# Enhanced Audio Steganography using Cryptography and Randomised LSB Algorithm

Shamneed. M
Department of Electronics and Communication
B.S. Abdur Rahman University
Chennai, India

P. Maya
Department of Electronics and Communication
B.S. Abdur Rahman University
Chennai, India

***Abstract*— The need for secure data communication has greater importance in the world of communication. Cryptography and steganography are the modern ways of secure data transmission. The main objective of this paper is to develop a new tactics for cryptography and steganography. The proposed algorithms are used in a single process. Cryptography is a method of converting a message in to an unreadable format. Steganography is the process of hiding a data in a cover signal. The data can be a text message, image, audio or video. The cover signal can be a text message, image, audio or video. The main inspiration of steganography is to preserve the confidentiality of the message. The main exertion in cryptography is the message itself attracts the third party. By using steganography, the secrecy of message can be maintained. The development of steganalysis method makes the need for better and efficient Steganographic algorithm. The usage of cryptography and steganography makes the algorithm stronger. In this paper, the text message to be transmitted is encrypted by using an advanced version of vernam cryptography and this encrypted message is hidden in the audio cover signal by replacing the LSBs of randomly selected samples. The random selection of samples depends on the length of the message to be transmitted. This enhanced technique decreases the probability of detecting the secret message by an intruder. The proposed technique is implemented using a text message and a .wav audio file. The sampling frequency for audio is 8000 samples/second with each sample containing 8 bits.**

***Keywords—cryptography,steganography,vernam,encryption***

## I. Introduction

Usually for perceiving high confidential message cryptography is the method employed. No matter how unbreakable, the encrypted datas attract the attention of the third party. Cryptography is the process of converting the message in to an unreadable format, whereas steganography is the method of hiding a secret message in a cover file. Steganography is commonly used in the method of watermarking for copy right protection. The recent research shows that it can be used for secured data communication. The reason for using both cryptography and steganography is that, even if someone is able to extract the message from the cover file, the secret message cannot be decoded with proper cryptographic algorithm. The cryptographic algorithm developed here is based on vernam cipher method. The Steganographic algorithm used is an enhanced form of conventional LSB algorithm.

## II. System analysis

In this section the need for proposed system and the algorithm for proposed system are defined.

### A. *Need For Proposed System.*

Covered writing (steganography) is the process of secretly embedding information into a data source in such a way its very existence is concealed, a form of security through obscurity to establish secure invisible channels for covert communications. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves; evidently noticeable encrypted messages, no matter how resilient, will awaken distrust, and may in themselves being incriminating in countries where encryption is unlawful [3]. Therefore, while cryptography protects the contents of a message, steganography is said to protect both datas and transceiver clients. For hiding secret information in video, there exist a large variety of Steganographic techniques some are more complex than others and all of them have respective strong and weak points.

Steganography is an art of secret communication. It is a part of information hiding that focuses on hiding the existence of messages. The term hiding refers to the process of making the information unnoticeable or keeping the existence of the information secret. The steganography algorithm were primarily developed for digital images and video sequences. Later the attention in exploring audio steganography was started. Any steganography technique has to satisfy two basic requirements. The first necessity is perceptual transparency that is cover object (object containing any additional data) and stego object (object containing secret messages) must be perceptually indiscernible. The second requirement is high data rate of the embedded data [3]. In audio steganography the weakness of the human auditory system is used to hide information in the audio.

### B. *Proposed System Design.*

The proposed system works in an organized way. Figure 1 represents both the transmitter and the receiver side of the algorithm. The upper portion of the block diagram is the transmitter side and the lower portion is the receiver side. The secret message to be transmitted is first encrypted using the proposed cryptographic algorithm. This encrypted data is embedded in the audio signal using the proposed Steganographic algorithm. At the receiver side, the audio signal containing the secret message (stego signal) is received at the receiver. From this signal, the encrypted data is retrieved by applying the retrieval algorithm. For decryption the same cipher used for encryption is used and the secret message is retrieved.

