An Enhanced Least Significant Bit Modification Technique for Audio Steganography

Muhammad Asad, Junaid Gilani, Adnan Khalid
Telecommunication Engineering Department, University of Engineering and Technology Taxila
UET Taxila, Taxila-47050, Rawalpindi, Pakistan
muhammad.asad@gmail.com, gilaniuet@gmail.com, adnan_uet38@yahoo.com

***Abstract*— Increased use of electronic communication has given birth to new ways of transmitting information securely. Audio steganography is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography. The conventional LSB modification technique is vulnerable to steganalysis. This paper proposes two ways to improve the conventional LSB modification technique. The first way is to randomize bit number of host message used for embedding secret message while the second way is to randomize sample number containing next secret message bit. The improvised proposed technique works against steganalysis and decreases the probability of secret message being extracted by an intruder. Advanced Encryption Standard (AES) with 256 bits key length is used to secure secret message in case the steganography technique breaks. Proposed technique has been tested successfully on a .wav file at a sampling frequency of 8000 samples/second with each sample containing 8 bits.**

***Keywords*— Steganography, Audio Steganography, Steganalysis, LSB Modification Steganography, Information Security, Secret Information Transmission, AES-256**

I. INTRODUCTION

In this era of emerging technologies, electronic communication has become an integral and significant part of everyone's life because it is simpler, faster and more secure. With adoption of electronic communication on such a large scale, it has become necessary to devise ways to transmit information secretly. Steganography is the branch of science which deals with embedding secret message on the transmitter side and retrieving it successfully on the receiver side. Whether it is about copyright protection for piracy prevention or private personal communication, steganography is the emerging technique which would be the solution to such issues. Strictly speaking, steganography is not only authentication provider through watermarking but a door to confidential communication as well.

Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message.

Steganography is often mixed up with cryptography. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message [1].

Steganography can be applied to different type of media including text, audio and video. Audio and video files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy [2]. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and stego message after steganography remains same. However, audio steganography is considered more difficult than video steganography because the Human Auditory System (HAS) is more sensitive than Human Visual System (HVS) [3].

To perform audio steganography successfully, the adopted technique should work against HAS. For any audio steganography technique to be implementable, it needs to satisfy three conditions; capability, transparency and robustness [4]. Capability is the amount of secret information that can be embedded within the host message while transparency means how well the secret message is embedded in the stego message. Robustness of a technique indicates the ability of embedded secret message to withstand attacks.

Steganalysis is the process of detecting secret message hidden through steganography [5]. Two commonly used steganalysis techniques are auditory inspection and statistical analysis. In auditory inspection, one can detect the presence of secret message through HAS. In statistical analysis, the intruder compares the original host message and modified host message to extract the secret message.

The objective of this paper is to come up with a technique hiding the presence of secret message and working against steganalysis as well. For this purpose, the technique needs to satisfy transparency. Apart from this, capability is also a major concern because an efficient technique is one which can embed more secret information. To increase robustness, the steganography technique could be backed by an encryption scheme. However, encryption will decrease the capability.

978-1-61284-941-6/11/$26.00 ©2011 IEEE

Existing conventional LSB modification technique is briefed in Section II. Section III presents proposed methodology enhancing existing LSB modification technique to make it more secure against steganalysis. Experimental results of the proposed methodology and conclusion are presented in Section IV and Section V respectively.

II. Least Significant Bit Modification Technique

The LSB modification is one of the simplest audio steganography techniques providing high capacity. In this technique, data is being hidden in least significant bit(s) of audio samples. The weightage of LSBs in comparison with the combined weightage of whole sample is very small. However, changing the LSBs will induce some noise but as long as the noise induced is below detectable threshold, audio steganography is possible. Increasing the number of altered LSBs will induce more noise. If noise increases above the threshold and becomes detectable through any of the steganalysis methods, audio steganography technique fails. Using more LSBs per sample increases the capacity and decreases the transparency. On the other hand, using less LSBs per sample will decrease the capacity and increase the transparency. So, there is always a trade-off between both these parameters.

Fig. 1 shows block diagram of a LSB modification technique encoder. The host message in analog form is converted to digital form through analog-to-digital converter (ADC). The LSB(s) of host message samples are being modified to embed the secret message. The modified host message or stego message is passed through digital-to-analog converter (DAC) to produce analog stego message.

Fig. 2 shows block diagram of a decoder. The decoder passes analog stego message through ADC to obtain samples of the stego message. On the basis of encoding, decoding is performed where the bits from different samples are extracted to retrieve complete secret message.

