An Approach of Robust High Capacity Audio Steganography and Cryptography Using LSB Algorithms

T. Ravi Kumar Naidu[#1] T.V.S. Gowtham Prasad[^2] P.G.Mamatha[*3]

[#]*Assistant professor, Dept. of ECE, SVEC, Tirupati, Andhra Pradesh.*
[^]*Assistant professor (SL), Dept. of ECE, SVEC, Tirupati. Andhra Pradesh.*
[*]*PG student, Dept. of ECE, SVEC, Tirupati, Andhra Pradesh.*

***Abstract*— Increased use of electronic communication has given birth to new ways of transmitting information securely. "Security has its importance and application in wide area. It is a measure of human negligence, in desire to seize the latest technological inventions". This measure may have adverse effect on human perception to the deployment of application, which needs serious concern in terms of security. Audio steganography is the science of hiding some secret text or audio information in a host message. The main challenge in audio steganography is to obtain high payload and robustness. A wide variety of techniques are existing such as LSB, Parity coding, phase coding for audio steganography. Here, a new approach with two level encryption of user data by combining cryptography and steganography is proposing to achieve high payload capacity and robust technique for Embedding information in Digital Audio data.**

***Keywords*— Audio Steganography, Cryptography, LSB, HAS, Security.**

I. INTRODUCTION

Steganography become more important as more people join the cyberspace revolution. Steganography is an art of hiding secret message in another host message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called cover message or host message. Once the contents of the host message or cover message are modified, the resultant message called as stego-message. In other words, stego-message is the combination of host message and secret message.

Steganography is often mixed up with cryptography. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message. The primary message is referred to as the carrier signal or carrier message and the secondary message is referred to as the payload signal or payload message.

The general steganography system is shown in Fig.1

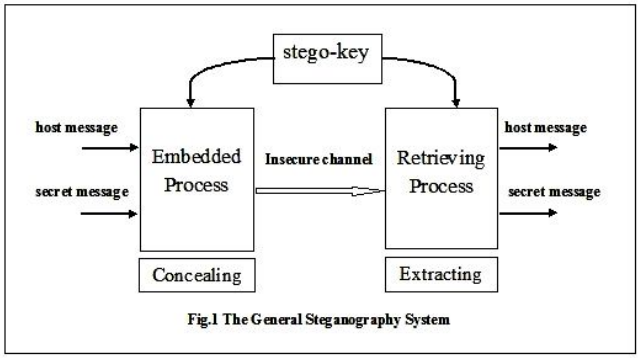


Fig.1 The General Steganography System

II. LITERATURE SURVEY

Steganography: The word steganography is derived from Greek words Steganos and graphia. Steganos means covered and graphia means writing. Thus steganography means covered writing which is an art of covert communication. Steganography can be applied to different types of media including text, image, audio and video. Audio and video files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy [1].

Audio steganography requires a secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and stego message after steganography remains same. However, audio steganography is considered more difficult than video steganography because the Human Auditory System (HAS) is more sensitive than Human Visual System (HVS).

In Audio steganography, secret message is embedded into digitized audio signal which results into altering the binary sequence of corresponding audio file [3]. There are several methods are available for audio steganography.

LSB Coding: Least significant bit (LSB) insertion is a common, simple approach to embedding information in a audio signal [2]. In this process embed the bits of the message directly into least significant bit of the cover audio in a specific way. There are several methods of data embedding in LSB technique which are Lowest Bit Coding, Sample selection, Bit selection, XORing of LSB's, Variable Low Bit Coding, Average Amplitude Method, Parity Coding etc.,

Cryptography: In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

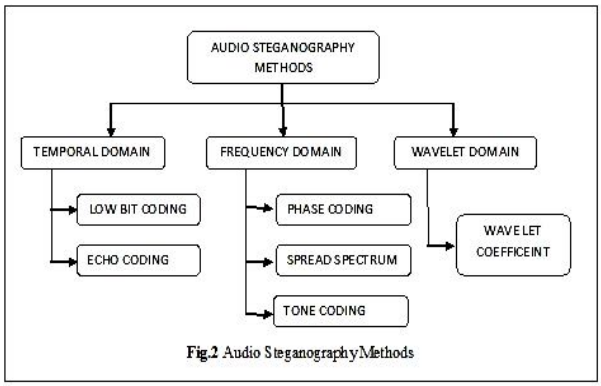


Fig.2 Audio Steganography Methods

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography as shown in Fig.2.

III. PROPOSED METHOD

The proposed scheme uses some encrypted algorithms to encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form and then apply embedding process [4].

The Major operations performed are :

- Read a secret message and apply changes by using Cryptography techniques and make it as payload message.
- Write a non-secret cover message or host message.
- Produce a stego-message by concealing a pay load message embedded on the cover message by using a stego-key.
- Send the stego-message over the insecure channel to the receiver.
- At the receiver end, on receiving the stego-message, the intended receiver extracts the secret embedded payload message from the stego-message by using a pre agreed stego-key.

Finally it converted to original secret message by using inverse cryptography techniques

Cryptography process:

Read a secret text message and convert that text message into binary form and apply changes by using binary to gray conversion technique and make it as payload message.