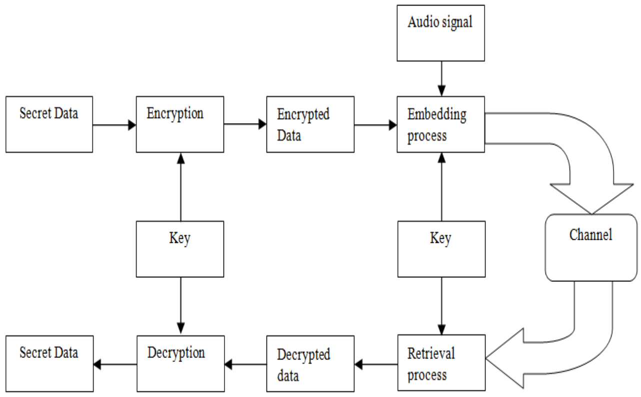

Fig.1. Proposed system block diagram.

## III. Advanced Vernam Cipher Mthod

The proposed cryptographic algorithm is named as advanced vernam cipher method. The conventional cipher method and advanced cipher are explained in detail below.

### A. *Conventional Vernom Cipher Method*

According to pro-technix, vernam cipher is considered as the most secure form of encryption ever programmed. The strength of cryptography is measured on the basis of mathematical computation. The conventional vernam cipher method was developed by an American scientist Gilbert Vernam, an engineer at bell labs during the First World War. The algorithm of conventional method is the message to be transmitted and the key generated is converted in to binary form. The message in binary form is bit wise XORed with key in binary form. The only condition is that the key generation should be random. The random key generation is possibly from certain hardwares like gathering and processing the output from Geiger counters or Zener diodes and it is possible to obtain truly random data.

TABLE I –
CONVENTIONAL VERNAM CIPHER

| **Secret message in binary form** | **Key in binary form** | **Output bit** |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

The table given (table.1) shows the bitwise XOR is performed in conventional vernam cipher method.

### B. *Advanced Vernam Cryptography*

The advanced vernam cryptography is developed using 4 modules. The entire encryption algorithm is described below.

Step 1: Enter the secret message to be encrypted.
Step 2: Enter the key.
Step 3: Use module-1 for the generation of pads.
Step 4: Use module-2 to perform bit manipulation of the input message.
Step 5: Use module-3 to perform bit wise XORing with the bit manipulated input message.
Step 6: Use module-4 to perform bit XOR method on the output of module-3.
The output of the module-4 is the encrypted message.

<u>Module-1:</u>
Step 1: Calculate the length of the key.
Step 2: Provide a condition,

```
if length<8
base=9-length
else, base=1
```

Step 3: Calculate the pad1 value using the equation

$$P1=\sum(base^{position}) * \text{ASCII value of character.}$$

Step 4: Calculate the sum of digits in P1 and store the result in P2.

<u>Module-2:</u>
Step 1: Convert the entire input file in to binary form.
Step 2: Extract 8 bits at a time from the input message.
Step 3: Reverse the 8 bits.
Step 4: Complement the reversed bits.
Step 5: Perform XOR operation between complemented bits, i.e. XOR bit 1 and bit 8, XOR bit 2 and bit 7, XOR bit 3 and bit 6, XOR bit 4 and bit 5 of the complemented bits.

<u>Module-3:</u>
Step 1: The pad P1 generated in module-1 is XORed with the module-2 output.
Step 2: The pad P2 is reversed and then XORed with the output of step1.

<u>Module-4:</u>
Step 1: Read the final output of module-3.
Step 2: Read 2 consecutive bits and perform XOR operation between the 2 bits.
Step 3: Store the result in 2nd position. Continue step1 to 3 till the end of the file.
Step 4: Create a loop, for i=1 to n
Read $i^{th}$ and $(i+2)^{th}$ bit, perform XOR. If ‘i’ is odd, store the result in i+2. Else store in ‘i’.
Step 5: Read 8 bits at a time. Interchange the bits as follows.

```
for i=1 to 4
interchange i and i+4
end
```

Step 6: Consider the entire message, interchange the bits as follows.

```
For i=1 to n (n=last position)
  Interchange bit 1 and n-1
```

Step 7: Reverse the entire bit pattern.

Decryption algorithm:

Step 1: Enter the key.
Step 2: Perform the module-1 operation for the generation of pads.
Step 3: Convert the file in to bits and then reverse the bits.
Step 4: Use module-4.
Step 5: Use the reverse process of module-3.
Step 6: Use module-2 operation.
Step 7: Convert the bits back to file. The resulting output is the decrypted message.

