An Efficient New Audio Steganography Scheme based on Location Selection with Enhanced Security

Shweta Vinayakarao Jadhav
Dept. of Electronics & Telecommunication Engg.
Chhatrapati Shahu College of Engineering,
Aurangabad, India.

Prof. A.M Rawate
Dept. of Electronics & Telecommunication Engg.
Chhatrapati Shahu College of Engineering,
Aurangabad, India.

Abstract— Steganography is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. The goal of steganography is different from classical encryption, which seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages. In this paper a new scheme for digital audio steganography is presented where the bits of a secret message are embedded into the coefficients of a cover audio. Each secret bit is embedded into the selected position of a cover coefficient. The position for insertion of a secret bit is selected from the 0th (Least Significant Bit) to 7th LSB based on the upper three MSB (Most Significant Bit). Also to improve the security, we had used GSM module at receiver end. While extracting data at receiver end, you have to enter the key, which you had used for data hiding process. If user given any wrong key then automatically we are sending message to authorized user as (Someone is trying to hack your data). This scheme provides high audio quality, robustness and lossless recovery from the cover Audio.

Index Terms— Header/Data separation, Location analysis, LSB substitution, Chaotic Encryption.

INTRODUCTION

Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it's projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that "security through obscurity" isn't necessarily a bad thing, provided that it isn't the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful 3rd party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention being distributed in the picture then it would otherwise.

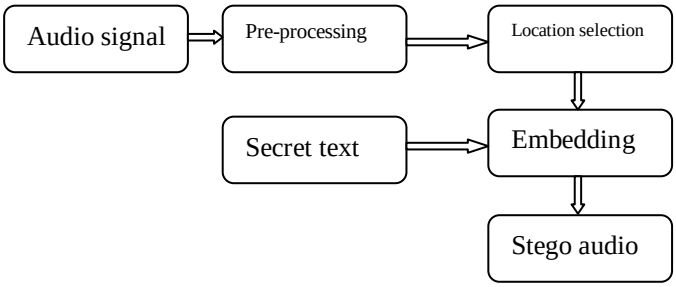


Fig 1: Tentative Model

The technique is compared with previous techniques as applied to simulated and unwanted parameters ie, mean square error and peak signal to noise ratio will be calculated for performance evaluation.

II. LITERATURE OVERVIEW

2.1.1 LSB: LSB [5], [6] is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used technique for audio steganography. In LSB encoding, the least significant bits of the cover media/original audio is altered to include the secret message. Even though this is a simple method, an attacker can easily extract the secret message from the stegano object.

2.1.2 Parity coding: Parity coding technique [3], [4] operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of each group is calculated. For inserting message bit one by one, check the parity bit of a group of samples. If the parity bit and message bit matches do nothing. Otherwise change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit.

2.1.3 Echo hiding: In echo hiding [7] method data is embedded in the echo part of the host audio signal. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio. Due to its low embedding rate and low security no researches are going on echo hiding technique.

III PROPOSED METHOD THEORY

Initially the secrete message has to encrypted with some standard encryption algorithm with a key supplied by the sender and shared with the receiver. Then the position for insertion inside the sample of the carrier audio file has to be selected based on the decimal value of first 3 MSB bits. Suppose, first 3 MSB bits' of a sample are 100 (decimal value is 4), then one bit of the secrete message has to be inserted at the 4th position of the corresponding sample of carrier audio file. After the decimal value for 3 MSB bits are considered for the next sample and similarly the next secrete bit has to be put at the decimal valued position and the process will be repeated for each bit in the secrete message till the full secrete message is hidden. The encoding example is as shown in fig. 2.

Fig 2. Bits of a secret Message are embedded in a 16-bit CD quality sample using the proposed method

Algorithm for encoding

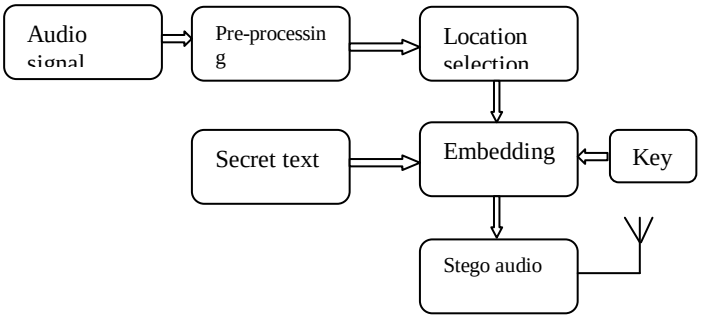
Input: Audio file in WAV format to use as carrier and the Secret Message to hide as text file, a key for encryption.

