Error Correction in Audio Steganography

Ajisha P
Department of Electronics and Communication
KMCT college of Engineering
Calicut, India

Shobin Mathew
Department of Applied Electronics and Instrumentation
KMCT college of Engineering
Calicut, India

***Abstract*— This paper presents an improved technique for hiding data in audio. The proposed method modifies the LSB of samples of the cover audio file to embed the secret message. To increase the security of the proposed scheme, using a key to adjust the hiding technique. To increase the robustness of this scheme, using hamming code as error correction code . The suggested scheme does not need the original signal for extracting the hidden bits. Under the context of using audio as the host message, this could mean that stego-audio file sounds looks almost like the original audio file. The secret message might be a text, an image, or any data that can be represented in the form of a stream of bits. Hiding data in audio use the weakness of the HAS to embed the hidden data in the regions of the audio signals at which human ears are unable to perceive the distortion caused by the data embedding process. The HAS is much more sensitive than the HVS, so the space of frequency domain or time domain in audio signals where data can be embedded imperceptibly is limited. Using a key as a seed to generate a binary string and the amplitude of the cover audio are adjusted based on this binary string. In data transmission lots of noises will be there, transmitting station must add extra data (called error correction bits) to the transmission. Parity bits are adding in the data . If an odd number of bits is changed in transmission, the message will change parity and the error can be detected. In received message, using hamming matrix finds the error location and removing the errors.**

Keywords*— *Steganography, hamming code, random numbe, phase coding, perceptiveness;

I. INTRODUCTION

Digital representation of media facilitates access and potentially improves the portability, efficiency , and accuracy of the information presented. The undesirable effects of facile data access include an increased opportunity for violation of copyright and tampering with or modification of content, which makes the information security becomes an important and urgent issue. The security of information often lies in the secrecy of its existence and/or the secrecy of how to decode it. Mainly there are two ways of concealing information: cryptography and steganography. Cryptography's main aspect is that the information is somehow scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The term steganography is the technique of embedding secret information in a communication channel in such a manner that the existence of the information is concealed [1]. A number of different cover objects (signals) can be used to carry hidden messages. Steganography techniques have been successfully applied on text files, images, audio and video files. Steganography in image exploits the weakness of the human visual system (HVS) while steganography in audio relies on the imperfection of the human auditory system (HAS). A steganography system , is expected to meet three key requirements, namely, the imperceptibility of embedding, correct recovery of embedded information, and large payload [2]. Some degradation in the perceptual quality of the stegosignal from that of the original host signal may be acceptable.

Steganography can be defined in equation (1) and equation (2). Given host message H and a guest message G. A steganography scheme should provide a data hiding function Sh and a data retrieving function Sr such that:

$$H' = Sh(H,G,K) \quad (1)$$

$$Sr(H',K) = Sr(Sh(H,G,K), K) = G \quad (2)$$

where K is the secrete key. That is, Sr can extract the guest message from the host message hidden by Sh. Further, to distract the opponents, it should be hardly detectable that H' has been hidden with information. Under the context of using audio as the host message, this could mean that H' sounds looks almost like the original H [3]. Fig.1. is an illustration of an audio steganography system.

The secret message might be a text, an image, or any data that can be represented in the form of a stream of bits.

Hiding data in audio use the weakness of the HAS to embed the hidden data in the regions of the audio signals at which human ears are unable to perceive the distortion caused by the data embedding process. The HAS is much more sensitive than the HVS, so the space of frequency domain or time domain in audio signals where data can be embedded imperceptibly is limited.

In this paper, present a method for hiding data in audio. The proposed method modifies the LSB of the samples

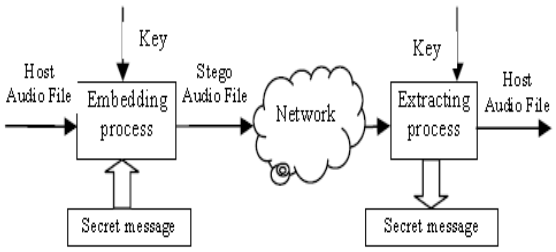

Fig. 1. A diagram of the audio steganography system.

of cover audio file to embed the secret message. Also use a key as a seed to generate a binary string and the amplitude

of the cover audio are adjusted based on this binary string. To increase the robustness of this scheme, using hamming code as error correction code . Adding parity bits in selected parity spots of the encrypted message before transmission . Parity bits indicates whether the number of ones (bit-positions with values of one) in the preceding data was even or odd. If an odd number of bits is changed in transmission, the message will change parity and the error can be detected. This error can be removed and decode to remove the parity bits.

