ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

A Multi-Level Approach of Audio-Steganography and Cryptography

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

[1]P.G student, Dept. of ECE, SVEC, Tirupati, Andhra Pradesh, India

[2]Assistant professor, Dept. of ECE, SVEC, Tirupati, Andhra Pradesh, India.

[3]Assistant professor (SL), Dept. of ECE, SVEC, Tirupati. Andhra Pradesh, India.

ABSTRACT: After a rapid growth of cyber revolution, developing a secret communication is a major task of security that has gained increasing importance. Cryptography and steganography are the best methods for introducing hidden communication. Current technology allows steganography applications to hide any digital file inside of any other digital file. Due to the existence of their redundancies, audio and video files are much suitable for the purpose of hiding. Audio steganography is a challenging subject because human auditory system (HAS) is more sensitive than human visual system (HVS). It requires a text or audio secret message to embed within a carrier audio file. Several basic audio Steganographic methods like LSB method, parity coding etc., are in existence, but the proposed LSB with XORing method gives high security which undergoes cryptographic randomized algorithm too. By performing two level encryption, capacity and robustness will be increased.

KEYWORDS: Audio steganography, cryptography, LSB, HAS

I. INTRODUCTION

Steganography is a process of hiding a secret message within a host message and extracting as its destination. Anyone else apart from the sender and intended recipient observing the message will fail to know it contains hidden data. The term hiding refers to the process of making the information secret. With the introduction of digital audio files, this has taken on a whole new meaning to create new methods for performing reversible data hiding as it is often dubbed. This has many possible applications including the copyright watermarking of audio, video and still image data.

In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another. In this process, first the secret data is encrypted and then hide it in an original data. The stego medium is obtained by the addition of cover medium, secret data and approached algorithm which is nothing but a stego key. The cover medium is the file in which the secret data is hidden. Here, the cover medium is typically an audio file. The stego medium is also the same type of file in the cover medium. In a computer based audio Steganographic system, secret messages are embed in digital signals. In audio Steganography the perception of the Human auditory system (HAS) is used to hide information in the audio because it perceives over a wider power range. Embedding secret messages in digital sound is usually a difficult process than embedding data in other media due to its perception. Here, Steganography is often mixed with cryptography. Unlike steganography, Cryptography changes the representation of the secret message. The main goal of approached method is to combine steganography and cryptography in such a way to make it harder for an intruder to retrieve the plain text of a secret message from a stego object. The general steganography system is shown in Fig.1.

II. LITERATURE SURVEY

Steganography:

The word steganography is a combination of two words which are taken from Greek language: steganos which means covered and graphie which means writing and literally called as covered writing. Thus steganography is said to be a covert communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a presence of second message [1]. Both steganography and cryptography are meant for secret communication but the approach is different. Hiding of secret message using steganography can be done in different forms like text steganography, image steganography, audio steganography and video steganography. Encoding secret messages in audio is the most challenging task while using steganography because human auditory system (HAS) is more perceptive than human visual system (HVS) [5]. Thus audio file is used as a cover file to hide secret data and it is called audio steganography. In Audio steganography, secret message is embedded into digitized audio signal which results into altering the binary sequence of corresponding audio file. There are several methods are available for audio steganography.

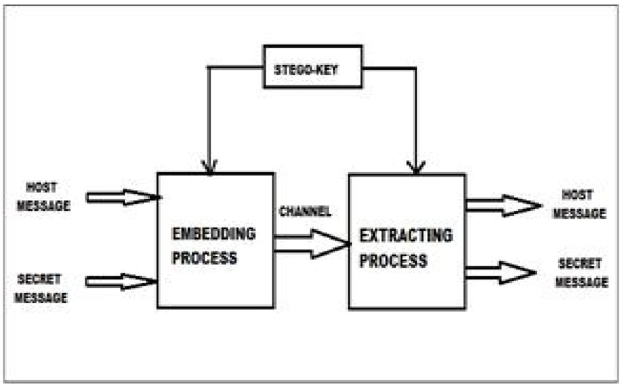

Fig1: The general Steganographic system

LSB coding:

The LSB modification is one of the simplest audio steganography techniques which is simple to implement and easy to detect but it provides high capacity. In this technique, data is being hidden directly in least significant bits of audio samples in a particular way [6]. 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.,

Parity coding:

Instead of dividing a signal down into individual samples, the parity coding method breaks a signal into isolated regions of samples and encodes each bit from the secret message in a sample region 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.

Spread spectrum:

It spread out the encoded data across the available frequencies as much as possible. This method spreads the secret message over the audio file’s frequency spectrum, using a code that is not dependable on actual signal. Thus, final signal occupies a band width which is in excess than requirement.

