International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

Encrypting and Disentangling Secret Data in .wav

N. Rajeev Reddy[1], Sk. Ch. Nagur Shareef[2], A. Raveendra Babu[3], Ch. Suresh Babu[4], P. Shajahan[5]
[1,2,3,4,5]*Assistant Professor, Department of Electronics and Communication Engineering, Narasaraopeta Engineering College, Narasaraopet, India*

***Abstract*: A method used to hide the textual information in an audio file is called audio steganography. In audio steganography, encoding process is carried out through inactive frames of low bit rate audio streams by performing iLBC (internet Low Bit rate Codec). This paper describes the methodology that be used in applications such as VoIP (Voice Over Internet Protocol), streaming audio, archival and messaging. Traditionally, data encoding is carried out in the inactive frames rather than the active frame of streams; that is inactive frame has large embedding capacity. In addition VAD (Voice Activity Detection) algorithm is used for detecting inactive frames. In this technique the audio file is first sampled and then the appropriate bit of each alternate sample is altered by embedding the textual information. Lastly to enhance security in steganography PCC (Parabolic Curve Cryptography) algorithm is introduced.**

***Keywords*: Terms-Audio streams, inactive frames, steganography, Voice over Internet Protocol (VoIP).**

1. Introduction

Steganography, coming from the Greek words stegos, meaning roof or covered and graphia which means writing. It is the art and science of hiding the fact that communication is taking place. Using the steganography, we can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. Varieties of techniques for embedding information in digital audio have been established. Least Significant Bit (LSB) technique is one of the simplest approach for secure data transfer. To hide text information within the audio file, we propose an approach that uses two LSB layers of the host file. The data hiding is done by minimum modification to the host file, which implies that changes of host audio file do not impact the Human Auditory System (HAS). The proposed approach is also robust with respect to the errors, occurred during embedding of text in the audio files, as minimum modifications are performed on the original host audio. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. Cryptography (hidden, secret"; and "writing", or "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties. The rest of this paper is organized as follows. Section II summarizes some related work, discussing the possibility of data hiding and transmission using Voice over Internet Protocol (VoIP). In Section III, the principal of the steganography algorithm for embedding data in the inactive audio frames is analyzed. Our proposed steganography algorithm is presented in Section IV. Section V details the scope. Implementation predicting performance evaluation results are shown in Section VI. Finally, the paper ends with performance analysis in Section VII and conclusion under Section VIII.

2. Related work

A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload. Steganography process does not modify the content of data rather it hides only the data. The aim of steganography is to hide the information in an undetectable manner such that information hidden cannot be predicated other than the receiver [1]. Audio steganography is the practice of hiding the message into another medium such as hiding the information into the audio file. The confidential information is hidden in an audio. Though information is hidden, the perception of an audio does not change; hence the intruders can never find that data is hidden. The basic model of audio steganography consists of cover file, data which we need to hide, stego key. Parameter, of the basic model is shown in the Fig.1. The term cover file refers to the medium that require hiding the data into audio. Message that has to be hidden are in various forms like video, audio, images. Secret information is embedded into the cover message by the secret key called stego key. Stego file is a collective term for cover file with secret information [2].Communication protocol like VoIP streams are used for broadcasting voice communication over the internet. This process involves the conversation of voice signal into appropriate digital signal [3]. VoIP is a protocol in which Internet is used as the transmission medium for telephone calls by sending voice data in the form of packets. The main challenge faced in such technology is security, as VoIP stream acts as the most essential cover object for steganography. Another challenge regarding the field of

data hiding is the digital steganography in low bit rate audio codec [4].

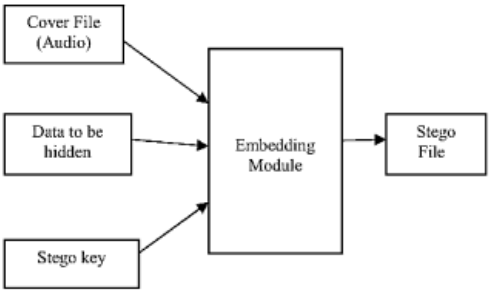

Fig. 1. Audio Steganography Basic Model

3. Principal of steganography in inactive frames

A. *Introducing voice activity detection (VAD)*

The voice activity detection (VAD) algorithm is used to find, whether the current audio frame is an active frame by comparing the energy (Enr) and threshold (Thr) using the equation (1). If VAD=0 means the frame is an inactive voice; else, the frame is an active voice is illustrated in the Fig.2. The VAD algorithm is trained for a small period by a prerecorded sample that contains only background noise.

$$VAD = \begin{cases} 1, Enr \geq Thr \\ 0, Enr \leq Thr \end{cases} \quad (1)$$

B. *VAD algorithm*

In general, network bandwidth in some source codecs introduces silence compression during the inactive period of audio streams. When the silence is enabled, RTP data is not sent, which conserves bandwidth. When the silence is disabled, RTP send data stream to the port, even if there is no actual digitized speech. VAD algorithm is used in real-time systems because of low complexity [5]. The characteristics are simplicity and robustness. Low SNR (Signal to Noise Ratio) environments are obtained. Detecting speech is a critical problem in many audio applications including speech coding, speech recognition, speech enhancement, and audio indexing. VAD is also useful in VoIP, where the required accuracy of detection needed is less stringent. [6].

