ISSN 2277-3061

MESSAGE GUIDED RANDOM AUDIO STEGANOGRAPHY USING MODIFIED LSB TECHNIQUE

Taruna,Dr. Dinesh Singh
Mtech, DCRUST, Murthal
taruna0408@gmail.com
Assistant Professor, DCRUST, Murthal
dinesh.madhav@gmail.com

ABSTRACT

Steganography is the science of hiding secret data in such a way that its presence can't be noticed. Techniques which hide more secret data in cover files and which doesn't affect transparency of cover signal are better one for steganographic purpose. In the proposed technique which keyless randomization is provided to insert secret information in multiple and variable LSBs. Cover signal is converted into binary format and then with the proposed algorithm 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. PSNR values show that there is no noticeable difference between cover audio signal and stego audio signal. Security increases due to the use of variable number of LSBs for insertion and keyless randomization are provided by counting out technique.

Indexing terms/Keywords

Data hiding, Audio steganography, Least significant bit (LSB), Most significant bit (MSB), Human Auditory System (HAS), Capacity.

Academic Discipline And Sub-Disciplines

Academic Discipline is Computer science and sub-discipline is information security.

SUBJECT CLASSIFICATION

Association for Computing Machinery (ACM)

TYPE (METHOD/APPROACH)

My research work is experimental because various experiments have been done on different audio signals. Also it is empirical because it is based on available data.

ISSN 2277-3061

INTRODUCTION

Now-a-days there are so many software's available which are cheap and easy to use and using these software's creation and modification of digital information becomes very easy. But this easiness and speed of widespread use of digital information pose a threat for security of information. Techniques for securing information from eavesdroppers are known as either cryptographic or steganographic techniques. Cryptographic algorithms are designed to convert information in a format not understood by person other than sender and intended receiver. On the other hand steganographic techniques are actually information hiding technique. In these techniques, the main focus is on hiding message in cover (audio or video) file to obtain new file called stego file which is indistinguishable from cover file.

TYPE OF STEGANOGRAPHIC TECHNIQUES

Depending on the cover file used, steganography can be

- Text steganography
- Image steganography
- Audio steganography
- Video steganography

During comparison scientists found that there is natural limitation in the auditory and visual perceptions of human. This limitation give benefit by minimizing the difference between the original medium and the one obtained after embedding the hidden data. Although the 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. 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].

AUDIO STEGANOGRAPHY

Audio steganographic system is characterized by following three features viz. transparency, capacity and robustness. Transparency measure distortion caused due to modification in signals. Perceptual transparency is defined as inaudibility of distortion in cover audio file. The perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS and the host media [6].

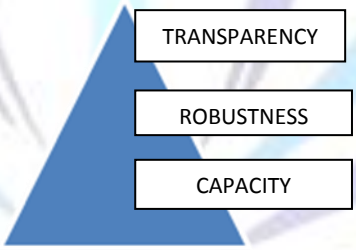

Fig 1: Three characteristics of steganographic system

Robustness is the ability of stego file to withstand attacks which 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 [5].

Capacity is a measure of quantity of data 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].

All the above discussed characteristics are dependent on one another. 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]. Changing one factor affects other two. 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 improvement in one of them affects the others. In this paper, two approaches are combined. Capacity and robustness of the steganographic system are improved 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.

COMPARISON AND EVALUATION OF EXISTING SYSTEMS

One of the simplest techniques of data hiding having high capacity is Least significant bit (LSB) technique [9]. Further improvement in capacity is made by increasing number of LSBs used for embedding secret data. But this introduces noise that becomes noticeable as the number of LSBs used for embedding of data increases [9]. Due to this, a limit is imposed 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.

H.B.Kekre et al in their paper, “Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding”, overcomes the limitation on maximum number of LSBs used for embedding without affecting perceptual transparency,, 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 characteristic i.e. capacity, keeping transparency constant. Robustness is not discussed.

PROPOSED METHOD

Existing system lacks robustness factor. This method completes this laciness. According to the algorithm firstly cover audio signal is converted into binary and then these binary bits are segmented into 8x8 blocks, with 16 bits/sub block. After segmentation apply next steps of proposed embedding algorithm on 16 bits of each sub block and the sub block used for embedding is evaluated by using counting out technique [3]. Position of next sub block is found by data to be embedded in the sub block. This ensures robustness because different data takes different embedding path, without affecting capacity and perceptual transparency. Table 1 shows the main steps for embedding data in cover audio signal of the proposed algorithm.

Table 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.

Table 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.

RESULTS AND DISCUSSIONS

Three audio sequences with different size and duration (3 to 4 minutes) are taken and proposed method was applied on them. Representation of audio sequences was by 16 bits per sample and analysis of proposed algorithm is in terms of PSNR (Peak Signal-to-Noise Ratio)..

Table 3. Steps for Data retrieval

	Input 1	**Input 2**	**Input 3**
Text 1	82.4978	85.3069	81.4624
	81.7060	84.7412	80.9272
Text 2	80.9027	83.7654	80.2578
	80.6744	83.4835	79.9960
Text 3	74.4835	77.2747	73.6278
	74.1340	77.1923	73.4498
Text 4	81.8990	85.2693	81.2201
	81.6126	84.5151	80.5941

Table 3 shows the results of the proposed method that increases randomization by using counting -out technique. Counting out technique is a repetitive process of picking an item from a set and omitting the picked item for the next iteration [3]. From Table III, 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.

