ISSN XXXX XXXX © 2016 IJESC

Research Article Volume 6 Issue No. 8

A New Audio Steganography with Enhanced Security based on Location Selection Scheme

Shweta Vinayakarao Jadhav[1], Prof. A.M Rawate[2]
Department of Electronics & Telecommunication Engineering
Chhatrapati Shahu College of Engineering, Aurangabad, India

Abstract:

Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. 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

I. INTRODUCTION

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing" [1]. Steganography is one such pro-security innovation in which secret data is embedding a cover [2]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983 [3].Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an "invisible" message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. [4]There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it [5].

For instance, text steganography is believed to be the hardest type of steganography because of the low degree of redundancy in text as compared to image, audio or video. Redundancy can be described as the bits of a media, signal or file that offer accuracy more than needed for the object's use [6]. The redundant bits of an object may also be defined as those bits that can be easily altered without this change being noticed easily [7]. Image, video and audio files in particular fulfill this requirement, while studies have also revealed other file formats that are suitable to be used for information hiding. Figure 2 illustrates the main categories of file formats or signals that can be efficiently used for steganography.

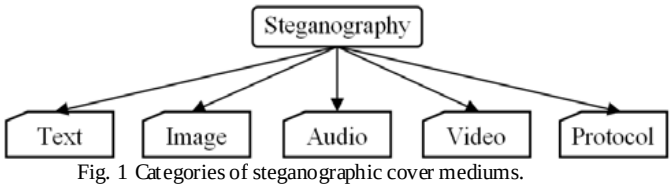

Fig. 1 Categories of steganographic cover mediums.

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 Echo Hiding: Echo hiding used to embeds secret data in a audio file by pass an echo into the discrete signal. This technique has advantages of providing a high data transmission rate and robustness when we make comparison of echo hiding to other methods. One bit of secret data could be encoded if one echo was produced from the original signal; before the encoding process starts the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal [17][18][19][20][21]

2.1.2 Phase Coding: Phase coding exploits HAS insensitivity to relative phase of different spectral components. In this method we can replace selected phase components from the original sound signal spectrum with hidden information .due to in audibility of information, phase components medication should be kept small. It is very effective coding methods in terms of the SNR ratio. When the phase relation between each frequency component is changed, phase dispersion will occur. The modification of the phase is sufficiently small (sufficiently small depends on the observer; professionals in broadcast radio can detect

modifications that are unperceivable to an average observer), an inaudible coding can be achieved.

2.1.3 Parity Coding: This technique is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, it breaks a signal into separate samples sections and embeds each bit of the secret message information from a parity bit. If the of a selected parity bit region does not match the secret message bit to be encoded, the process inverts the LSB of one of the section in the region. Then the sender has many choices for encoding the secret bit.

2.1.4 Spread Spectrum: In this technique spread out the encoded information across the available frequencies. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. This method spreads the secret data over the audio file frequency spectrum which using a code that is independent of the original signal. The final signal occupies a bandwidth in excess of what is actually required for transmission at end. The sampling is used in chip rate for the sound signal communication.

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.

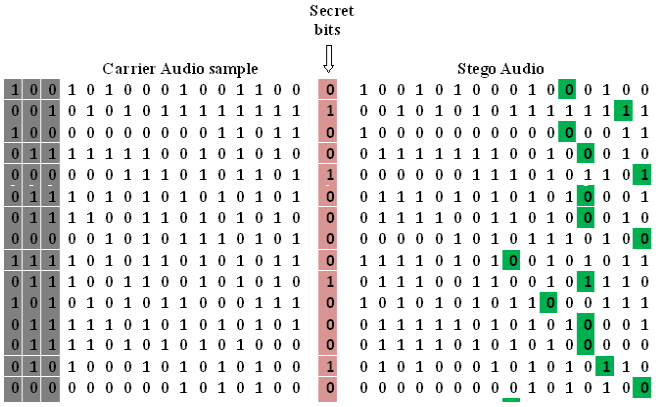

Fig 2. Bits of a secret Message are embedded in a 16-bit CD quality sample using the proposed method