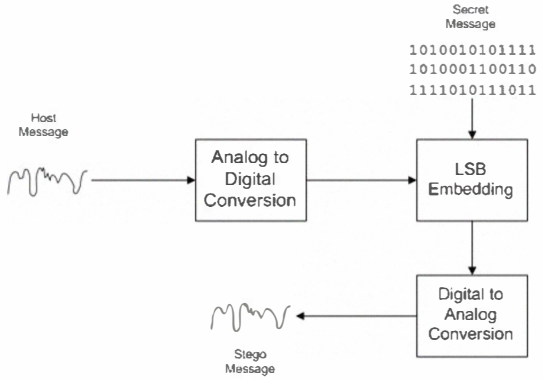

Fig. 1 LSB modification technique encoder

III. Methodology

The LSB modification technique is vulnerable to steganalysis. Secret message is being embedded in the LSB(s) of audio samples. Any intruder analyzing the samples of stego message could easily retrieve the secret message. In the proposed methodology called enhanced LSB modification technique, on the encoder side, the host message is being passed through an ADC where it is sampled at sampling frequency of 8000 samples/second with each sample containing 8 bits. Through experimentation presented in Section IV, it has been observed that modifying first, second or third LSB of a sample with secret message bit doesn't produce a detectable change or noise. On the basis of this analysis, two techniques named Bit Selection and Sample Selection to improvise the LSB modification technique are being proposed. Apart from this, the secret message is encrypted by AES-256 to make the relationship between plaintext and ciphertext more complex. Adding encryption will reduce the capacity but will increase the robustness.

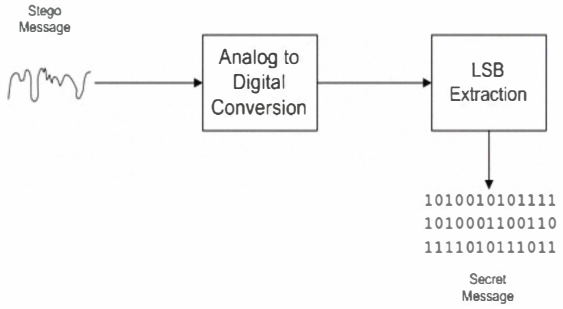

Fig. 2 LSB modification technique decoder

Fig. 3 shows the proposed methodology encoder where enhanced LSB embedding is being performed on the basis of Bit Selection and Sample Selection. Encryption is also being included. In case the steganography algorithm breaks, the use of encryption algorithm will make the encrypted secret message to be exposed to the intruder instead of the actual secret message. Fig. 4 shows the proposed methodology decoder which extracts the encrypted secret message. The encrypted secret message is then decrypted to obtain the actual secret message.

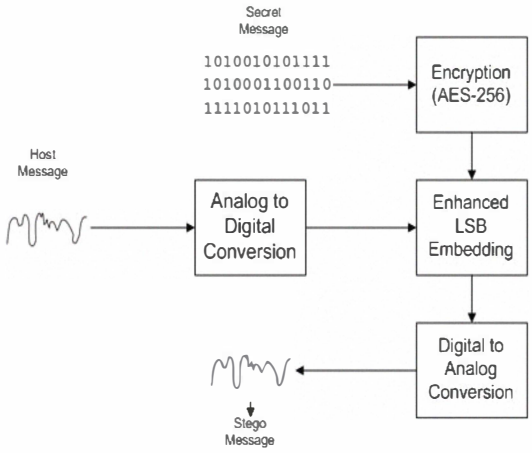

Fig. 3 Enhanced LSB modification technique encoder

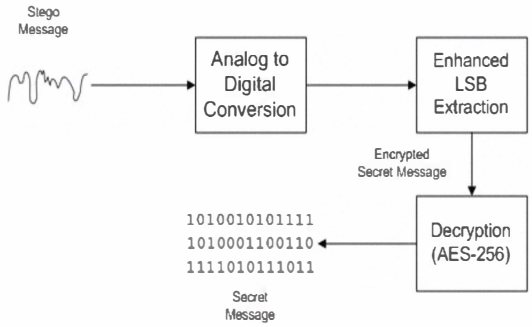

Fig. 4 Enhanced LSB modification technique decoder

A. Bit Selection

To confuse the intruder, same bit of a sample is never used to embed the secret message. Randomness is produced by selecting a different bit in every sample to hide secret message. First two Most Significant Bits (MSBs) of a sample will decide which bit of the same sample would contain the secret message bit. Table I shows a possible Bit Selection mapping. Different Bit Selection mappings can be designed but the secret message bit should always be embedded in first three LSBs of a sample.

If the first two MSBs of a sample are equal to 00, the third LSB will be replaced with secret message bit. If the first two MSBs are equal to 01, the second LSB will be replaced and if the first two MSBs are either 10 or 11, the first LSB will be replaced with the secret message bit.