Plotting of the cover audio signal is shown in figure 2 and plotting of the stego signal after applying the proposed algorithm is shown in figure 3. It is evident from the figures that cover audio signal and stego signals obtained after applying proposed algorithm have no noticeable difference.

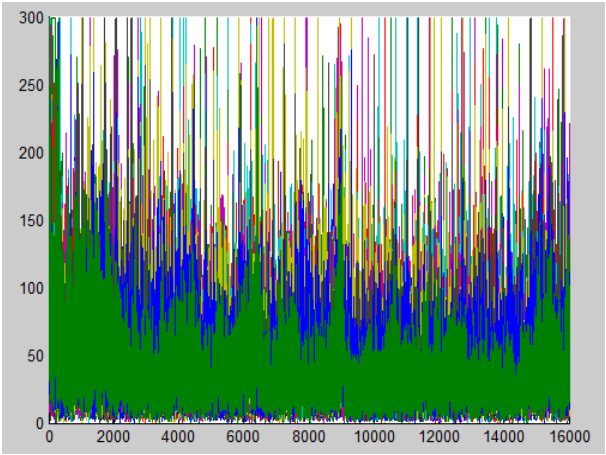

Fig 2: Plot of cover audio signal

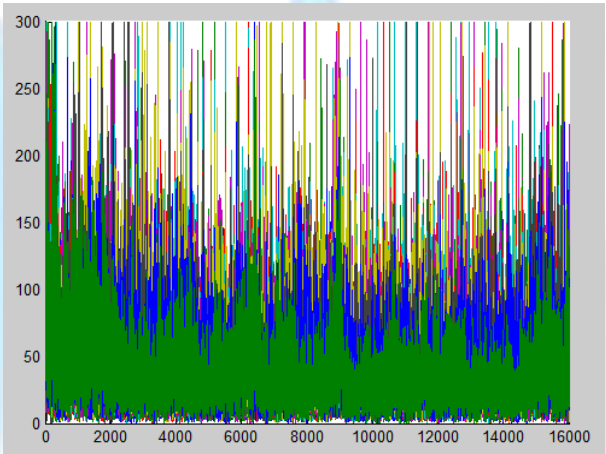

Fig 3: Plot of stego audio signal

CONCLUSION

The proposed algorithm provides keyless randomization in order to improve robustness. Cover signal is divided into 8x8 blocks with 16 bits in each block. First two MSBs of each sub block's 16 bits are checked for insertion purpose and data inserted is checked to find next sub block for insertion. This enhanced security by introducing randomization. Proposed algorithm uses counting out technique which increases security two folds without affecting perceptual transparency. Simplicity of the logic, recovery of hidden data without error and enhanced security factor, are the main advantages of the proposed algorithm. All these advantages makes steganalysis much more challenging.

ACKNOWLEDGMENTS

I would like to convey my heart felt gratitude to Dr. Dinesh Singh who has been a constant source of inspiration throughout this research work. I also owe my gratitude to Dr. Deepika Tiwari for guiding me at various stages. I am also thankful to all the people who have directly or indirectly participated in completion of my research work. No research work exist in vacuum. I, too, am thankful to all the researchers and scholars whose studies served as the foundation for my research.

REFERENCES

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

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

[3] "audio steg: overview", Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/overview.html.

[4] Sarosh K. Dastoor, IEEE World Congress on Information and Communication Technologies 2011. Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices.

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

[6] Martin Alvaro, Sapiro Guillenno and Seroussi Gadiel, IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005. Is Image Steganography Natural?.
[7] Anupam Kumar Bairagi, Saikat Mondal, Amit Kumar Mondal, IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision, 2012. A Dynamic Approach In Substitution Based Audio Steganography.
[8] Dr. H. B. Kekre et al, IEEE Third International Conference on Emerging Trends in Engineering and Technology, 2010. Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding.
[9] N. Cvejic, T. Seppanen, in Proc. IEEE Int. Conf Info. tech.: Coding and Computing, Vol. 2, pp.533-537, April 2004. Increasing the capacity of LSB Audio Steganography using a novel embedding method.
[10] Haider Ismael Shahadi and Razali Jidin, 7th International Conference on Information Assurance and Security (IAS), 2011. High Capacity and Inaudibility Audio Steganography scheme.

Author' biography with Photo

Mrs. Taruna has completed her B.tech in computer science from Vaish College of engg., MDU, Rohtak, Haryana. She has also completed her M.tech in computer science from DCRUST, Murthal, Sonepat. She is specializing in audio steganography. Her research interests include information security, operating system and networking. She has papers published in reputed international journals.

Dr. Dinesh Singh is working as assistant professor in department of computer science and engineering in DCRUST, Murthal, Sonepat. He has completed his doctoral work in networking. His research interest includes computer networking, digital security, and software project management. He has to his credit various papers published in reputed national and international journals. He has also attended and organized various workshops.