International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 5, Issue 6, Oct. 2016, pp.1035-1037, ISSN 2278 -1412

A Review of Dwt and Lsb Based Audio Steganography

Monika Saxena[1], Uttam Mishra[2]
[1]*M.Tech Student, Dept. of ECE, Ojaswini Institute of Management and Technology, Damoh, M.P. India*
[2] *Assistant Professor, Dept. of ECE, Ojaswini Institute of Management and Technology, Damoh, M.P. India*

Abstract *– As a review of this paper present a novel method for digital audio steganography where encrypted covert data is embedded by DWT based and LSB based. Steganography may be a technique for hiding data in a host signal. The host signal may be a still image, speech or video and therefore the message signal that's hidden within the host signal can be a text, image or an audio signal. Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions,*

Keywords*: DWT, LSB, PSNR, Audio steganography,*

I. Introduction

The goal of steganography is to insert a message into a carrier signal so that it can- not be detected by unintended recipients. Due to their widespread use and availability of bits that can be changed without perceptible damage of the original signal images, video, and audio are widespread carrier media. Steganalysis attempts to discover hidden signals in suspected carriers or at the least detect which media contain hidden signals. Therefore, an important consideration in steganography is how robust to detection is a particular technique. We review the existing steganography and steganalysis techniques and discuss their limitations and some possible research directions.

Steganography, anonymity, and covert channels all refer to secret communications. Anonymity refers to communicating in a way that protects the identity of the sender and/or the receiver. Covert channels refer to the means of secretly communicating a small amount of information across tightly monitored channels by exploiting possible loopholes in the communication protocols (Simmons, 1998). Digital steganography refers to modifying a digital object (cover) to encode and conceal a sequence of bits (message) to facilitate covert communication. Digital steganalysis refers to orts to detect (and possibly prevent) such communication. Copyright marking refers to modifying a digital object so that its owner(s) can be identified. The goal of digital watermarking is to modify a digital object in a way that will both identify the owner and be hard to remove without destroying the object or making it unusable.

Steganography is usually employed in covert communication in military application and government communication application. Often it needs relatively high payloads in comparison to watermarking. The major needs that should be glad for good steganography algorithms include perceptual transparency, payload or capacity and robustness. High capacity is considered as a very important aspect for steganography when compared to watermarking. For watermarking, robustness must be a main aspect. Improvement for one among the mentioned requirements will tend to degrade the other performances as they're contradictory consistent with the magic triangle. Steganography has evolved into a digital strategy of hiding a get into some type of multimedia, such as an image, an acoustic file (like a .wav or mp3) or maybe a video file [1]. Stenographic systems are often divided into 2 classes. In which one is very existence of the message is kept secret and different non-steganography Systems. The main goal of steganography is to communicate securely in an exceedingly completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. That's not to information even exists. Steganography is of 3 types Audio, Image and Video. Through image steganography is that the additional illustrious of the 2, audio steganography is nowadays more secure due to the fact that the hackers don't suspect the presence of a hidden message in an audio file.

II. Literature Survey

Neha Gupta et. al[1] "Dwt and Lsb Based Audio Steganography", in this paper The main aim is to come up with a technique to hide the data in audio file in such a way there are no perceivable changes in the audio file after the message insertion. Also, if the message that is to hidden was also encrypted then the level of security would be hidden was also encrypted then the level of security would be further raised to a more satisfactory level. The person who got the message would only have the encrypted form of the message with no way of decrypting it so the hidden messages were to be discovered. Proposed scheme has been discussed in this paper for embedding image in cover audio file. Emphasis is on proposed scheme from simple LSB based data hiding in audio, and their robustness in term of steganolysis. Proposed method is better by using the concept of DWT (Discrete Wavelet Transform) and LSB technique. By taking the higher frequency from DWT and using in LSB (Least Significant Bit) we get the PSNR values.

