Performance Improvement: Audio Steganography Technique Parity Bit Combined With Cryptography

Prutha Bhalde
Student ME, Jawaharlal Neheru Engineering College,
Aurangabad, Maharashtra
Prutha.bhalde@gmail.com

ABSTRACT

Data communication over internet is very insecure due to attacks made on data transfer and information sharing. This is the reason why data hiding has become so important for such internet data communication. Conventionally, Cryptography and steganography are two methods which are used to share information in a secured manner. In Cryptography, intermediate person knows that the message is in encrypted form, whereas, when you go for steganographic information sharing, the message is hidden in covered image, audio file or any other type of file, so that any intermediate person never knows whether there is any hidden message in information being shared. Hiding secrete message in an Audio file is called Audio steganography, so that, no other person than a message receiver, be able to read it. There are various audio steganographic methods used to hide information and research is still going on to improve the robustness of these techniques. In order to achieve this robustness against intentional attacks, in which the hackers always try to reveal the hidden message, we have proposed to first encode the message using robust algorithm and then the message is being fed to the traditional steganographic technique like (Parity coding).

Keywords: Steganography, Cryptography, MD5, Stego-file, LSB, Parity-Bit, Hash function, data hiding.

1. INTRODUCTION

Steganography is a Greek word which means secret writing.

Fig. 1.1 Greek Meaning of Steganography

The main aim is to hide the message in such a way that no one apart from the receiver knows that a message has been sent. This can be done by hiding the existence of data within apparently harmless cover or carrier.

Steganographic process is nothing but to cover the hidden data into a medium which can be a text, image, audio or video file providing a key along with it, which is denoted as:

[Carrier] + [Secrete Data] + [stego key] = [stego medium]

The carrier hides the secrete message, and stego key is used to encrypt the data. This results in stego medium which is same as the carrier medium. The carrier mediums may be image or audio files or video files.

Cryptography is to obscure a message or communication so that no one can recognize the hidden message. The main aim of Steganography is to hide information, whereas, that of cryptography, is to make data unreadable by a third party.

In steganography, the structure of the secrete message is hidden under the cover image so as to make it invisible, without altering the original structure of the message. That is the reason why steganography is used widely over cryptography as it can hide the whole message, enabling the third person not be able to see the message or get to know that any message is being transferred under the audio cover. If we use these form of steganography along with various forms of cryptographic methods, it becomes more secured for communication. Firstly the message can be encrypted and then hidden under the audio file.

When a hacker tries to hack the communicating message, he will need to find the data under the audio file and then apply decryption algorithms. It may happen that the message gets recognized easily but it may not be always possible to again decrypt without its key, making the message more robust. Cryptographic methods protect the content of a message, while Steganographic methods hide both the message as well as the content. Using Steganography along with Cryptography, better security can be achieved.

1.1 Cryptography using hash Function: MD5 message digestive

MD5 is a cryptographic message digest hash function designed by Ronald Rivest in 1991 to replace earlier hash function MD4.

The main reason to use a hash function is that it is extremely easy to calculate a hash for any message though it is computationally hard to calculate an alphanumeric text that has given a hash. Moreover, it is extremely

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org
***ICTCS '16,* March 04 - 05, 2016, Udaipur, India**
**Copyright is held by the owner/author(s).
Publication rights licensed to ACM.**
**ACM ISBN 978-1-4503-3962-9/16/03□$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905196**

unlikely that two slightly different message will have same hash.

The message is the input and hash function is called as digest. MD5 is a hash function used to encrypt a variable length text to a fixed-length output of 128 bits file. The input message is modularized into small blocks of 512-bits i.e. chunks of sixteen 32-bits words.

The first step is appending Padding Bits. The original message is extended so that its length is congruent to 448, modulo 512. Where, the original message is always padded with 1's first and then 0's are padded to bring the length of the message up to 64 bits.

In second step, 64 bits are concatenated to the end of the message to indicate the length of the original message in bytes, where the length of the original message is converted to its binary format of 64 bits. Only 64 low-order bits are utilized, if overflow happen.

Then, break the 64-bit length into 2 words (32 bits each). The low-order word is appended first followed by the high-order word.

MD5 algorithm requires a 128-bit buffer with a specific initial value. In third step, the buffer is divided into 4 words (32 bits each), named as A, B, C, and D and are initialized to 0x67452301, 0xEFCDAB89, 0x98BADCFE and 0x10325476 respectively.

