Combination of Steganography Using Parity Encoding and Spread Spectrum Technique

Manish Mahajan[1] and Sumeet Kour Bali[2]
[1]*Asst. Prof. Dept. of Information technology, Chandigarh Engineering College Landran, Mohali, Punjab, India*
[2]*Dept. of Information Technology, Chandigarh Engineering College, Landran, Mohali, Punjab, India*

Abstract: Steganography is a well-known method of hiding covert messages to obtain information security. In steganography the unused bits of data in sound, image etc. files are replaced with bits of secret information. In audio steganography an algorithm is used for hiding secret messages in audio files. Here in this paper information hiding is achieved using two different steganographic methods instead of a single steganographic method. This is called as Multi-level steganography. Multi-level steganography allows the hiding of two messages into a single cover object.

Keywords: *Cryptography, RSA, Multilevel steganography, Parity encoding method, spread spectrum technique, Decoy object.*

I. INTRODUCTION

Steganography is the art of hiding secret messages which is digital data such as text documents, audio, video and images. The secret message is called as message object [1]. The message object can be hidden inside different type of objects like text, audio, video called as cover object. Someone who is tapping the communication wire would not notice anything without the normal carrier. The output file produced by the application of steganography is called as stego object. One of the properties of steganography is the imperceptibility in which no one other than the original sender and the receiver can suspect the presence of the hidden file inside the carrier object [2]. In this paper we use Multilevel Audio Steganography in which an intermediate object is used called as decoy object .The decoy object is the result of the steganography applied at the first level and act as the cover object for the second level of the steganography [3]. Steganography is applied at two different levels instead of the single level. Here two steganography techniques used at two levels are Parity Encoding and Spread Spectrum Techniques. Here in this paper we use cryptography along with the steganography [4].

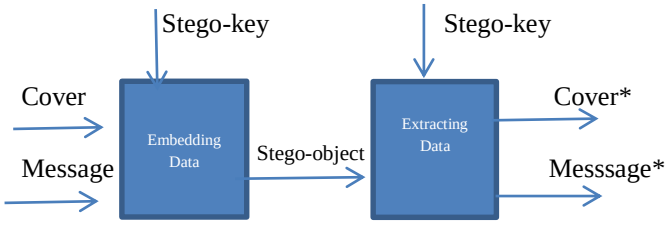


Fig.1: Structure of Steganography System

II. LITERATURE SURVEY

A. *Parity Encoding Technique*

One of the prior techniques in audio data hiding is the parity coding method. Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion [5].The advantage of using the parity encoding method is that the sender has a choice in encoding the secret bit. There are two main disadvantages of the parity encoding method. The method introduces the slightest bit of noise in the signal and the other disadvantage is that the parity coding method is less robust.

B. *Spread Spectrum Technique*

In relation to the audio steganography, the basic spread spectrum method is to spread the secret information across the audio signal's frequency spectrum as much as possible. Unlike any other steganographic method, the spread spectrum method spreads the secret data over the audio file's frequency spectrum using a code that is independent of the actual signal. The final signal after the application of the steganography occupies a bandwidth in excess of what is actually required for transmission. Two schemes of spread spectrum can be used for the audio steganography: the direct

sequence (DSSS) and frequency hopping (FHSS) schemes. In direct sequence method, the secret data 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 method the audio file's frequency spectrum is altered so that it hops rapidly between frequencies [6]. The spread spectrum method has an advantage that it maintains a high level of robustness. Spread spectrum method shares a disadvantage with the parity coding method in that it can also introduce the noise in the audio file. In [7] spread spectrum can be combined to the phase shifting to increase the robustness of the transmitted data against additive noise. In this method a reliable hiding capacity of 3 bps was attained. To obtain a higher hiding capacity of 20 bps, the [8] uses spread spectrum technique in sub-band domain.

III. PROPOSED METHOD

A. *Multilevel Steganography*

In this paper a layered approach is used in which two secret messages are transmitted inside a single cover object. We use the combination of steganography and the cryptography. For encryption and decryption public key cryptographic algorithm RSA is used. In the sender side, the secret message S1 which is to be embedded in the audio file is encrypted using public key cryptography algorithm RSA. The cipher text obtained is then embedded into the cover file(C) using parity encoding method. This is the first level of the multilevel steganography resulting into the stego object (C1) which acts as the cover object for the next level, called as decoy object. At the second level the secret message denoted as S2 is encrypted using RSA algorithm. The cipher text obtained is embedded into the decoy object C1 using spread spectrum technique. The result of the second level of the multilevel steganography is stego object (C12). C12 hides both the messages S1 and S2.

B. *Parity Encoding*

The parity encoding method is implemented by breaking the data part of wav file into number of regions. Each region includes the same number of elements of secret message text. Then the parity flag of each region is calculated. If it does not match with the message bit then we change the last bit of that region with the message bit. It is observed that stego object has not been audibly modified. There is reasonable no change between the input carrier file and the output stego object.

