Message Guided Adaptive Random Audio Steganography using LSB Modification

Taruna
M.Tech
DCRUST, Murthal

Rishabh Jain
Assistant Professor
NIEC, New Delhi

ABSTRACT

Steganography is an art of hiding secret messages such that its very presence can't be identified. Techniques which hide more secret data in cover files are better and they will be more better if they doesn't affect transparency of cover signal and make steganalysis difficult. We propose a technique which provide keyless randomization to insert secret information in multiple and variable LSBs. Using this method, binary cover signal is divided into blocks of size 8x8 with 16 bits per sub block, and then checking each sub block's first two MSBs to find how many LSBs will be used for insertion of secret data bits. Results show that there is no noticeable difference between cover audio signal and stego audio signal. Capacity and security increases due to the use of variable number of LSBs for insertion and keyless randomization provided by counting out technique.

General Terms

Security, robustness, algorithm, capacity, transparency.

Keywords

Data hiding, Audio steganography, Least significant bit (LSB), Most significant bit (MSB), counting out technique, Human Auditory System (HAS), Robustness.

1. INTRODUCTION

Digitalization of data facilitates us with fast and simple mean of communication. Easy-to-use software's make it easy to create and modify digital information. But this simplicity and pace of digital communication pose a threat for security of information. From years scientists are searching for better and better techniques for securing information from eavesdroppers. In a broader sense these techniques are known as either cryptographic or steganographic techniques. Both techniques enhance security of information exchanged, but in different manner. Cryptographic algorithms are designed to convert information in a format not understood by person other than sender and intended receiver.

Steganography is basically information hiding technique. In this data hiding techniques, the main goal is to hide message 'M' (text, image or audio) in cover (audio or video) file 'F' to obtain new file 'F^1', practically indistinguishable from 'F'. Watermarking is also a technique similar to steganography. The difference is, in steganography message is hidden in such a way that an eavesdropper cannot detect the presence of 'M' in 'F^1' while in watermarking it is done in such a way that an eavesdropper cannot remove or replace 'M' from 'F^1'[1]. Watermarking preserves quality of signal carrying secret data and also protects it against manipulations trying to remove hidden secret data from marked object.

Recently scientists design steganographic techniques considering the fact that there is natural limitation in the auditory and visual perceptions of human. This benefit by minimizing the difference between the original medium and the one obtained after embedding the hidden data. Although capacity of audio files, i.e. amount of data that can be embedded into cover audio file maintaining perceptual transparency is lower as compared to data rate of images or video files as cover. The reason is the dimension of audio files which is less than two dimensional image or video files [2]. Also embedding data in cover audio file is more difficult than embedding data in images [3].

In spite of difficulty in embedding and low data rate of audio files, they are preferred over images. This is because many attacks that are malicious against image steganography algorithms (e.g. geometrical distortions, spatial scaling, etc.) cannot be implemented against audio steganography schemes [2]. Thus Embedding information into audio seems more secure due to less steganalysis techniques for attacking to audio [2]. Also HAS is resistant to low scale audio alterations and thus it can't detect the phase changes. Unlike stego digital audio files, when original and watermarked digital images are compared, a clear difference between the two will be there due to stretching of pixels. This is undesirable for data hiding techniques [4].

A good audio steganographic system (stego system) has three characteristics viz. transparency, capacity and robustness. These characteristics are called magic triangle for data hiding.

- Transparency: Transparency is a measure of distortion caused due to modification in signals. A good steganographic method performs insertion of data fulfilling perceptual transparency factor. Perceptual transparency refers to inaudibility of distortion in cover audio file. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS and the host media [5].

- Robustness: Robustness refers to the ability of stego file to withstand attacks. These attacks can be unintentional or intentional. Unintentional attacks generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, re-quantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colored noise, rescaling, rotation (for image and video steganography schemes), resizing, cropping, random chopping, and filtering attacks [6].