C. *iLBC algorithm*

Internet Low Bit Rate Codec (iLBC) referred to a royalty free speech codec. ILBC is designed mainly for encoding and decoding speech for transmission via VoIP (Voice over Internet Protocol). Controlled response is necessary for packet loss, delay and jitter. Generally, iLBC can be easily implemented in Packet Loss Correction (PLC) system [7]. Compression usually reduces the bandwidth requirements for these applications. VoIP' is implemented in the User Datagram Protocol (UDP) for better efficiency, thus exposing any unreliability of underlying network protocol to the user's program. Packet loss correction is needed to be maintained for voice quality over lossy networks, iLBC is mainly designed for compression of speech that is transmitted over the Internet [8].

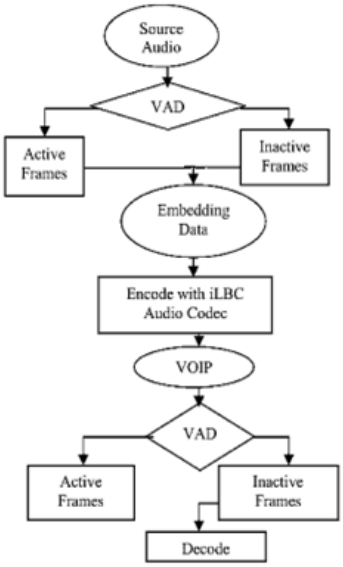

Fig. 2. Flow chart of steganography in inactive and active frames

4. Comparison of existing methods

A. *Least significant bit (LSB) coding*

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

B. *Parity coding*

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. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner. Disadvantage: This method like LSB coding is not robust in nature.

C. *Phase coding*

Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It “works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments”. Disadvantage: It is a complex method and has low data transmission rate.

D. *Spread spectrum (SS)*

It attempts to spread out the encoded data across the available

frequencies as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Advantage: It offers moderate data transmission rate while maintaining a high level of robustness. Disadvantage: It can introduce noise into a sound file.

E. Echo data hiding

Text can be embedded in audio data by introducing an echo to the original signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded.

5. Experimental methods

A. Existing method

In [9] the secret message and carrier files are taken as audio files. Before performing the embedding process the secret message is encrypted using a private key cryptography. Then the stego object is created. Thus using the key the secret information is retrieved at the receiver side. In [10] audio files AES of 256 bits key length is used for the encryption of secret audio file to ensure the security.

B. Proposed method

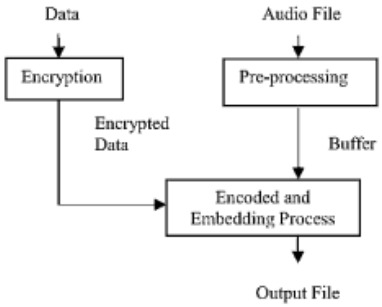

Fig. 3. Proposed method block diagram representation

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Here a key is taken at the transmitter with that a pseudo sequence is generated and this sequence is performed a logical operation with the secret message. Then the embedding process is carried out with the carrier audio file and is transmitted at the transmitter side. In the receiver side with the audio stego file the LSB are recovered first and with the known key generated at the transmitter the decryption process is carried out and the secret message is recovered from the stego file. The entire proposed de-steganography process. Data to be hidden is first encrypted by the PCC algorithm and then the encrypted data is suspended. An audio file is taken for the pre-processing where the inactive frames are detected. After which the inactive frames are stored in the temporary buffer. Now the encrypted data is encoded with low bit rate source codec by using iLBC algorithm and embedded to the inactive frames. The output file is sent to the receiver, which decrypts the code by means of a secret key. So that the original data can be obtained is illustrated in the Fig. 3.

6. System architecture

A. Parabolic curve cryptography

Parabolic Curve Cryptography (PCC) is a public key cryptography. In public key cryptography, each user have a pair of keys to communicate, which are the public key and the private key, and a set of operations associated with the keys to do the cryptographic operations. Generally, particular user only knows the private key, whereas the public key is distributed to all users taking part in the communication. Public key cryptography, unlike private key cryptography does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

B. Algorithm

The data to be encrypted and then hidden using Parabolic Curve Cryptography involves the following steps.