II. RELATED STUDY

There are many techniques for hiding secret data or messages in audio in a way that the modifications made to the embedding domain, the hiding techniques can be classified into time domain and frequency domain methods. In time domain schemes, the hidden bits are embedded directly into the time signal samples. These methods are easy to implement and are usually very efficient but they tend to be weak against common signal processing attacks. In frequency domain, after taking one of the usual transforms such as Fast Fourier Transform (FFT), Discrete Wavelet Transform (DWT) from the signal, the hidden bits are embedded into the resulting transform coefficients. Using methods based on transforms provides a better perception quality and robustness against common attacks at the price of increasing the computational complexity [3].

A. Parity Coding.

Parity coding is one of the robust audio steganographic technique. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit[4][6]. 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. Thus, the sender has more of a choice in encoding the secret bit. Fig.2. shows the parity coding procedure.

B. Phase Coding.

The phase coding technique works by replacing 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. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods[6]. When there is a drastic change in the phase relation between each

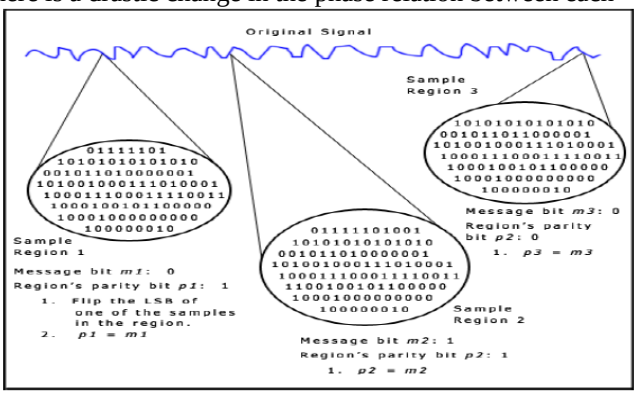

Fig .2. Parity coding

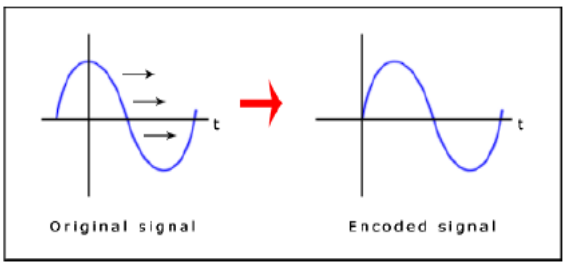

Fig. 3. The signals before and after Phase coding procedure.

frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved.

This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise. Phase coding is explained in the following procedure:

a. Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.
b. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
c. Calculate the Phase differences between adjacent segments.
d. Phase shifts between adjacent segments are easily detectable. It means, we can change the absolute phases of the segments but the relative phase differences between adjacent segments must be preserved. So the secret information is inserted only in the phase vector of the first signal segment as follows in equation (3):

$$\text{phase\_new} = \begin{cases} \pi/2 & \text{if message bit=0} \\ -\pi/2 & \text{if message bit=1} \end{cases} \quad (3)$$

e. Using the new phase of the first segment a new phase matrix is created and the original phase differences.
f. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.

The receiver must know the segment length to extract the secret information from the sound file. Then the receiver can use the DFT to get the phases and extract the secret information. Consider Fig.3. For phase coding procedure.

III. PROPOSED METHOD

The proposed method modifies the amplitude of the cover audio file to embed the secret message. To increase the security of the proposed scheme, we use a key to adjust the hiding technique. The suggested scheme does not need the original signal for extracting the hidden bits. To increase the robustness of this scheme, using hamming code as error

correction code . Here, inserting parity bits in data before transmission to detect the errors. Number of parity bits needs to be added is calculates using the length of encrypted message. And finding the parity bits using hamming matrix. Adding parity bits in selected parity spots of the encrypted message before transmission . If an odd number of bits is changed in transmission, the message will change parity and the error can be detected. In received message, using hamming matrix finds the error location and removing this error. Then decode the message to remove the parity bits. The Fig 4 and Fig 5 represents block diagram of embedding and extracting process for hiding secret data.