Output: Stego Audio File containing hidden message

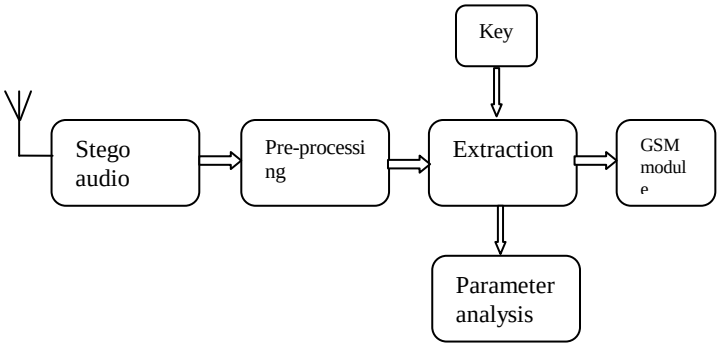
The steps are as follows:-

- The secrete message has to be encrypted using a key supplied by the sender and shared with the receiver. Consider the binary of the cipher text of the secrete message to be hidden. If the secret message is in text then convert it into the respective ASCII [4] value and after that it will be converted into binary pattern.
- Read a secret bit from the sequence to hide.
- Convert each audio sample into a 16 bit sequence.
- For each audio sample value
  - From the carrier sample first (MSB) 3 bits to be read and converted into decimal value. That generated values is the insertion position of the secret bit inside that audio sample.
  - Insert a secret bit into a selected position which was determined by the previous step.
  - Repeat the steps until all the secret bit values are replaced.

Transmitter:



Receiver:



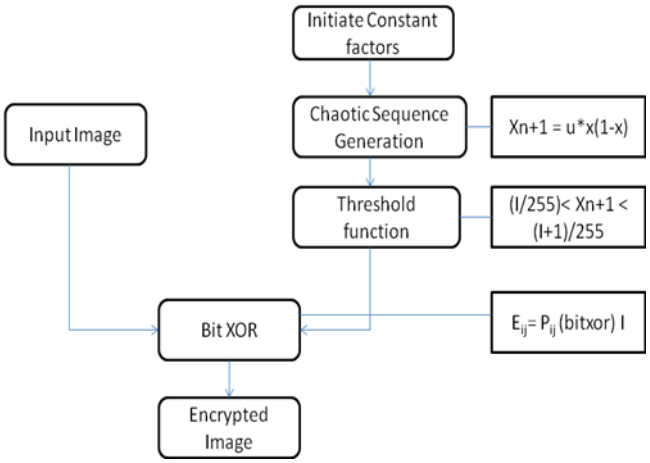
Chaotic Encryption Scheme:

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is High level security. The encryption is achieved by iteration. Simplest. No short cuts are available. Whereas the requirement of large cipher storage and slow in speed are considered the major disadvantages. The properties of chaos are slightly producing some changes in the entire.

cryptography. Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values. The topology transitivity defines

that the state points reside in a bounded space state and approaches.

Process Flow



QUALITY MEASURES FOR IMAGE The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σq2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE} = \sigma_q^{\,2} = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^{\,2}$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

Correlation Coefficient: It is used to find the similarity between two different images with their intensities. It will be described by,

Cor_coef = [sum (sum (u1.*u2))] / [sqrt (sum(sum(u1.*u1))*sum(sum(u2.*u2)))];

IV CONCLUSION

In the proposed scheme, the secrete message will be embedded at selective positions within the audio carrier also we had used secret key to increase the security (the selective positions to be generated by the encoding process), it can be considered as better and efficient method for hiding the data. This proposed system will not change the size of the file even after embedding and also suitable for any type of audio file format. Also the encoding and decoding techniques are similar to be implemented. Though it is a well built system, it has been limited to some restrictions. Quality of the sound depends upon the size of the audio file selected by the user and the length of the message to be hidden. There are a number of ways that this project can be extended. Its performance can be upgraded to higher levels by using a better algorithm for encoding and decoding. Instead of having random insertion point generated by the decimal conversion of 3 MSB bits we can use a secret bit pattern to make this algorithm more secure. While extracting data, user has to enter the secret key. We had used GSM module in case of any incorrect key we are sending message to authorized person.

V REFERENCES

[1] Sara Khosravi, MashallahAbbasiDezfoli, Mohammad HosseinYektaie, " A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication" , Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA,2000.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.

[4] Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at:http://www.krenn.nl/univ/cry/steg/article.pdf

[5] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

[6] ShashikalaChannalli et al ," Steganography An Art of Hiding Data "International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[7] Gruhl D, Lu A, Bender W. Echo hiding. Lecture Notes inComputer Science, 1996, 1174: 295-315.

[8] Xu Chansheng, Wu Jiankang, Sun Quibin, et al. Applications of digital watermarking technology in audio signals. Journal of Audio Engineering Society, 1999, 47(10): 805-812.

[9] Garcia R A. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In: 107th AES Convention. New York, USA, 1999:2713-2720.

[10] XU Shuzheng, ZHANG Peng, WANG Pengjun, YANG Huazhong, "Performance Analysis of Data Hiding

in MPEG-4 AAC Audio" TSINGHUA SCIENCE AND TECHNOLOGY Volume 14, Number 1, February 2009.

[11] MengyuQiao, Andrew H. Sung, Qingzhong Liu, "Steganalysis of MP3Stego" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009.

[12] Sridevi, R., Damodaram, A., Narasimham, S.V.L.: Efficient Method of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enhanced Security. Journal of Theoretical and Applied Information Technology (2005)

[13] Cvejic, N., Seppanen, T.: Increasing Robustness of LSB Audio Steganography using a novel embedding method. Proc. IEEE Int. Conf Info. Tech.: Coding and Computing 2, 533–537 (2004)

[14] Cvejic, N., Seppänen, T.: Reduced distortion bit-modification for LSB audio steganography. In: ICSP Proceedings. IEEE (2004)

[15] K. Bhowal, D. Bhattacharyya, A Pal, T-H Kim A GA based audio steganography with enhanced security, Telecommunication Systems April 2013, Volume 52, Issue 4, pp 2197-2204.