Steganography process:

Bit selection:- For the purpose of hiding the secret data, in every sample the selectable bits can be varied or distinct. Only first 2 MSB's will decide in which bit the secret message would be encrypted but only 1st two LSB's are used for embedding. Thus intruder can gets confuse by developing randomness.

If the first 2 MSB's of a sample are equal to either 00 or 11 then the 1st LSB will be replaced with secret message bit. Likewise if the first 2 MSB's are either equal to 01 or 10 then the second LSB is replaced with secret message bit.

TABLE I

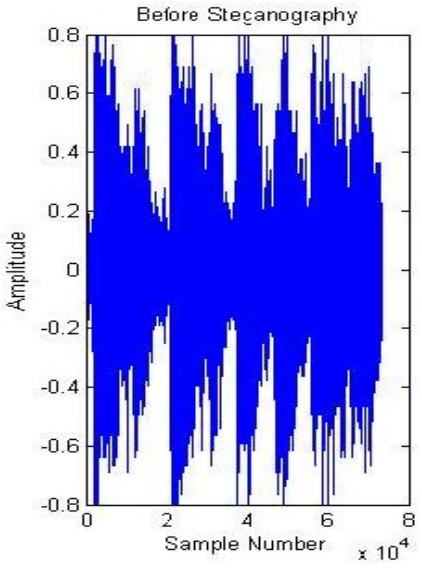
1st MSB	2nd MSB	Secret message bit
0	0	1st LSB
0	1	2nd LSB
1	0	2nd LSB
1	1	1st LSB

Sample selection:

In this method instead of using all the samples only few are selected and used for data hiding. The randomness created for selecting samples provide higher security.

IV. EXPERIMENTAL RESULTS

First we embedded our secret message in least significant bits by using approaches and compared the sound and graph with original one. We observed that no change in sound and graph and results are plotted in fig.3.



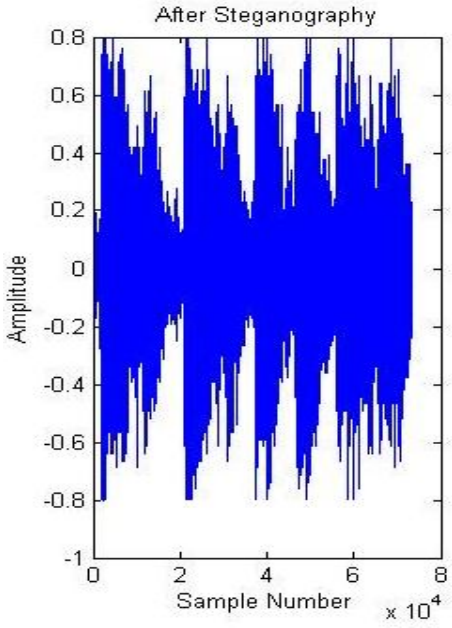


Fig.3 Resultant Graph before and after Steganography

V. CONCLUTION

In this paper, a novel approach that combines steganography and cryptography have been proposed to embed the data into an audio file. When compared to standard LSB coding method, these methods embed data in multiple and variable LSBs depending on the MSBs of the cover audio samples. By combining cryptography and steganography in data hiding payload capacity and robustness will be improved.

REFERENCES

[1]. Masoud Nosrati, Ronak Karimi, Mehdi Hariri "Audio Steganography: A Survey on Recent Approaches"World Applied Programming, Vol (2), No (3), March 2012. 202-205.ISSN: 2222-2510 ©2011 WAP journal. www.waprogramming.com

[2]. K.P.Adhiya , Swati A. Patil, " Hiding Text in Audio Using LSB Based Steganography" International Institute for Science,Technology and Education (IISTE), Information and Knowledge Management ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.3, 2012.

[3]. Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik . "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012

[4]. Padmashree G, Venugopala P S "Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers". International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012, ISSN: 2277-3754 ISO 9001:2008 Certified

AUTHOR BIOGRAPHY

Mr. T .Ravi Kumar Naidu Assistant Professor, Dept of ECE, Sree Vidyanikethan Engineering College, A. Rang ampet, Tirupati received B.Tech in Electronics and Communication Engineering from SVPCET, Puttur and M.Tech received from HIET affiliated to JNTUH, Hyderabad. Interesting Areas Digital Signal Processing, Array Signal Processing, Image Processing, Video Surveillance, Embedded Systems, Digital Communications.

Mr. T V S Gowtham Prasad Assistant Professor, Dept of ECE, Sree Vidyanikethan Engineering College, A. Rangampet, Tirupati received B.Tech in Electronics and Communication Engineering from SVEC, A .Rangampet, Tirupati and M.Tech received from S V University college of Engineering, Tirupati. Pursuing Ph.D from JNTU, Anantapur in the field of Image Processing as ECE faculty. Interesting Areas are Digital Signal Processing, Array Signal Processing, Image Processing, Video Surveillance, Embedded Systems, Digital Communications.

Ms. P.G .Mamatha, P.G Student, Dept of ECE, Sree Vidyanikethan Engineering College, A. Rangampet, Tirupati received B.Tech in Electronics and Communication Engineering from SRET, Tirupati Interesting Areas Digital Signal Processing, Image Processing, Embedded Systems,Digital Communications