Step 1) Consider a parabolic curve n, nP= 1P+2P+3P.... P times value of curve

Step 2) The X sends message m to Y. G is called generator point and where n is the order of G

Step 3) Let us consider sender X generates random number, private key is $n_x < n$, where public key is $P_x = lG+2G+.... n_xG$ times

Step 4) Then receiver Y generates random number, private key is $n_Y < n$ where public key is $P_Y=G+G+.... n_Y$ times

Step 5) Consider key generation $k=P_x+ P_x+ n_Y$ times and another key generation $k= P_Y+ P_Y+ n_x$ times, both keys has the same value.

Step 6) Let P_{ml} = a P_m, a is ASCII value of text, P_m is random number on parabolic curve.

Step 7) The encryption() using $C_m=2$ cipher text value contains $\{KG, P_m+k P_Y\}$

Step 8) If $(P_{ml}+k P_Y- n_Y KG) = P_{ml}$

Step 9) Decryption(), where $p_Y= n_YG$

Step 10) Else, key value not matched. End if.

C. Example

Let the equation of the parabolic curve be y mod p =x2 +ax +b; Inputs: a, b, p where p is key of the PCC algorithm and parameters a, b are the two non-negative integers on the curve. The P, Q lie on the curve and P+Q gives another point that lie on the line that connects P and Q as described in the Fig.4 below.

Fig. 4. All points (x, y) which satisfies the above equation plus a point at infinity lies on the parabolic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private

key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants, the domain parameter of PCC is obtained. During the implementation of PCC, the plaintext encoding should be performed before encryption and the decoding process should be held after decryption. PCC Encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages.

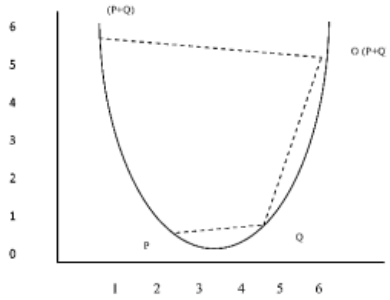

Fig. 4. Parabolic Curve Example $y=x^2+x+1$

7. Implementation

A. *Frame implementation*

The process of hiding a data through steganography and the audio file is sent via VoIP has been implemented. In the audio file the active frames and inactive frames are differentiated and spectrogram is viewed, the amount of data hidden can be analyzed shown in the Fig. 5. Energy of a frame indicates possible presence of voice data. Energy will be greater in active frames and lesser in inactive frames.

B. *VoIP implementation*

The basic operation is to load a speech signal and then pass it to the iLBC Encoder block as shown in the Fig.8, which convert it to iLBC packets. Next, the packets are sent through a simulated lossy channel, which causes all random packets to be zeros. After encoding, the packets are sent to the iLBC Decoder block as shown in the Fig. 9 to be converted back into a speech signal. After decoding the audio is played. User Datagram Protocol (UDP) is part of the Internet Protocol (IP) suite. UDP provides efficient transmission of data, but does not guarantee reliability, data order, or data integrity. These characteristics make UDP suitable for streaming audio and video data, but not for binary files and similar situations where data loss is unacceptable. The decoder's transmission rate must be set to same as the encoder, or else an error will occur.