- Capacity: It refers to the quantity of data that can be concealed in cover file without violating the other two characteristics. The embedding capacity is the all included embedding capacity (not the payload) and can be measured in percent (%), bits per second or frame and bits per mega byte or kilo byte audio signal.[7]

These three characteristics are interdependent and contradicted. The maximum number of bits of cover audio signal used for data embedding without causing audible distortion to the cover audio signal restricts the amount of data for hiding purpose, i.e. capacity [8]. If capacity is improved without taking care of transparency of host audio signal, robustness is affected. In such case attacks will be easy and the basic idea of steganography will diminish. Thus all the three factors depend on each other and improvement in one of them affects the others. In this paper, two approaches are combined to improve capacity and robustness of the steganographic system, without affecting perceptual transparency of the host audio signal. The algorithm can be applied on audio, image or video as cover medium; secret data can be in the form of audio, images, text etc. In this paper, the proposed algorithm is demonstrated using audio file as cover medium and text data as secret data to be embedded in audio cover. Rest of the paper is organised as follows: Section II: describes the existing method improving capacity, Section III: describes the proposed algorithm, Section IV: gives the results and Section V: concludes the paper.

2. COMPARISON AND EVALUATION OF EXISTING TECHNIQUES

Least significant bit (LSB) technique of data hiding is one of the simplest algorithms with very high capacity from 8kbps to 44.1 kbps, when all samples are used [9]. To further increase capacity, number of LSBs used for embedding secret data can be increased. But this introduces noise that becomes noticeable as the number of LSBs used for embedding of data increases [9]. This imposes limit on the number of bits of cover signal that can be replaced by message bits. N. Cvejic and T. Seppanen,, in their paper "Increasing Robustness of LSB Audio Steganography using a novel embedding method" [10], show that maximum 4 LSBs of host audio signal can be used for embedding purpose(if 16 bits per sample are used) without causing noticeable perceptual transparency.

To overcome this limit on maximum number of LSBs used for embedding without affecting perceptual transparency, H.B.Kekre et al in their paper, “Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding”, introduces a range of LSBs which can be used for embedding, depending upon the MSBs[8]. The idea is to check the MSBs of the samples of cover audio and depending upon the values of MSBs, the number of LSBs for embedding is decided. This focuses only on one side of magic triangle, i.e. capacity, keeping other side named transparency, constant. Robustness is left untouched.

3. PROPOSED METHOD TO IMPROVE CAPACITY AND ROBUSTNESS

This method adds robustness factor to the above method. Cover audio signal is converted into binary bits which are then segmented into 8x8 blocks, with each sub block carrying 16 bits. Then the above explained method is applied on 16 bits of each sub block and the sub block used for embedding is evaluated by using counting out technique [3]. Counting out technique is a repetitive process of picking an item from a set and omitting the picked item for the next iteration. Data to be embedded will act as a key to find position of next sub block for embedding and in this way different embedding paths can be achieved for each secret data. So the proposed method will provide adaptive randomization and increased capacity without affecting the imperceptibility.

3.1 Steps for data embedding

1. Read the cover audio signal and convert it into sequence of binary bits.
2. Read the message text to be embedded. Convert it into a sequence of binary bits.
3. Segment binary audio into 8x8 sub blocks each with 16 bits.
4. Every message bit from step 2 is embedded into the variable and multiple LSBs of each sub block and that too in random sub blocks of the digitized cover audio.
5. For first sub block, first 2 MSBs of cover samples are checked:

- If they are ‘00’, then use 4 LSBs for data embedding.
- If they are ‘01’, then use 5 LSBs for data embedding.
- If they are ‘10’, then use 6 LSBs for data embedding.
- If they are ‘11’, then use 7 LSBs for data embedding.

6. The message bits embedded are converted to decimal and this acts as a key for the next pixel/sub block to which data is to be embedded
7. Repeat step 5 for each sub block obtained from step 6 and strike out the sub block used once for next iteration.
8. The modified cover audio samples are then written to the file forming the stego audio signal.

3.2 Steps for data retrieval

1. Read the stego audio signal.
2. Convert it into a sequence of binary bits.
3. Segment binary audio into 8x8 sub blocks each with 16 bits.
4. For first sub block, check first 2 MSBs

- If they are ‘00’, retrieve 4 LSBs.
- If they are ‘01’, retrieve 5 LSBs.
- If they are ‘10’, retrieve 6 LSBs.
- If they are ‘11’, retrieve 7 LSBs.

5. Bits obtained from step 4 are converted to decimal and next sub block for retrieval is obtained.
6. Repeat step 4 for each sub block obtained from step 5 and strike out the sub block retrieved once.
7. The retrieved message bits are obtained from all sub blocks.

4. FIGURES

Flow chart in figure 1 shows the main steps for embedding data in cover audio signal of the proposed algorithm.