## IV. Randomized Steganographic LSB Algorithm.

The projected Steganographic algorithm is named as randomized LSB algorithm. The conventional LSB algorithm and the proposed algorithm are discussed in detail.

### *A. Conventional LSB Algorithm.*

The Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. The datas are hidden in the cover signal by replacing the LSB of each sample of the cover signal. Even if we are varying the LSB, it will not affect the characteristic of the sample and the audio signal. The reason is, the weight age of the LSB compared with the other bits in the sample is comparatively negligible [1]. It will introduce some noise, but the noise level should be kept below a threshold. The table below shows an example for conventional LSB technique.

TABLE II
LSB algorithm

| Audio samples | Message in binary form | Stego signal samples |
|---|---|---|
| 0100001**0** | **0** | 0100001**0** |
| 0100010**0** | **1** | 0100010**1** |
| 0100001**1** | **0** | 0100001**0** |
| 0010001**0** | **1** | 0010001**1** |
| 0100000**1** | **1** | 0100000**1** |
| 0110000**1** | **0** | 0110000**0** |
| 0110001**0** | **1** | 0110001**1** |
| 0101001**1** | **1** | 0101001**1** |

It is easy for the intruder to extract the message from the stego signal if the conventional LSB technique is used. Steganalysis method is developed for finding the existence of secret message in the LSB technique [2]. In order to overcome this issue, the proposed algorithm can be used to overcome the steganalysis algorithm.

### *B. Randomized Steganographic Algorithm.*

The proposed algorithm provides randomness in the selection of samples and the selection of LSBs from each sample based on the MSBs of each sample.

1. Methodology for selection of samples.

The audio signal is conceded through an ADC and it is sampled at a sampling frequency of 8000 samples/sec and each sample is of 8 bit. The algorithm for sample selection is mentioned below.

Step1: Calculate the length of the message.
Step2: If the length of the message is odd, from the first 10 samples, choose the even samples and in the next 10 samples choose the odd and so on for the LSB replacement.
Step3: If the length of the message is even, then extract 10 samples at a time, choose the odd samples and from the next 10, choose even samples and so on for LSB replacement.

So in an alternative way the samples are chosen based on the length of the message to be transmitted.

2. Methodology for LSB selection.

From the literature survey, it has been observed that replacing the first, second or third LSB of a sample doesn't produce any detectable change in characteristics of the signal [4]. The first 2 bits of a sample (MSBs) determine which LSB of the sample is replaced, i.e. if the MSB varies the bit to be replaced will also varies.

If the first 2 MSBs of a sample appear to 00, then 1st LSB of the sample is to be replaced. If the MSBs of the sample appear to be 01, then the 2nd LSB of the sample is replaced. If the LSB of the sample appears to be 10, then 3rd LSB of the sample is replaced. If the MSBs of the sample appear to be 11, then also the 3rd LSB is chosen for replacement. The LSBs to be replaced can be varied by the user. The main factor is providing randomness in the selection of LSB. Below is the tabular form of the LSB selection.

TABLE III
LSB selection

| 1st MSB of sample | 2nd MSB of the sample | LSB selected |
|---|---|---|
| 0 | 0 | 1st LSB |
| 0 | 1 | 2nd LSB |
| 1 | 0 | 3rd LSB |
| 1 | 1 | 3rd LSB |

## V. Results And Discussion

The proposed algorithm is implemented using MATLAB. The secret message to be transmitted is a text message. The cover signal is an audio file of .wav extension. In the simulation, the user can implement the option to either use an existing audio file or user can record an audio signal. The results for both the conventional LSB algorithm and proposed algorithm are shown below.

Case 1: conventional LSB algorithm

Secret message= **“engineering and technology”**

Audio file= .wav audio file

Fig.1. shows the original audio signal and the fig.2 shows the audio signal containing the secret message “engineering and technology”. The 2 signals are identical. But the steganalysis methods are developed for the conventional LSB technique, hence going for the proposed system.