Ross J. Anderson et. al[2] "On The Limits of Steganography", in this paper explored the limits of steganographic theory and practice. We started o by outlining a number of techniques both ancient and modern, together with attacks on them (some new); we then discussed a number of possible approaches to a theory of the subject. We pointed out the difficulties that stand in the way of a theory of \perfect covertness" with the same power as Shannon's theory of perfect secrecy. But considerations of entropy give us some quantitative leverage and the \selection channel"| the bandwidth of the stego key|led us to suggest embedding information in parity checks rather than in the data directly. This approach gives improved efficiency, and also allows us to do public key steganography. Finally, we have shown that public key steganography may sometimes be possible in the presence of an active warden.

Zoran Duric et. al.[3] "Information Hiding: Steganography and Steganalysis", in this paper Survey of methods for steganography and steganalysis was presented. It was shown that most methods used in digital steganography can be divided into embedding by modifying carrier bits and embedding using pairs of values.These methods were described formally and their uses, merits, and requirements were discussed. Various approaches to steganalysis were discussed; chisquare method was described and examples of its application were shown. Relationship between steganography and watermarking was also discussed and it was argued that, although superficially similar, these two fields have many differences and should be treated separately.

W. Bender et. al[4] "Techniques for data hiding", in this paper several techniques are discussed as possible methods for embedding data in host text, image, and audio signals. While we have had some degree of success, all of the proposed methods have limitations. The goal of achieving protection of large amounts of embedded data against intentional attempts at removal may be unobtainable.

Parul Shah et. al[5] "Adaptive Wavelet Packet Based Audio Steganography using Data History", in this paper The adaptive nature of the proposed AWPAS embedding scheme makes it possible to embed covert data anywhere in the host audio file. Embedding is performed irrespective of the magnitude of audio in time domain or frequency domain, because of which full payload is independent of the nature of the audio content. The modification of host audio is done by imposing a constraint which forces the modified value to be in the same range as its neighborhood. Due to this constraint the noise introduced due to embedding is very low compared to existing methods. This is evident from quantitative and qualitative analysis. The quality of the retrieved covert data is not affected by the proposed embedding scheme as can be seen from the zero bit error. The time required for embedding and retrieving is also much less. Moreover, AWPAS does not alter the pattern of the PSD, offering better concealment of the covert data. The characteristics of the proposed method are imperceptible covering capability, higher hiding capacity with superior SNR value and zero bit error which are the most desired features of any steganography technique.

III. Method

III.1. Audio Steganography

Like steganography in other media, the simplest method for steganography in audio is hiding information in Least Significant Bits (LSB) in the time domain, frequency domain or even in wavelet domain [3]. One of the problems of steganography in non-time domains is their unhiding errors [3]. Some of these methods employ LSB technique and combine it with other techniques such as error diffusion [4], minimum error replacement (MER) [5] and temporal masking effect [6]. In [1], [7] image steganography techniques are utilized for audio steganography. The aim of these methods is to increase robustness against MPEG compression. In [8] two techniques of spread spectrum and phase shifting are combined to increase robustness against additive noise for aerial data transmission. In [9] perceptually masked coefficients in the cepstral domain are modified to increase robustness against additive noise and band-pass filtering. In [1] the host audio is first decomposed into three levels of DWT coefficients and the LLH band is used for embedding, sampled coefficients in LLH band are converted into 2D image and a well established image-in image steganography method is used for embedding [10]. Here though the bit error is zero for recovered data, SNR values are not encouraging. Furthermore increase in hiding capacity degrades SNR further considerably. Noise introduced here is of high frequency in nature whereas embedding is performed in

lower frequency band LLH which makes the noise clearly audible. In [2], [11], [6], [12], encrypted covert data is embedded into integer wavelet coefficients of host audio LSB of wavelet transform signal. Though the BER is zero in all these methods, SNR is inferior compared to our proposed method. The best result out of these papers is for Pop music where 80% of full payload gives SNR of around 47 dB whereas the proposed method gives an SNR of 49.3 dB for the same music category.