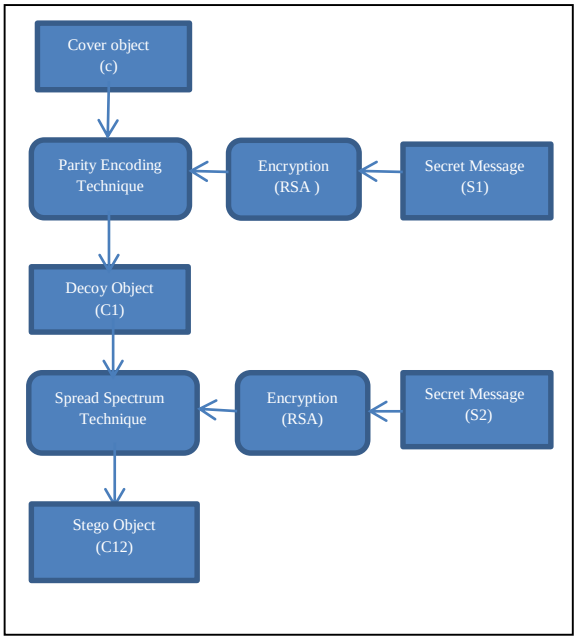


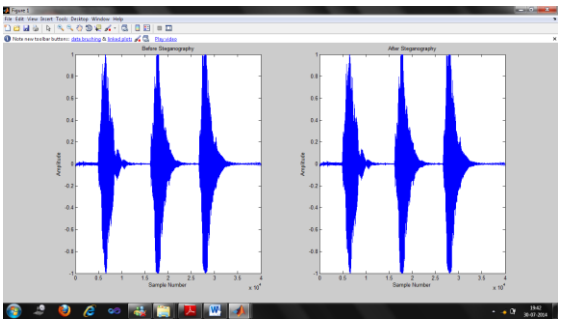
Fig.4: Flow-chart for proposed method

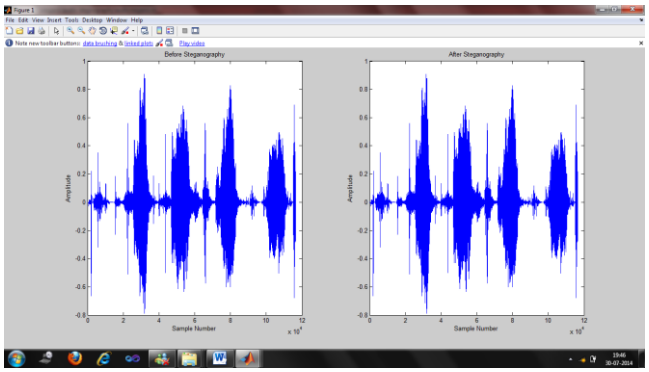
C. *Spread Spectrum*

In the direct sequence method the input Carrier audio file of particular bandwidth is spread deliberately in a frequency domain. The secret message is spread over audio file's frequency spectrum. As a result the final signal occupies a bandwidth in excess of what is required. If the distortion is introduced in the signal it damages only certain frequency bands, the message is still in a recoverable state. The distortion is too undersized to introduce a visible artefact and the secret message is scattered over wide range of frequencies, that it became robust against many signal distortions.

D. *Blend of Parity Encoding and Spread Spectrum in Multilevel Steganography*

At the level 1 the first message is hided under cover object using parity encoding. The output of this level is an intermediary object called decoy object. Decoy object is the input for second level. At the level 2 the second secret message is hided under the decoy object using spread spectrum technique.





E. Decoding Result

When the stego object passes over the decoding algorithm of the spread spectrum method the secret message of second level is retrieved. When the decoy object passes through the decoding algorithm of parity encoding method the secret message of first level is retrieved.

IV. CONCLUSION

In this paper a new method of audio steganography is introduced. Two traditional methods of steganography are combined in a multilevel approach to hide the secret message properly. The output stego object is difficult to decode and carrier audio file after embedding is same as before embedding, which makes it a successful method in the world of audio steganography.

V. REFERENCES

[1] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik, "Multilevel audio Steganography for hiding messages: using LSB and Parity Encoding" international journal of emerging trends & technology in computer science, vol. 1, issue 2, july – august 2012.

[2] K.P.Adhiya Swati A. Patil, "Hiding Text in Audio Using LSB Based Steganography" information and knowledge management, vol 2, no.3, 2012.

[3] Dr. Atef Jawad Al-Najjar1, Computer Engineering Department, King Fahd University of Petroleum & Minerals, Saudi Arabia, "The Decoy: Multi-Level Digital Multimedia Steganography Model" 12th WSEAS International Conference on Communications, Heraklion, Greece, July 23-25, 2008.

[4] Shailenra Gupta, Ankur Goel, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" International journal of Modern Education and Computer Science, 2012, 6, 27-34.

[5] Poulami Dutta, Debnath Bhattacharyya, and Tai-hoon Kim, "Data Hiding in Audio Signal: A Review" international journal of database theory and application, vol. 2, no. 2, june 2009.

[6] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum" international journal of modern engineering research (ijmer), vol.1, issue1, pp-157-161.

[7] Swati Malviya, Manish Saxena, Dr. Anubhuti Khare, "Audio Steganography by Different Methods" international journal of emerging technology and advanced engineering, vol. 2, issue 7, July 2012.

[8] K. Gopalan, et al, "Covert Speech Communication Via Cover Speech By Tone Insertion", Proceeding of IEEE Aerospace Conference, Big Sky, MT, March 2003.