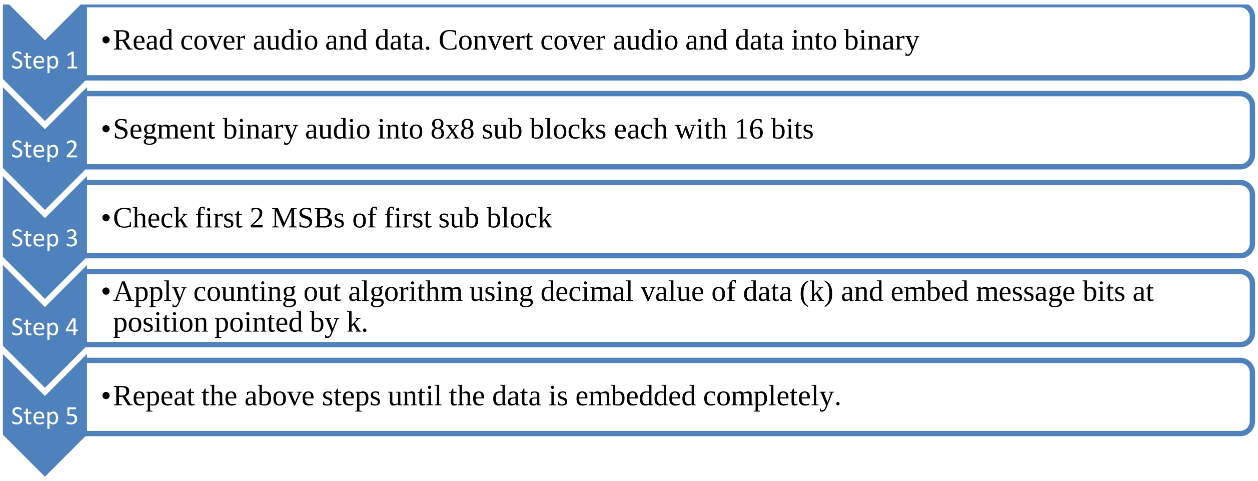
Step 1
•Read cover audio and data. Convert cover audio and data into binary
Step 2
•Segment binary audio into 8x8 sub blocks each with 16 bits
Step 3
•Check first 2 MSBs of first sub block
Step 4
•Apply counting out algorithm using decimal value of data (k) and embed message bits at position pointed by k.
Step 5
•Repeat the above steps until the data is embedded completely.

Fig 1: Flow chart showing main steps of proposed algorithm for data embedding in cover audio file

5. COMPARATIVE ANALYSIS OF EXISTING TECHNIQUES

Proposed method was tested on 3 audio sequences of different duration and sizes. Audio sequences were represented by 16 bits per sample. Duration of the clips ranged from 3 to 4 minutes .The performance of the proposed method is analyzed in terms of PSNR (Peak Signal-to- Noise Ratio). Table I gives the results of the proposed method that considers 2 MSBs for increasing the capacity of the cover audio and use counting -out to increase randomization. From Table, it can be seen that PSNR values of proposed algorithm are better than existing algorithm which only improve capacity of cover audio considering 2 MSB. Values of existing system are also compared with algorithm considering replacement of 4 LSBs. From Table, it is obvious that for all cover signals, PSNR is either close or more than values of existing algorithms.

Table 1.showing PSNR values of existing system and proposed system

	Input 1	Input 2	Input 3
Text 1	81.4624	82.4978	85.3069
	80.9272	81.7060	84.7412
	81.1533	81.6126	84.5151
Text 2	80.2578	80.9027	83.7654
	79.9960	80.6744	83.4835
	80.1249	81.1735	84.0387
Text 3	73.6278	74.4835	77.2747
	73.4498	74.1340	77.1923
	73.5696	74.4419	77.3406
Text 4	83.2412	83.9666	86.0462
	83.1879	83.8106	86.7757
	83.7527	84.1838	86.8830
Text 5	81.2201	81.8990	85.2693
	80.5941	81.6126	84.5151
	81.1533	81.7376	85.0860

Fig. 2 shows the plotting of the cover audio signal and Fig. 3 shows the plotting of the stego signal obtained after applying the proposed algorithm. From the figures, no difference is found in the stego signals obtained from proposed method as compared to the cover audio signal.