Cryptography:

Cryptography is also meant for secret communication but unlike steganography it doesn’t conceal the secret data but it scrambles the data. So, cryptography makes the secret data meaningless which is difficult to detect by the third party. Cryptography is also derived from the Greek word ‘cryptos’ which means hidden and ‘graphie’ which means hidden writing and it undergoes the process called encryption. The process of transforming plain text into cipher text is called encryption. Cryptography also provides authentication which is used to verify the identity. Here, the cryptographic process involved is randomized algorithm which consists of parity level and di-bit level.

Cryptographic process:

Step 1: The encryption of parity checking level starts here. The fundamental aspect of this level is that the key for encryption is stored in the data bits pattern itself and this key varies according to the varying data bits. The encryption is done in bit- by-bit operation. For encrypting data bits having index number (odd) like 1 3 5 7, its corresponding key is data bits having index number (even) 2 4 6 8. The two nibbles are then checked bit-by-bit so that the final result has even parity with data bits 1 3 5 7. This final result is the pseudo-encrypted bit pattern 1` 3` 5` 7` likewise even sequence of bits also encrypted.
Step 2: The di-bit level is taking the first and last bits of encrypted bits as reference bits.
Step 3: By using reference bits, the remaining bits are indicated as NC (not complement), LSB-C (least significant bit-complement), MSB-C (most significant bit-complement), FC (full complement). The inverse process is done in decryption process.

III. PROPOSED METHOD

LSB CODING WITH XORING METHOD:
LSB coding gives high bit rate but it is easy to implement and easy to detect. So instead of using simple LSB method alone, combining it with XORing method increases the level of security. This method performs XOR operation on the LSBs and depending on the result of XOR operation and the message bit to be embeds, the LSB of the sample is modified or remains same [2]. The algorithm for data embedding and data retrieval are explained below and tabular representation of embedding process is given in table I.

TABLE I. DATA EMBEDDING USING XORING METHOD

LSB	Bit next to LSB	XOR	if message bit is 0	if message bit is 1
0	0	0	No change	Flip LSB
0	1	1	Flip LSB	No change
1	0	1	Flip LSB	No change
1	1	0	No change	Flip LSB

Steps for data embedding:
1. Read the host audio message and convert it into binary sequence of bits.
2. Read the secret message to be embedded and convert it into binary sequence. Its size must be less than the size of the cover audio.
3. The XORing procedure takes place as follows:
• If the message bit to be embedded is 0, then flip the LSB so that the XORing of LSB and next to LSB is 0.
• If the message bit to be embedded is 1, then flip the LSB so that the XORing of LSB and next to LSB is 1.
4. Embedding of message bit into the LSB’s of the cover audio is done.
5. The modified cover audio samples are then forms the stego audio signal.
Steps for Data Retrieval:
1. Read the Stego audio file.
2. Retrieving of message bit is obtained by XORing the LSB and the bit next to LSB.
• If the result of XORing is 0, then the message bit is 0.
• If the result of XORing is 1, then the message bit is 1.
3. After retrieval of every such 16 message bits, they are converted to their equivalent decimals.
4. Finally the secret message is reconstructed.

IV. PERFORMANCE MEASURES

Mean square error:
It is defined as the square of error between cover audio signal and stego audio signal. The distortion in the audio signal can be measured as follows.

MSE= sqrt $\sum [x(n)-y(n)]^2$

Where x(n) represents audio signal and y(n) represents stego audio signal

PSNR:

It is the measure of quality of audio signal by comparing cover audio with stego audio and it is calculated as follows.

PSNR=10$\log_{10}$ (maxvalue/MSE)

The mean square error values and PSNR values for different data of an audio file can be tabulated approximately as follows.

TABLE II: MSE & PSNR VALUES FOR DIFFERENT SIZES OF DATA

Audio file of size: 188Kb

Data size	MSE	PSNR
10B	0.00021	36.70
50B	0.00042	33.76
100B	0.00069	31.26
300B	0.00112	29.47
500B	0.00147	28.32

IV. EXPERIMENTAL RESULTS

This paper proposes the LSB coding with XORing method in which the data embedding is done by XORing the LSB’s. Fig.2 shows one of the secret signals used in XORing method. Fig.3 shows the secret signal retrieved at the receiver side. It is obvious from both figures that there is no distraction between the original and retrieved message. Thus, by combining steganography and cryptography gives high security.

