] Seshadrinathan K, Sheikh H R, Bovik A C (2005) Detecting spread spectrum watermarks using natural scene statistics. In Proceedings of IEEE International Conference on Image Processing, vol. 2, 1106-
1109

[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.