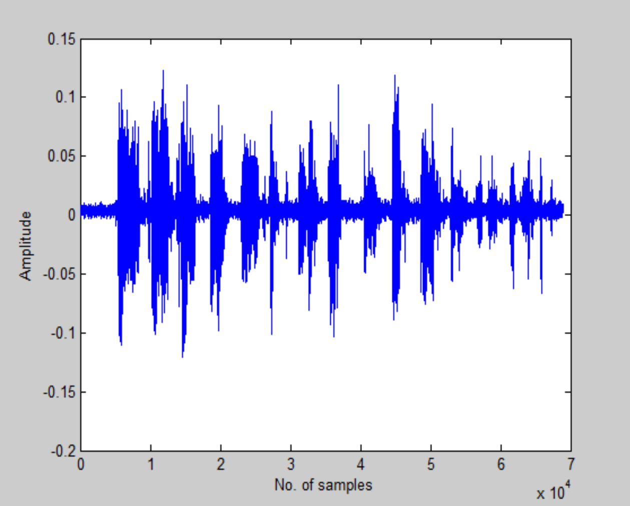

Fig.2. Original Audio File

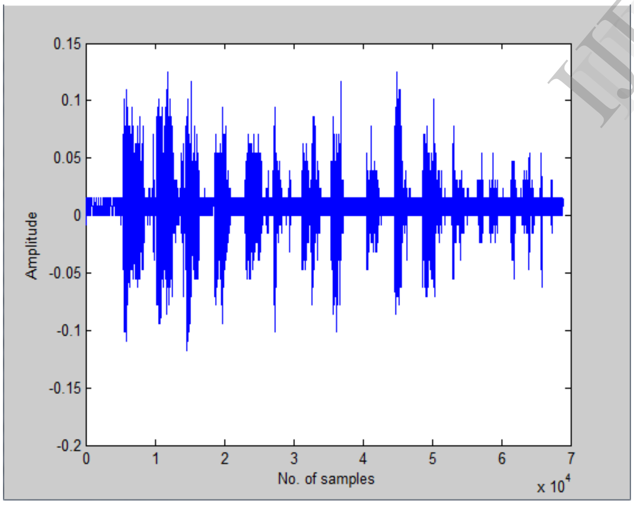

Fig.3. Stego Signal (Conventional LSB)

Case 2: proposed algorithm

Secret message= **“engineering and technology”**
Audio file= .wav audio file.

In the proposed algorithm, we use advanced vernam cryptography and randomized LSB algorithm. For encryption, we need to enter the key.

Key=**journal2014**

Secret message encrypted using advanced vernam cryptography is given as follows.

Encrypted data= **- OE3õ 1 3åÿó}åuã ! ÍO± ±ïx**

This encrypted data is embedded in the audio file using the randomized LSB algorithm. Fig.3. shows the original signal and fig.4 shows the stego signal containing encrypted data, embedded using randomized LSB algorithm.