In fourth step, message is processed in 512-bit Blocks. This is the main step of MD5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round which are as followed.

$$F(X, Y, Z) = XY \text{ v } \text{not}(X)\ Z$$
$$G(X, Y, Z) = XZ \text{ v } Y \text{ not } (Z)$$
$$H(X, Y, Z) = X \text{ xor } Y \text{ xor } Z$$
$$I(X, Y, Z) = Y \text{ xor } (X \text{ v not } (Z))$$

In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X)Z will never have 1's in the same bit position.) It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X, Y, Z) will be independent and unbiased.

The functions G, H, and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X, Y, Z), H(X, Y, Z), and I(X, Y, Z) will be independent and unbiased. Note that the function H is the bit-wise "xor" or "parity" function of its inputs.

1.2 Audio Steganography

The basic Structure of Audio steganography consists of Carrier (which is nothing but an Audio file), communication Message/ information to be transferred and Password. Carrier is also known as a cover-file, which encapsulates the secret information.

The model for steganography is shown in Fig 3. The sender always wants to keep the communication Message confidential, which can be in any form like plain text, image, audio or any type of file. Password is known as a stego-key. This key take cares that only the receiver to whom the message is to be communicated, should be able to decrypt the message from a cover-file. Only the receiver knows the stego key. The cover-file with the secret information is known as a stego-file.

The process of hiding information has following two steps [9, 10].

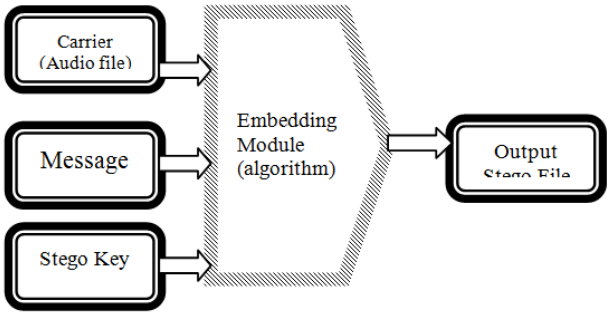

Fig. 1.2 Process of Steganography

i. Redundant bits detection in a cover-file. Redundant bits are those bits which can be modified without corrupting the quality or destroying the integrity of the cover-file.
ii. Hiding secret information in the cover file and replacing the redundant bits in the cover file with the bits of the secret information.

Audio steganography is on of the most effective way to protect your message being hacked by the intermediate person. It is the most challenging technique because Human Auditory System (HAS) has a dynamic range that it can listen over. But the only drawback is to differentiate the minute differences in the audio file. Taking this as advantage, audio file are used to cover message to communicate in steganographic transform.

There are various Techniques used for Audio Steganography such as:

LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data [11].

Parity coding algorithm is one of the robust audio steganographic techniques which breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region.

Phase coding technique replaces the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments.

Spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal [2]. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission.

LSB coding is not much secured in nature, which can be considered as major disadvantage of this method.

The main disadvantages associated with the use of existing methods like spread spectrum are human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness.

Phase coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred.

Thus, parity bit is advantageous over such methods.

1.3 Parity Bit coding

In parity bit coding, signals are modularized into separate samples and each module is embedded individually with a secret message from a parity bit, instead of breaking into individual sample. Secret message hiding into the sample regions parity bit [1]. Firstly breaks down the signal into separate regions of samples and encode each bit from secret message in a sample regions parity bit. If the parity bit of sample region does not match with secret message bit then process flips the least significant bit of the samples in the region. It provides more choice to the sender for encoding the secret message and the signal can be changed in a more unobtrusive manner.
Steps used in Parity Method :

- Even Parity is: No. of one's is even.
- Odd Parity is: No. of one's is odd.
- Cover File is broken into samples of 16 bits.
- Least significant bits are modified comparing the parity of samples.

$$SNR_{DB} = 10 \text{ Log }_{10} (A_{signal} / A_{noise})$$
$$= 20 \text{ Log }_{10} (A_{signal} / A_{noise})$$

The LSB is replaced at higher LSB layer. The parity of samples of audio file is checked along with secret message bit and accordingly LSB of sample is replaced.

The benefit of using this method is that the LSB at higher layer makes it imperceptible. As data is hidden at higher level, it increases the capacity to hold lengthy text. Using this algorithm reduces distortion due to noise, which makes it difficult to detect hidden text.

Algorithm:

1. Input Audio File in .wav format and find total count size.
2. Input the secret message which is converted to binary format.
3. Create 16 bit samples of cover audio.
4. Select higher order LSB.
5. Implant LSB's of samples into the secret message.
6. Check the parity of each sample.
7. No change in LSB if message to be embedded is 0 and parity of sample is even.
8. Change LSB to 0 if message to be embedded was 1and parity of sample is even.
9. Change LSB to 1 if message to be embedded was 0 and parity of sample is odd.
10. No change in LSB if message to be embedded was 1 and parity of sample is odd.
11. Transfer the modified audio to next level.
12. Check parity of samples at the receiving end.
13. Message bit is 1 if parity is odd.
14. Message bit is 0 if parity is even.