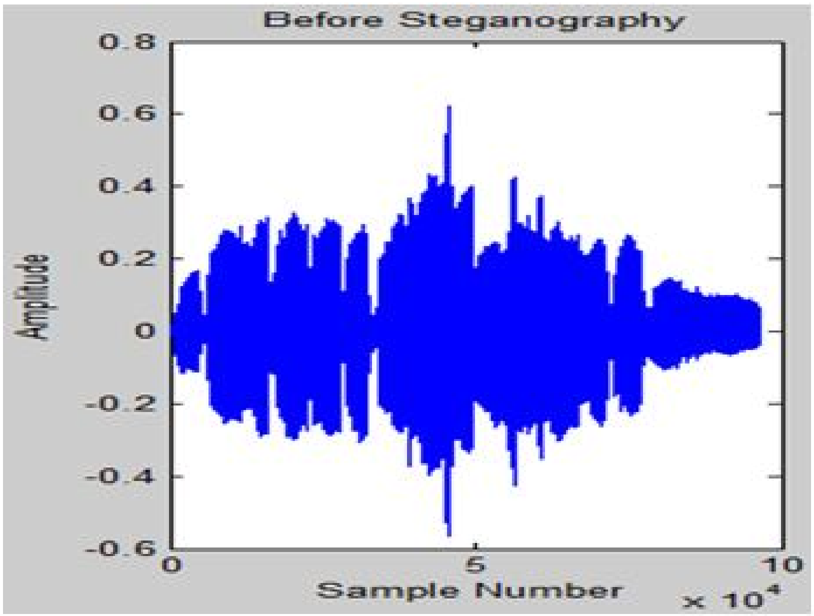

Fig 2: plot of host audio signal

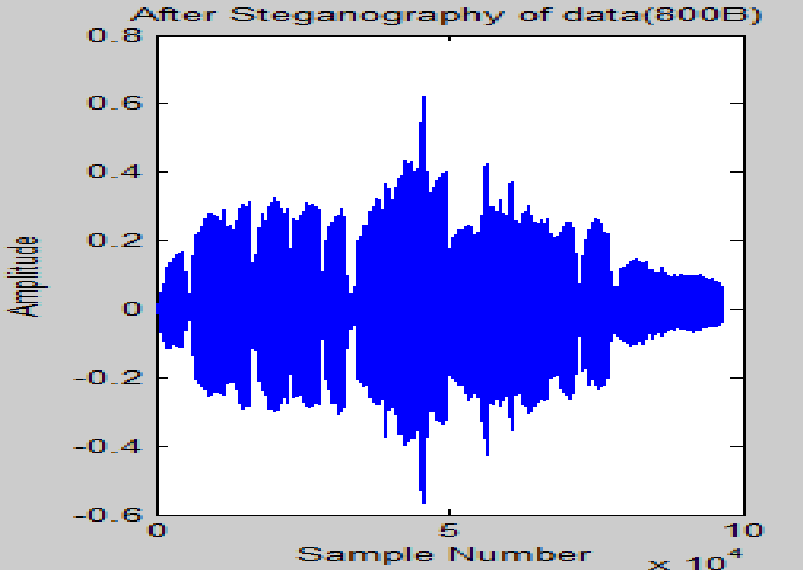

Fig 3: plot of retrieved signal

V. CONCLUSIONS

Audio steganography is more challenging than image steganography because the HAS has more sensitive than human visual system (HVS). This paper proposes the method of LSB coding along with the cryptographic encryption to hide the data in digital audio files. There is no difference between stego audio signal & the original audio signal i.e. hidden information is recovered without any error. It gives great security and high payload capacity

REFERENCES

[1] Bret Dunbar," A detailed look at Steganographic techniques in an open systems environment", SANS institute 2002.
[2] Prof.Sonal k.jagtap, Asst-professor, "Intelligent Processing: An Approach of Audio Steganography", IEEE trans.2012 international conference on 10.11.2009., oct.2012.
[3] Masoud Nosrati et al., World Applied Programming, Audio Steganography: A Survey on Recent Approaches Vol (2), No (3), March 2012.
[4] F.Djebbar, B.Ayady, H.K.Abed Meraimx," A view on latest audio Steganography techniques", International Conference on Innovations in Information technology,2011.
[5] Gunjan Nehru," A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.
[6] Muhammad Asad," An Enhanced Least Significant Bit Modification Technique for Audio Steganography", IEEE trans.2011
[7] An article on "A Brief History of Cryptography", S. Hebert
[8] Modern Cryptography: Theory and practice by Wenbo Mao Hewlett-Packard Company
[9] An article on An Introduction to Cryptography by Edward J.Delp,Purdue University School of Electrical and ComputerEngineering

BIOGRAPHY

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

Mr. T .Ravi Kumar Naidu Assistant Professor, Dept of ECE, Sree Vidyanikethan Engineering College, A. Rangampet, Tirupati received B.Tech in Electronics and Communication Engineering from SVPCET 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, ArraySignal Processing, Image Processing, Video Surveillance, Embedded Systems, Digital Communications.