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:

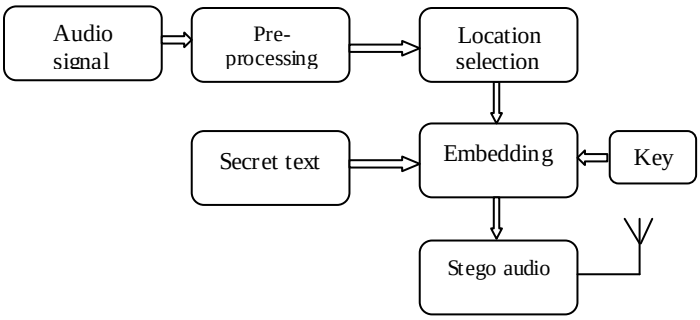

Fig3. Transmitter section

Receiver:

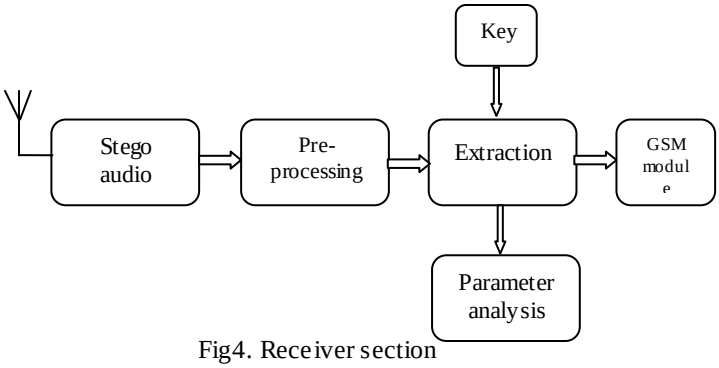

Fig4. Receiver section

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

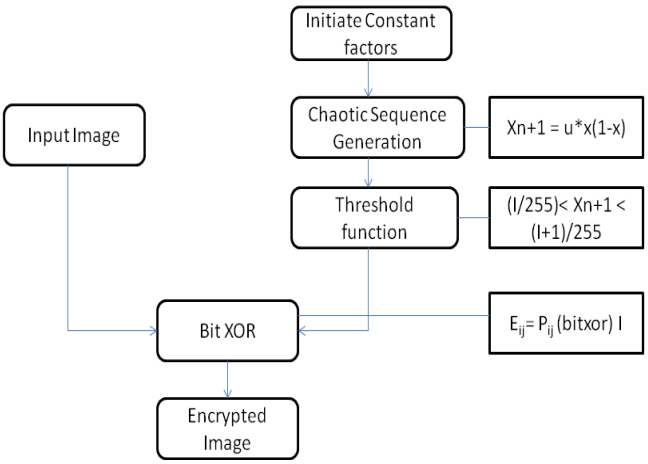

Fig5. Chaos algorithm

Step1. This method is one of the advanced encryption standard to encrypt the data for secure transmission.

Step2: It encrypts the original data ASCI values with encryption key value generated from chaotic sequence with threshold function by bitxor operation.

Step3: Here logistic map is used for generation of chaotic map sequence.

Step4: It is very useful to transmit the secret data through unsecure channel securely which prevents data hacking.

Step5: The chaotic systems are defined on a complex or real number space called as boundary continuous space.

Step6: Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression (Wei et al., 2006)

Step7: The properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity (Hermassi et al., 2010).