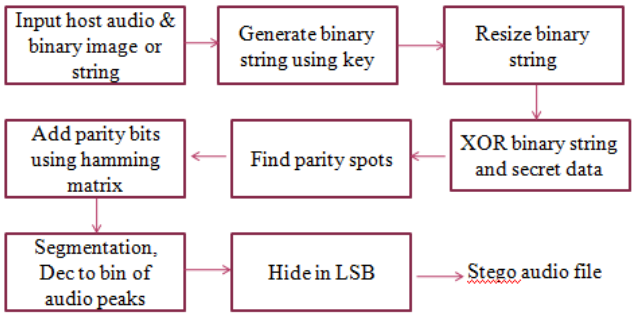

Fig .4. Block diagram of the embedding process

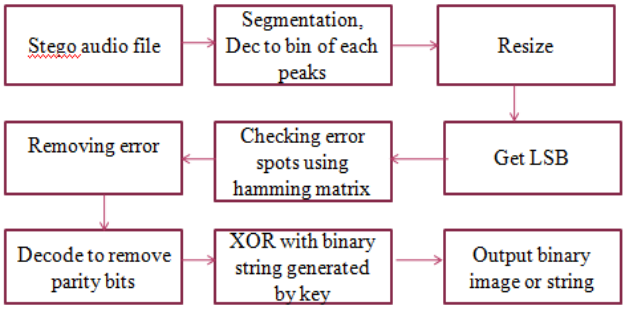

Fig .5. Block diagram of the extracting process

A. *Generate Pseudo-Random Numbers.*

Pseudo-random number generators (PRNG) are algorithms that can automatically create long runs of numbers with good random properties but eventually the sequence repeats (or the memory usage grows without bound) [6][7]. The string of values generated by such algorithms is generally determined by a fixed number called a seed. One of the most common PRNG is the linear congruential generator, which uses the equation (4) to generate numbers.

$$X_{n+1}=(aX_n+ b)\bmod m \quad (4)$$

where X0 is a seed and a, b, m are constants.

In the proposed scheme, using the multiplicative congruential generator (MCG) to generate the binary string. Parameters used in pseudo-random sequence generator is composed of three numbers (seed, a, m), is the key used in the embedding process and the extracting process. The formula to generate the binary string R is defined in equation (5) and equation (6).

$$X_{n+1}=(aX_n)\bmod m \quad (5)$$

$$R_i=X_i \bmod 2 \quad (6)$$

If we use key is the set of three numbers (7, 5, 37) to generate X and R, the result is in Table I

TABLE I value of binary string using MCG

Vetor	1	2	3	4	5	6	7	8	9	10
X	7	35	27	24	9	8	3	15	1	5
R	1	1	1	0	1	0	1	1	1	1

B. *Error-correction Code*

An error-correcting code (ECC) or forward error correction (FEC) code is a process of adding redundant data, or *parity data*, to a message, such that it can be recovered by a receiver even when a number of errors (up to the capability of the code being used) were introduced, either during the process of transmission, or on storage. Since the receiver does not have to ask the sender for retransmission of the data, a backchannel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting[8]. Error-correcting codes are frequently used in lower-layer communication, as well as for reliable storage in media such as CDs, DVDs, hard disks, and RAM[10].

Error-correcting codes are usually distinguished between convolutional codes and block codes. repetition codes, Hamming codes and multidimensional parity-check codes are examples of block codes.

1. *Hamming Codes*

Hamming codes are a family of linear error-correcting codes. Inserting parity bits in data before transmission to detect the errors. Parity bit indicates whether the number of ones (bit-positions with values of one) in the preceding data was even or odd. If an odd number of bits is changed in transmission, the message will change parity and the error can be detected at this point; however, the bit that changed may have been the parity bit itself. The most common convention is that a parity value of one indicates that there is an odd number of ones in the data, and a parity value of zero indicates that there is an even number of ones[9]. If the number of bits changed is even, the check bit will be valid and the error will not be detected.

Number of parity bits needs to be added is calculates using the length of encrypted message using the equation (7).

$$nbp=floor(log2(n+ceil(log2(n))))+1 \quad (7)$$

And finding the parity bits using hamming matrix. Adding parity bits in every 2^n position .

If an odd number of bits is changed in transmission, the message will change parity and the error can be detected. In received message, using hamming matrix finds the error location and removing this error. Then decode the message to remove the parity bits.

C. The Embeded Algorithm

To hide a secret bit, modify the amplitude of the audio sample, based on the value of Ri.

Algorithm:

Input: Host audio file H, secret key (seed, a, m), secret message (in binary form).

Output: Stego-audio file H'.

- Step 1
  - Using the secret key (seed,a,m) to generate the binary vector R.
- Step 2
  - Read the host audio file H to get the audio samples Y.
  - Divide the audio file into equal segments with 2048 samples.
- Step 3
  - Read the secret message. ie,binary image or a string.
  - Get data of secret message.
- Step 4
  - Resize the binary string from key.
- Step 5
  - Find peaks, and convert decimal to binary.
  - XOR binary string with secret data.
- Step 6
  - Measure the length n of this encrypted message .
  - Number of parity bits

    nbp=floor(log2(n+ceil(log2(n))))+1

- Step 7
  - Even parity
  - Find parity spots
  - Find parity bits using hamming matrix.
  - Insert parity bits
- Step 8
  - Get LSB of each sample and replace the LSB with the parity bit added message.

D. The Extracted Algorithm

Input: Stego-audio file H', secret key (seed, a, m), the length of the hidden message q.

Output: Secret message M.