TABLE I
BIT SELECTION MAPPING

1st MSB	2nd MSB	Secret Message Bit
0	0	3rd LSB
0	1	2nd LSB
1	0	1st LSB
1	1	1st LSB

B. Sample Selection

Another way to confuse the intruder is to add some more randomness in secret message embedding by using selective sample numbers to hide secret message. This means all the samples will not contain the secret message bit but a few. This randomness will be controlled by the first three MSBs. Table II shows a possible Sample Selection mapping. Different Sample Selection mappings can be designed but skipping more number of samples will decrease the capacity.

If i is the current sample, the last column of Table II indicates the next sample that will contain secret message bit. The number of samples skipped between two consecutive secret message bits is equal to one more than the decimal value of first three bits. If the first three MSBs of first sample (i = 1) in an audio signal are equal to 010, the last column indicates the next secret message bit to be embedded in sample number i + 3 = 4. This means the first bit of secret message will be embedded in first sample and the second bit of secret message will be embedded in fourth sample skipping the second and third samples. In the same way, if the first three MSBs of the fourth sample are equal to 011, the third secret message bit will then be embedded in the eighth sample.

TABLE II
SAMPLE SELECTION MAPPING

1st MSB	2nd MSB	3rd MSB	Sample Containing Next Secret Message Bit
0	0	0	i + 1
0	0	1	i + 2
0	1	0	i + 3
0	1	1	i + 4
1	0	0	i + 5
1	0	1	i + 6
1	1	0	i + 7
1	1	1	i + 8

IV. EXPERIMENTATION

To find the threshold after which the difference between host message and stego message becomes detectable, audio steganography is performed on fixed LSBs. Without using the randomness proposed in Bit Selection and Sample Selection, fixed bits of every sample of host message are replaced with secret message bits. The original host message is shown by Fig. 5. The resulting stego message after embedding secret message in third LSB, fourth LSB and eighth LSB are shown in Fig. 6, Fig.7 and Fig. 8 respectively. As there is no difference in Fig. 5 and Fig.6, changing of first three LSBs doesn't make any detectable change. Comparison of Fig. 5 with Fig. 7 shows a slight change between host message and stego message. Fig. 8 shows a stego message in which the eighth LSB of host message is being modified in every sample to contain the secret message. The shape of the stego message is completely changed in Fig. 8. Therefore, third LSB is considered threshold for the steganography technique. When the threshold is crossed and higher weightage LSBs are being modified, the difference becomes detectable.

Steganography is performed on the basis of proposed enhanced LSB modification technique. Initially, the secret message on the encoder side is encrypted using AES-256 making the relationship between plaintext and ciphertext much complex. A secret message "STARTMISSIONBETA" is encrypted to "-=ÇF=m¥¿8~3ââm→ À". For embedding this encrypted secret message, changing bits with higher weightage than the third LSB will result in a detectable change in the stego message. The proposed Bit Selection technique embeds secret message on first, second and third LSBs in selective samples according to proposed Sample Selection technique. In this way, the proposed technique satisfies the threshold condition and is more difficult for an intruder to break. The audibility of host message and stego message as well as the spectrum of both these messages are not differentiable. Fig. 9 shows audio steganography performed on the basis of proposed technique. Fig. 5 and Fig. 9 are not differentiable.