IV 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:

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

[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:

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

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)))];

V RESULTS

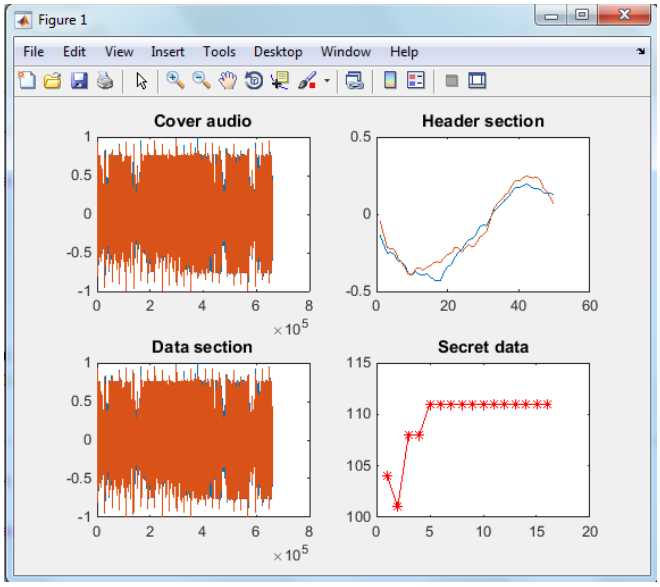

Fig6 a) Cover audio, b) Header section, c) Data section, d) Secret data in the form of ASCI value.

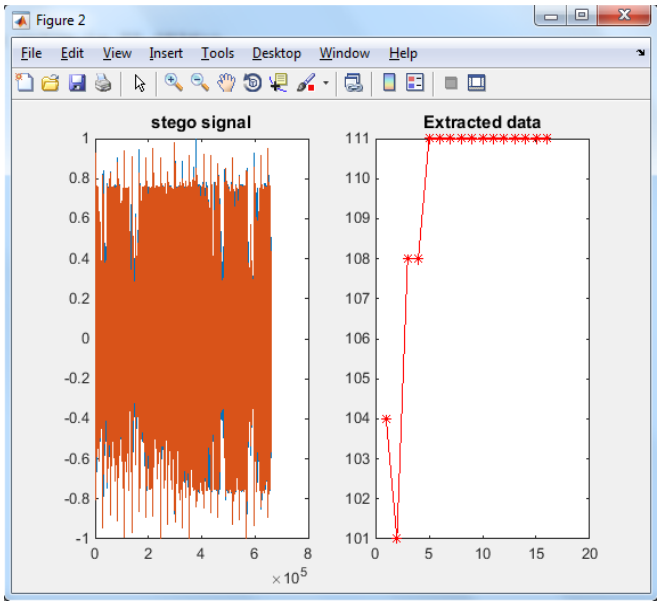

Fig7 a) Stego audio, b) Extracted data in the form of ASCI value.

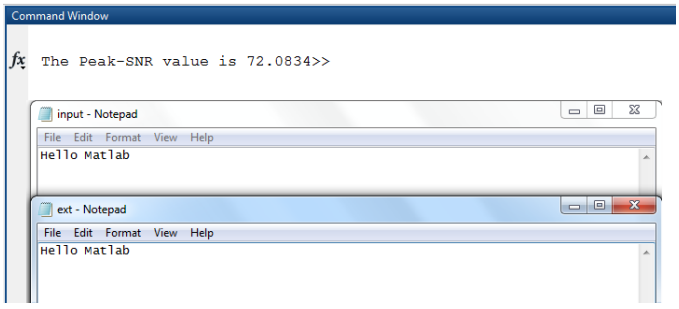

Fig8 a) PSNR calculation and (input & extracted secret data)

VI 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] Currie, D.L. and C.E. Irvine, 1996. Surmounting the effects of lossy compression on steganography. Proceedings of the 19th National Information Systems Security Conference, Oct. 22-25, Baltimore, Maryland, pp: 194-201

[7] Anderson, R.J. and F.A.P. Petitcolas, On the limits of steganography. Selected Areas in Communications, IEEE Journal on, 1998. 16(4): p. 474-481.

[8] Pfitzmann, B. (1996) (collected by): Information Hiding Terminology – Results of an informal plenary meeting and additional proposals; Information Hiding,

[9] M. Pooyan, A. Delforouzi, *"LSB-based Audio Steganography Method Based on Lifting WaveletTransform",* in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[10] Singh, Pradeep Kumar, Hitesh Singh, and Kriti Saroha. "*A survey on Steganography in Audio* ." National Conference on Computing for Nation Development, Indiacom. 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.