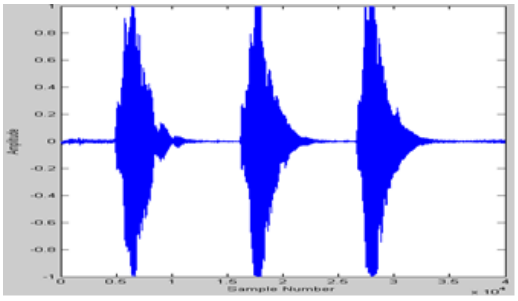

Fig. 5. Audio wave before embedding the confidential info

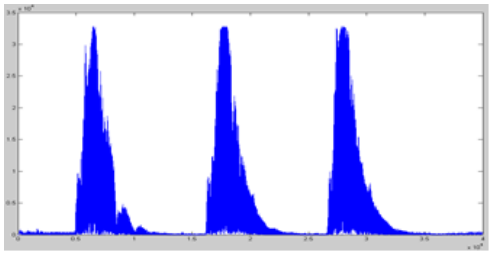

Fig. 6. Audio wave inactive frames for confidential info

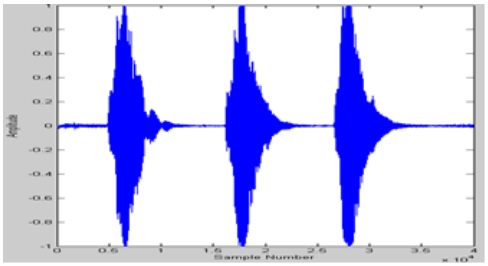

Fig. 7. Audio wave after embedding the confidential info

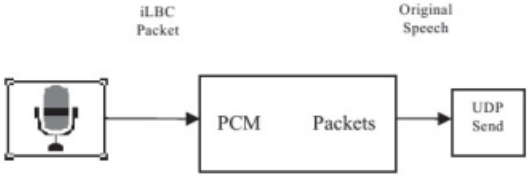

Fig. 8. iLBC Encoder

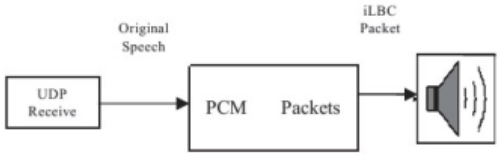

Fig. 9. iLBC Decoder

8. Performance analysis

Based on the energy and spectrogram the active and inactive frames are calculated. An inactive frame is clipped where the spectrogram viewed in the Fig. 6, after data embedding, the audio spectrogram of inactive spectrogram is obtained as illustrated in the Fig. 7. The comparison of the inactive frames before data embedding and after data embedding shows the variation in the wave (spectrogram).

9. Conclusion and future work

This paper, suggests a high-capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded by iLBC source codec's. The experimental results have shown that our steganography algorithm can achieve a larger data embedding capacity when compared to other algorithm. The VAD algorithm, which is suitable for embedding data in inactive audio frames, is used rather than active audio frames. Thus data is transmitted and received using the VoIP protocol. A text file of size 1KB data is hidden in an audio file of size 78.1KB .From the above audio file frames of size 70KB are active frames and 6KB is found to

be inactive frames, where LSB algorithm is used for hiding a data in the inactive frames, Therefore the number of inactive frame used is 1KB for hiding a text, storage limit is based on the threshold value. The security implemented using Parabolic Curve Cryptography that provides the data to be encrypted and then hidden. Thus PCC allows for high security solutions that do not impact performance even on constrained devices. The encryption process in cryptography is under progress. Future work is to assure the integrity of hidden messages in the case of packet loss.

Acknowledgement

I wish to express my heartfelt thanks to Dr. V. Venkata Rao, B.E., M.E., Ph.D., Professor & Head, Mr. J. Narasimha Rao, B.Tech., M.Tech., (Ph.D)., Coordinator and Mrs. B. Rajyalakshmi, M.Tech., Guide of our Department for their support for my project; without them this would not have happened successfully. I wish to express my thanks to Mr. B. Koteswara Rao, Lab Technician, for helping me to learn more about the project. I would like to express my gratitude towards the professors of our college for their able guidance while making this paper. I also thankful to all those who directly or indirectly helped me in making this paper a reality.

References

[1] R. Sridevi, A. Darnodaram, and S. V. L. Narasimham, " Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enchanced security", in JATIT, Joumal of Theoretical and Applied Information Technology, 2005-2009.

[2] P. Jayaram, H. R. Ranganatha, H. S. Anupama "' Information hiding using audio steganography-a survey", 3rd ed., vol. 3. UMA (International Journal of Multimedia & its Applications), August 2011.

[3] Mathew Desantis, "Understanding VoIP (Voice over Internet Protocol)", Produced 2006; updated 2008, by US-CERT, a government organization.

[4] Yong Feng Huang, shanyu tang, "Steganography in Inactive frames of VOIP streams encoded by source codec", IEEE transactions on information forensics and security, vol. 6, no. 2, 2011.

[5] M. H. Moattar and M. M. Homayounpour, "A Simple But Efficient Real-Time Voice Activity Detection Algorithm", 17th EUSIPCO (European Signal Processing Conference), 2009.

[6] V. Ramesh Knaana, J. SelvaKumar. Advanced integrated steganographic approach with VOIP communication ", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 2, February 2012.

[7] Huang Sai, "Implementation of iLBC Codec Algorithm on DSP", 1983.

[8] http.//www.mathworks.in/help/dsp/exampIes/internet-low-bitrate - codecilbc-for-voip.html.

[9] Gopalan, "Audio steganography using bit modification", 2003 IEEE International conference on Acoustic, Speech and Signal Processing page(s): II – 421-4 vol. 2.

[10] Muhammad Asad, Junaid Gilani, Adnan Khalid "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 2011 international conference on Computer Networks and Information Technology (ICCNIT), pages 143-147.

[11] N. Sudha Lakshmi, "Audio Steganography Using Least Significant Bit," in Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14), International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, Special Issue-1, pp. 1-5, March 2014.

[12] A. R. Dengre, A. D. Gawande, and A. B. Deshmukh, "Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video," in International Journal of Application or Innovation in Engineering & Management, vol. 2, no. 6, pp. 363-370, June 2013.