- Step 1.
  - Read the stego-audio file H' to get the audio samples Y.
  - Divide the stego-audio file into segments with 2048 samples each segment.
- Step 2.
  - Using the secret key (seed, a, m) to generate the binary vector R contains q elements.
- Step 3.
  - Find peaks, and convert decimal to binary.
  - Get LSB of each samples.
- Step 4
  - Generate hamming matrix for error check.
  - Remove error
  - Decode to remove parity bits.
- Step 5
  - XOR the LSB string with binary string which is generated by key.

IV. EXPERIMENTAL RESULTS

In the experiment, using a host audio file with size 308 KB. The secret message is a string or binary image of 256x256. The security of the proposed scheme is based on the key used for generating the binary vector R. If the steganalyst knows the modify scheme but has no key, he cannot extract the secret message. Here, key used is the set of three numbers (7, 5, 37).

Fig. 6. shows the input binary image and Fig.7. shows the wave form of the host audio. Fig. 8. shows the audio file with secret message and Fig.9. shows the output image.

Fig.6. input binary image.

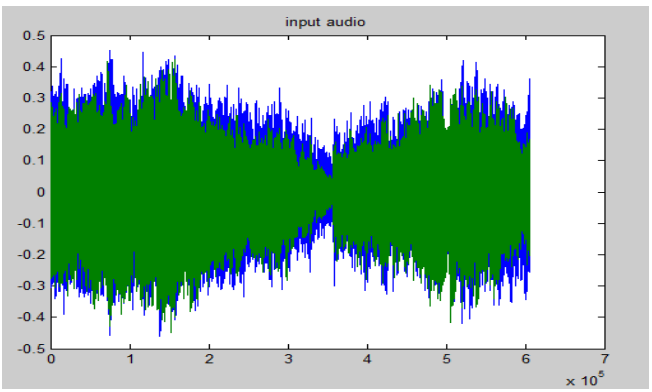

Fig. 7. host audio file

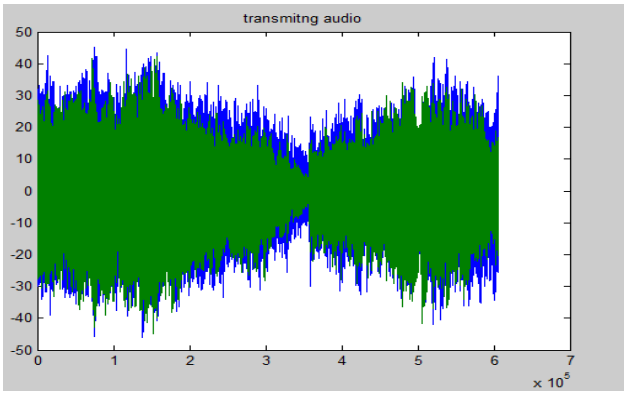

Fig.8. Audio file with secret data.

fig.9 Output image

V CONCLUSIONS

In this paper, a scheme for hiding data in audio has been proposed. The proposed method modifies the amplitude of the cover audio file to embed the secret message. To increase the security of the proposed scheme, using a key to adjust the hiding technique. To increase the robustness of this scheme, using hamming code as error correction code .The experiment shows that this method is secure, imperceptible and can be used for hiding data in the audio file. If the steganalyst knows the modify scheme but has no key, he cannot extract the secret message.

ACKNOWLEDGMENT

I would like to thank my project guide Asst.Prof .Shobin mathew and Head of the Department Asst.Prof. Nishida.T for their guidance and support and also grateful to all the staff members of the Department of Electronics&Communication Engineering of KMCT College of Engineering and Technology, Calicut for providing all the important facilities like internet access and books, which were essential to carry out the project. I am grateful to Huynh Ba Dieu and Nguyen xuan huy making their source codes open to public. I also thank my family, friends for their support and encouragement.

REFERENCES

[1] An Improved Technique for Hiding Data in Audio,Huynh Ba Dieu,Nguyen xuan huy ISBN: 978-1-4799-3724-0, 2014 IEEE.
[2] F. Djebbar, B. Ayady, H. Hamamz and K. A Meraim, “A view on latest audio steganography techniques”, Proc. International Conference on Innovations in Information Technology (IIT 2011).
[3] Information hiding using audio steganography – a survey, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3.
[4] Hiding Text in Audio Using LSB Based Steganography, Information and Knowledge Management www.iiste.org,ISSN 2224-5758,ISSN 2224-896X ,Vol 2, No.3.
[5] M. Fallahpour, D. Megías, “High Capacity Method for Real-Time Audio Data Hiding Using the FFT Transform”, Advances in Information Security and Its Application,springer-verlag pp 91-97
[6] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.
[7] information hiding using audio steganography – a survey,The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011
[8] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography” ICASSP 2008
[9] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001
[10] M. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.
[11] R.A. Santosa and P. Bao, “Audio-to-image wavelet transform based audio steganography,” Proc. Of 47th Int. Symposium ELMAR, June 2005, pp. 209- 212.