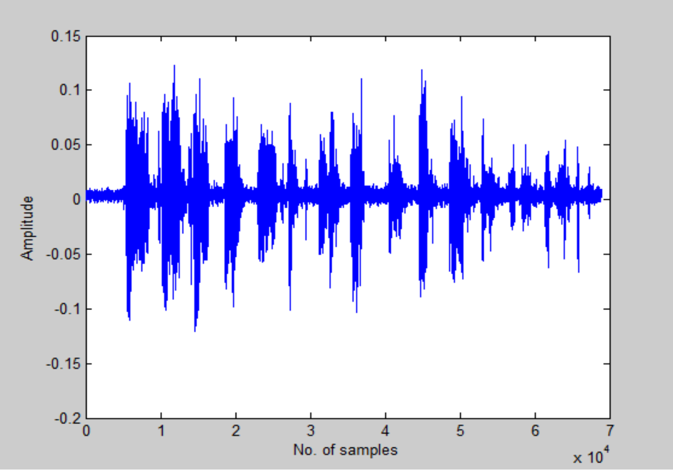

Fig.3. original audio file

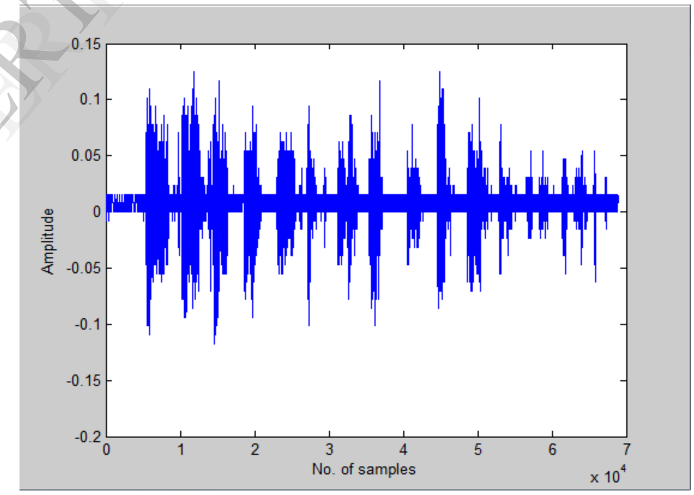

Fig.4. Stego Signal (Proposed Algorithm)

## VI. CONCLUSION

The aim of the project has been achieved in perspective manner with the available environment. The proposed system provides a well-organized method for hiding the data from hackers and sent to the destination in a safe manner. The existence of elitism to the steganography has been elevated by means of the project. The process of both cryptography and the steganography are procured in the MATLAB environment in a perpetual manner. Advanced vernam encryption and decryption technique have been used to make the security system robust. The randomized LSB algorithm used in steganography is secure against steganalysis. The method can be further improved by providing random key generation using certain hardwares like Geiger counters or Zener diodes.

## ACKNOWLEDGMENT

S.M thanks the almighty for giving potency for the completion of this work. S.M expresses his sincere gratitude to P.M for supporting throughout the project. S.M is grateful towards their parents and their friends for supporting them. S.M genuinely expresses his gratitude to Department of Electronics and communication, B.S. Abdur Rahman University for providing necessary help and assistance.

## REFERENCES

[1] Harish Kumar, Anuradha,“ Enhanced LSB technique forAudioSteganography”,2012

[2] S.R. Khosravirad, T. Eghlidos ,S. Ghaemmaghami, “Closure of sets: a statistically hypersensitive system for steganalysis of least significant bit embedding”,2012

[3] Cox, J. Miller, M.L Bloom, J.A Fridrich & Kalker T., “Digital Watermarking and Steganography”, Morgan Kaufmann Pub., Elsevier Inc., 2008.

[4] Muhammad Asad, Junaid Gilani, Adnan Khalid, “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”,2011

[5] S.J Chapman, “MATLAB Programming for Engineers”, Thomson, 2004.

[6] D.J Higham and N.J Higham, “MATLAB Guide”, Siam, second edition, 2005.

[7] K. Li, Y.C Soh, and Z. G Li, “Chaotic cryptosystem with high sensitivity to parameter mismatch”, IEEE Trans. Circuits Systems I, Fundamental Theory Applications, 2003.

[8] G. Manjunath and G.V Anand, “Speech encryption using circulant transformations,” Proc. IEEE Int. Conf. Multimedia and Expo, 2002.

[9] H.J Beker and F.C Piper, “Secure Speech Communications”, London, U.K Academic, 1985.

[10] K. Gopalan, “Audio Steganography using bit modification”, Proc. IEEE Int. Acoustics, Speech and Signal Processing Vol 2.

[11] F.A.P Petitcolas, R.J Anderson, and M.G Kuhn, “Information Hiding-A survey,” Proc. IEEE, 1999.

[12] R.J Anderson and F.A.P Petitcolas, “Hiding Techniques for steganaography and Digital Watermarking”, S. Katzenbeisser and F.A.P Petitcolas, Eds. Boston, MA: Artech House, 2000.

[13] D Gruhl. A. Lu, and W. Bender, “Echo hiding,” in Proc. Information Hiding Workshop, Cambridge, U.K., 1996.

[14] H.S Malvar, “A modulated complex lapped transform and its application to audio processing,” in Proc. Int. Conf. Acoust., Speech, Signal process., Phoenix, AZ, May 1999.

[15] K Brandenburg, “Coding of high quality digital audio,” in Applications of digital Signal Processing to Audio and Acoustics, M. Kahrs and K. Brandenburg, Eds. Boston, MA: Kluwer, 1998.