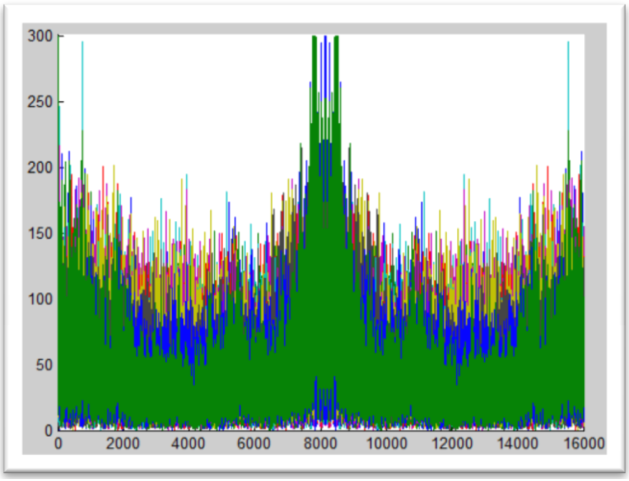

Fig 2: Plot of cover audio signal

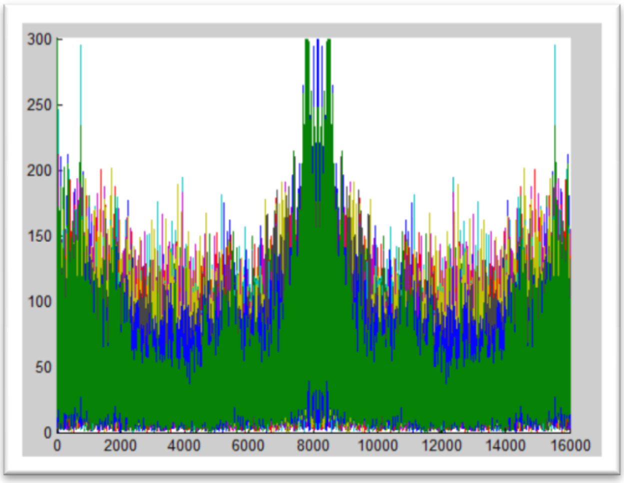

Fig 3: Plot of stego audio signal

6. CONCLUSION

The method proposed in this paper increases capacity as well as provides keyless randomization. The method first divide cover signal into 8x8 blocks with 16 bits per block and then check first two MSBs of each sub block’s 16 bits. This increases capacity with enhanced security factor due to randomization. From results, it is seen that there is a remarkable increase in capacity of cover audio for hiding additional data and without affecting the perceptual transparency of the host audio signal. Also counting out technique included in the method enhanced security without affecting perceptual transparency. The main advantages of the proposed algorithm are that it is logically simple, recovery of hidden data can be achieved without error and the foremost advantage is that it has enhanced security factor, so steganalysis is much more challenging. The algorithm fulfills basic requirements of data hiding techniques.

7. REFERENCES

[1] Fatiha Djebbar et al, ”A view on latest audio steganography techniques”, IEEE international conference on innovations in information and technology, 2011.

[2] Zamani M., Ahmad R.B., Manaf A.B.A., Zeki A.M., “An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography”, in Proc. IEEE International Conference on Computer Science and Information Technology, ICCSIT pp: 5-9, 2009

[3] “Audio steg: overview”, Internet publication on www.snotmonkey.com.

[4] http://www.snotmonkey.com/work/school/405/overview.html.

[5] 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”, IEEE World Congress on Information and Communication Technologies 2011.

[6] Martin Alvaro, Sapiro Guillenno and Seroussi Gadiel, "Is Image Steganography Natural?”, IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005.

[7] Cvejic N. and Seppanen T. "Increasing the capacity of LS B based audio steganography", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[8] Anupam Kumar Bairagi, Saikat Mondal, Amit Kumar Mondal, “A Dynamic Approach In Substitution Based Audio Steganography”, IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision, 2012.

[9] Dr. H. B. Kekre et al, “Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding”, IEEE Third International Conference on Emerging Trends in Engineering and Technology, 2010.

[10] N. Cvejic, T. Seppanen, "Increasing the capacity of LSB Audio Steganography using a novel embedding method", in Proc. IEEE Int. Conf Info. tech.: Coding and Computing, Vol. 2, pp.533-537, April 2004.

[11] Haider Ismael Shahadi and Razali Jidin, “High Capacity and Inaudibility Audio Steganography scheme”, 7th International Conference on Information Assurance and Security (IAS), 2011