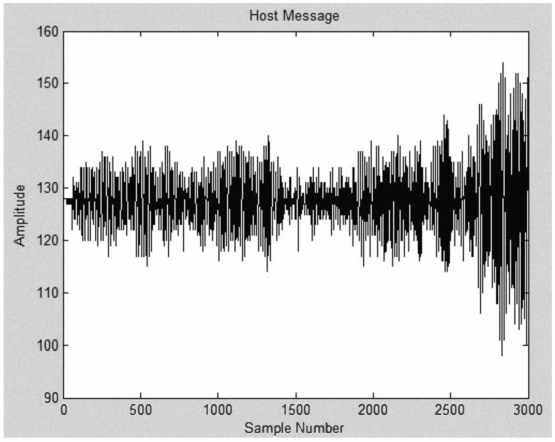

Fig. 5 Original host message

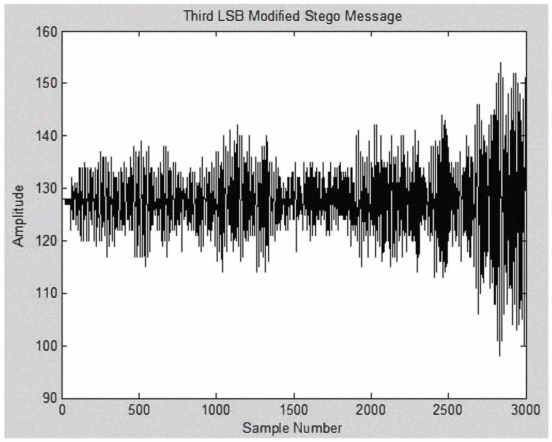

Fig. 6 Third LSB modified stego message

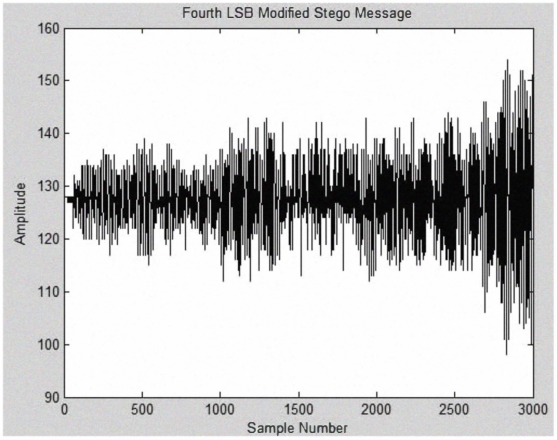

Fig. 7 Fourth LSB modified stego message

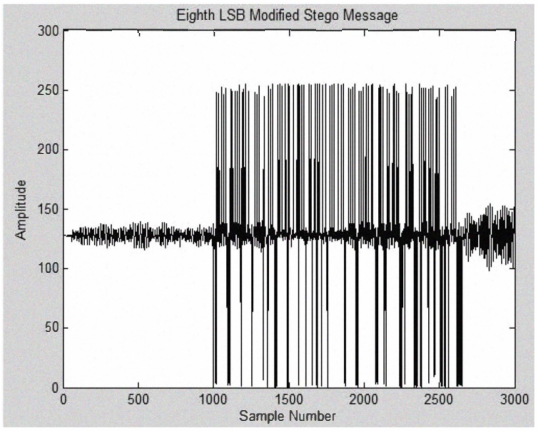

Fig. 8 Eighth LSB modified stego message

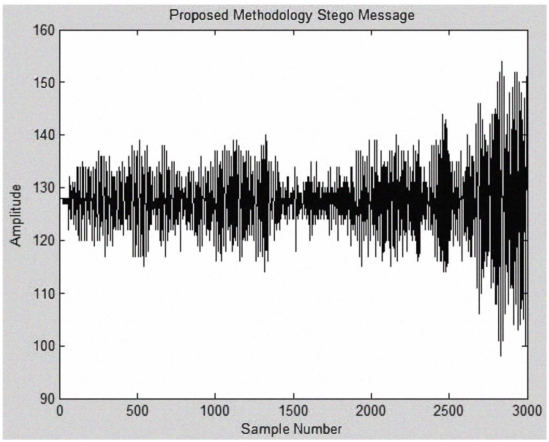

Fig. 9 Proposed methodology stego message

V. CONCLUSION

This research paper has extended the conventional LSB modification technique for audio steganography to make it more secure against steganalysis. On average, the technique embeds one secret message bit per four samples of host message. The maximum embedding rate is one secret message bit per sample of host message while minimum embedding rate is one secret message bit per eight samples of host message. In order to make sure the secret message is completely embedded, the samples of host message should be eight times the number of bits of secret message.

Samples of Host Message = 8 * Bits of Secret Message (1)

The stego message formed on the basis of proposed methodology cannot be differentiated from host message. The secret message on the receiver side can be extracted from the stego message as well.

ACKNOWLEDGMENT

We would like to say ALHAMDULILLAH for giving us the strength to work on this subject and coming up with this research paper. We are grateful to our families for supporting us and praying for us. We would like to show our gratitude to Engr. Hassan Bhatti for his direction, assistance and guidance. Special thanks to Centre of Excellence for ASIC Design and DSP, UET Taxila for providing all the required software/hardware.

REFERENCES

[1] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009, Page(s): 1 - 5.

[2] Andreas Westfeld, "Steganography and Multilateral Security", pp. 223–232 in Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications Bd. 3: Technology, Infrastructure, Economy. Addison-Wesley-Longman, München 1999.

[3] Gopalan, K., "Audio steganography using bit modification", 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.

[4] Zamani, M., Manaf, A., Ahmad, R.B., Jaryani, F., Taherdoost, H., Zeki, A.M., "A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009, Page(s): 1 – 6.

[5] Yali Liu, Ken Chiang, Cherita Corbett, Rennie Archibald, Biswanath Mukherjee, Dipak Ghosal, "Novel Audio Steganalysis Based on High-Order Statistics of a Distortion Measure with Hausdorff Distance", ISC '08 Proceedings of the 11th international conference on Information Security.