2. LITERATURE SURVEY

Many algorithms have been proposed for robust Steganography. Manipulation and addition of redundant noise as secret key in the message is known as Least Significant Bit (LSB). This method is applied to hide data in images. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) both are used for data hiding in audio files.

Method was used where, instead of original message, an encrypted message by Prime Number and Gray Code Encryption (PGE) Algorithm is hidden into an Image (Stego Image) using a new approach named Linear Block parity coding (LBP) which provides more security than conventional approaches. The computational complexity of this method low comparatively with other methods because feature vector space is limited interference is not objectionable.

One method with using HAS including Parity Coding, Least Significant Bit (LSB) Coding, Phase Coding, Echo data hiding and Spread Spectrum (SS) and some basic concept of audio steganography is used to increase the robustness of the algorithm.

One more technique of steganography, i.e. Hash-LSB with RSA algorithm, for providing more robustness to data as well as our data hiding method is being used. It uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image [5].

3. PROPOSED WORK

To make steganography more robust and secured it is proposed to combine it with cryptography. It means, combining the algorithm of embedding the message into the cover message along with encrypted data can help increase the robustness of the method.

When we use parity coding method, we can use a robust method to encode the message that is need to be send over the network, and this cipher text is then surpassed to form a stego file by covering it into the audio file.

This process adds a new layer over the regular parity bit coding steganographic method shown in figure 3.1.

This will consist of three layers:

1. Encrypt the message using MD5 message digest algorithm of cryptography. This will contain its own key.
2. Cover this encrypted message output from MD5 into the cover file i.e. audio file using parity coding algorithm. There will be another separate stego key for this stage now. For more secured purpose we use different keys in both the stages but to make it simple we can use the same key at each level. This makes it easier to remember the key but makes it less robust. To avoid this discrepancy I have used different keys in both the algorithm.
3. This whole process gives an output stego file which is much more robust than the regular parity coding algorithm.

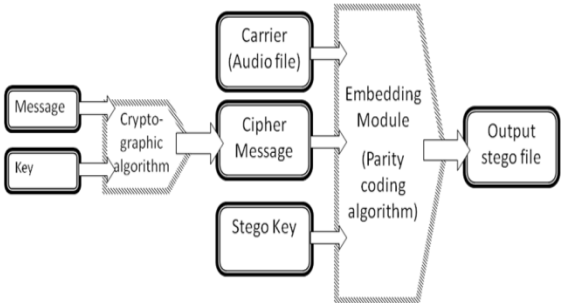

Fig. 3.1 Process of Steganography with cryptography in parity coding

4. RESULTS

For encryption of the text message that is to be hidden under the cover file, I have used MD5 hash function algorithm, completing the code in VB.net using MD5 *CryptoServiceprovider*, we can get the encrypted text easily. The output images are given below:

Firstly message is encrypted using MD5 algorithm: "This is a message to encrypt." Considering this as a message to encrypt, we get the following as output encrypted message shown in figure 4.1.For doing further process, an audio file of wave format is taken as input to the parity bit algorithm. Plotting this file looks like figure 4.2. The sound file is also plot to its magnitude which is shown in figure 4.3.

After applying parity bit algorithm, the file looks like figure 4.4.The audio file is plot to its magnitude in figure 4.5 after applying audio steganography.

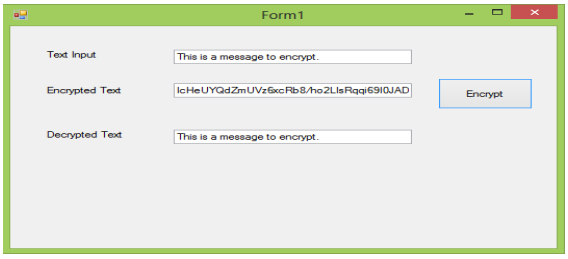

Fig. 4.1 Cryptography of text file using MD5 message digest algorithm;