As mentioned earlier, perceptual transparency and hiding capacity is more important for steganography applications than robustness. The objective of the proposed method is to formulate an embedding procedure with better hiding capacity and high SNR. In the proposed method, we were able to achieve high hiding capacity while maintaining appreciably high SNR values.

A typical steganographic embedding method has two parts. In the first part a message is prepared and in the second it is embedded in the carrier object e.g., an image. The preparation can include compression and encryption. It can be assumed that the sender and the intended recipient share a key that is used to encrypt the message. Either compression or the encryption is expected to produce a random-looking sequence of bits. In addition, since the message embedding needs to be reversible a small amount of formatting data such as a password and a message length needs to be included with the message. The formatting information and the message are concatenated and embedded into the cover using the same algorithm. Therefore, it will be assumed here that a message is a random bit sequence and only the message embedding and extraction processes will be considered.

IV. Conclusion

This paper has reviewed the mainly latest research trends and proposed the DWT and Lsb method. In this discrete wavelet transform and least significant bit method are proposed for Audio Steganography. In this paper we have presented Dwt and Lsb Based Audio Steganography.

References

[1] Gupta, Neha, and Nidhi Sharma. “Dwt and Lsb Based Audio Steganography” Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014.

[2] Anderson, Ross J., and Fabien AP Petitcolas. “On the limits of steganography” IEEE Journal on selected areas in communications 16.4 (1998): 474-481.

[3] Duric, Zoran, Michael Jacobs, and Sushil Jajodia. “Information Hiding: Steganography and Steganalysis” Handbook of Statistics 24 (2005): 171-187.

[4] Bender, Walter, et al. “Techniques for data hiding” IBM systems journal 35.3.4 (1996): 313-336.

[5] Shah, Parul, Pranali Choudhari, and Suresh Sivaraman. “Adaptive wavelet packet based audio steganography using data history” IEEE Region 10 and the Third international Conference on Industrial and Information Systems 2008.

[6] Johnson, Neil F., et al. "Information hiding: steganography and watermarking—attacks and countermeasures." Journal of Electronic Imaging 10.3 (2001): 825-826.

[7] Wu, M., & Liu, B. (2013). “Multimedia data hiding” Springer Science & Business Media.

[8] Amin, Muhalim Mohamed, et al. “Information hiding using steganography” Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.

[9] Anderson, Ross J., and Fabien AP Petitcolas. “On the limits of steganography” IEEE Journal on selected areas in communications 16.4 (1998): 474-481.

[10] K. Gopalan, “Audio steganography using bit modification”, Proceedings of International Conference on Multimedia and Expo, Vol. 1, pp.629- 632, 6-9 July 2003.

[11] N. Cvejic, T. Seppiinen, “Increasing the capacity of LSB-based audio steganography”, IEEE Workshop on Multimedia Signal processing, pp. 336 -338, 2002.

[12] N. Cvejic, T. Seppanen, “Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method”, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04), vol. 2, pp. 533, 2004.

[13] N. Cvejic, and T. Seppnen, “Reduced distortion bit-modification for LSB audio steganography”, Journal of Universal Computer Science, vol. 11, no.1, pp. 56-65, January 2005.

[14] Mohamed A. Ahmed, Miss Laiha Mat Kiah, B.B. Zaidan and A.A. Zaidan, ”A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm”, Journal of Applied Sciences,vol. 10, pp. 59-64, 2010.

[15] D. Gruhl, W. Bender, “Echo hiding”, Proceeding of Inforomation Hiding Workshop, pp. 295315, 1996.

[16] Erfani, Y. and Siahpoush, S, “Robust audio watermarking using improved TS echo hiding”, Digital Signal Processing, vol. 19, pp.809-814, September 2009

[17] B. Paillard, P. Mabilleau, S. Morissette, J. Soumagne, “PERCEVAL: Perceptual Evaluation of the Quality of Audio Signals” journal of Audio Engeneering Society, vol. 40, pp 21-31, February 1992.