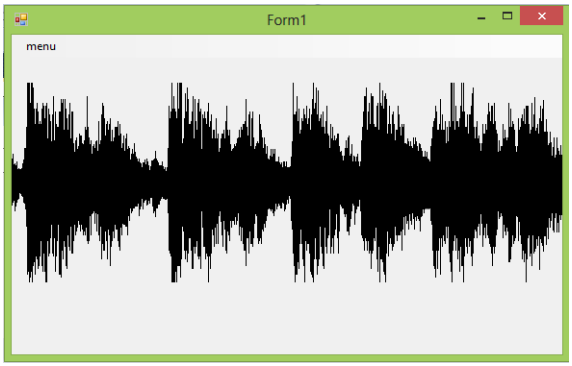

Figure 4.2 Original Sound.wav audio file graph

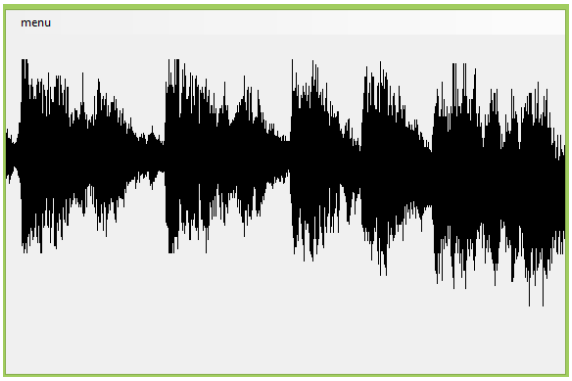

Figure 4.3 Stego Sound.wav audio file graph after applying Parity Bit Algorithm.

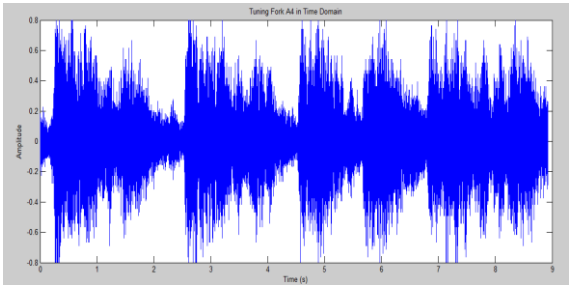

Fig. 4.4 Original Sound.wav audio file plot per magnitude

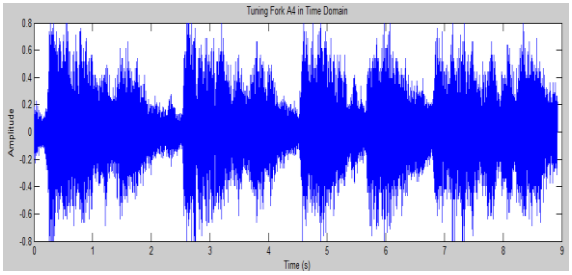

Figure 4.5 Stego Sound.wav audio file after applying parity bit algorithm plot by magnitude

5. CONCLUSION

In this paper, I presented an over view of audio steganography starting with introductions and basic principles and proceeding through specific techniques of parity bit algorithm along with cryptographic method that is message digest hash function of MD5 method. There are many specific techniques for embedding data within the various mediums like text, images, video and sound to text to IP packets, and each has its own strengths and weaknesses. Some such as LSB encoding, are considered especially weak where as Parity bit is one of the robust technique. Taking all of this data I have used parity bit along with cryptographic method MD5 message digest algorithm. MD5 is widely used hash based algorithm in today's world which is very hard to decrypt. This allows making the message more secured and hard to decrypt. I tried this algorithm on wave file which can be further used on other audio formats so as to store more data.

6. REFERENCES

[1] Anil Kumar , Rohini Sharma, *A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[2] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, *An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution*, International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.

[3] Ch. Rupa, P. S Avadhani, E. SrinivasReddy, A*n efficient security approach using PGE And parity coding*, international Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6, November 2012.

[4] C. C. Chang, T. S. Chen and H. S. Hsia, *An Effective Image Stenographic Scheme Based on Wavelet Transform and Pattern- Based Modification*, IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[5] Fatiha Djebbar and Beghdad Ayad and Karim Abed Meraim and Habib Hamam, *Comparative Study of Digital Audio Steganography Techniques*, EURASIP journal on audio, speech and music processing, Oct 2012.

[6] Gunjan Nehru, Puja Dhar, *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.

[7] Kamalpreet Kaur and DeepankarVerma, *Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique*, International Journal of Advanced Research in Computer Science and Software Engineering, January 2014.

[8] K.Sakthisudhan, P.Prabhu and P.Thangaraj, *Secure Audio Steganography for Hiding Secret information*, International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012).

[9] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, *Audio Steganography: A Survey on Recent0020Approaches*, World Applied Programming, Vol (2), No (3), March 2012.

[10] Nishu Gupta, Mrs.Shailja, *A Practical Three Layered Approach of Data Hiding Using Audio Steganography*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014.

[11] S.S. Divya, M. Ram Mohan Reddy, *Hiding Text in Audio using Multiple LSB Steganography and provide Security using Cryptography*, International Journal of Scientific and Technology Research, July 2012.

[12] Yan Diqun, Wang Rangding, Zhang Liguang, *Quantization step parity-based Steganography for MP3 Audio*, IOS Press, Fundamenta informaticae 97 2009.