ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Secured Communication Using Audio Cover and Encryption

Athira M Joshy[1], Priyanka Udayabhanu[2]

PG Student [Comm.Engg.], Dept. of ECE, SNGCE, Kolenchery, MG University, Kottayam, Kerala, India[1]

Assistant professor, Dept. of ECE, SNGCE, Kolenchery, MG University, Kottayam, Kerala, India[2]

ABSTRACT: Audio steganography is the method of hiding secret information in an audio file. The audio file in which the secret information is hidden is known as audio cover. The sender embeds the secret message in the audio cover file using a key to produce a stego-file. At the receiver end, the receiver processes the received stego-file and extract the hidden message. In this paper a three layer audio steganographic approach is done for efficient data hiding and another algorithm is also proposed for hiding image in audio file.

KEYWORDS: Audio cover, Stego-file, Bit selection mapping, Sample selection mapping.

I. INTRODUCTION

Information security is becoming very important part of our life now-a-days. Information hiding is the fundamental of information security. Information hiding can be achieved by steganography as well. Embedding secret messages into digital sound is known as audio Steganography. It is usually a more difficult process than embedding messages in other media.

Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. The properties of the human auditory system (HAS) are exploited in the process of audio Steganography. Auditory perception is based on the critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane. The power spectra of the received sounds are not represented on a linear frequency scale but on limited frequency bands called critical bands.

Digital audio is discrete rather than continuous signal as found in analog audio. A discrete signal is created by sampling a continuous analog signal at a specified rate. Forexample, the standard sampling rate for CD digital audio isabout 44 kHz . Digital audio is stored in a computer as a sequence of 0's and 1's. With the right tools, it is possible to change the individual bits that make up a digital audio file. Such precise control allows changes to be made to the binary sequence that are not discernible to the human ear.

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password.Carrier is also known as a cover-file, which conceals the secret information.Basically, the model for steganography. Message is the data that the senderwishes to remain it confidential. Message can be plain text, image, audio or any type of file.Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

II. RELATED WORK

K Gopalan proposed a paper [1] which describes a method of hiding information in a cover audio or image by modifying the spectrum of the signal at an arbitrary pair of frequencies has been described. The proposed method is simple and fast to implement. Although no perceptually masked frequencies have been used in the audio or the image, low levels of spectral change contribute to little or no discernibility of embedding. The key for embedding and retrieval can be made stronger with the use of different pairs of frequencies for each frame. The key can be further strengthened if some or all frequency pairs are obtained from audibly masked frequencies. Use of asked frequencies, additionally, will reduce perceptibility of embedding.With high payload and potential for imperceptible embedding and data robustness under adverse conditions,The technique can be extended to video embedding for video indexing, watermarking and authentication applications.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

k Gopalan's audio steganography using bit modification [2] discuss about LSB coding in steganography .Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. Among many different data hiding techniques proposed to embed secret message within audio file, the LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise free environments, which merely embeds secret message-bits in a subset of the LSB planes of the audio stream.This method provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This system will not change the size of the file even after encoding and also suitable for any type of audio file format.

Muhammad Asad [4] proposed a paper on "An enhanced least significant bit modification technique for audio steganography"and suggested about enhanced LSB modification technique which is different from conventional LSB modification technique. The enhanced steganography technique proposes two simple and easy ways against steganalysis; bit selection and sample selection. Due to bit selection and sample selection techniques, Layer 3 results in an increased transparency and robustness with a decreased capacity. As the main focus of this paper is confidentiality of the secret message, a compromise could be made to achieve higher transparency and robustness against lower capacity. Today, this trade-off seems reasonable because lower capacities can be overcome with advanced broadband networks, however, these networks don't help much to increase robustness or transparency.Bit Selection is a way to confuse the intruder by changing the secret message bit in every sample. Sample selection is another way to confuse the intruder by randomly selecting samples that will contain the secret message bits.

K Gopalan in [7] presented some results of a study on the conflicting requirements of payload, perceptibility and data robustness in bit modification audio steganography. The study demonstrated the capability of the technique for hiding a potentially large payload of data with robustness using high bit indices for embedding. A tradeoff between noise tolerance and payload,both of which depend on higher bit indices, is needed for a reasonably imperceptible embedding.

Masahiro Wakiyama[8] describes an audio steganography using low bits coding. This approach is to replace the data of lower bit in a cover audio data by a secret data.In this paper, the author explains two kinds of new methods by low bit coding.We used wave file as an audio data. The wave file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. This paper used 8 bits mono audio data. The secret data is a written text file.

III . PROPOSED ALGORITHM

A. LAYER 1:CHARACTER ENCODING

Character encoding is used to map characters to bits and bits to characters in the reverse operation. On the sender side,the secret message is in the form of characters. These characters have to be mapped to bits before they are embedded in a cover message.

A possible scheme to achieve both custom and compressed encoding is Huffman coding. A Huffman character encoder assigns smaller length code words (in bits) to more probable symbols and vice versa. Huffman coding is a lossless coding scheme with an efficient compression ratio. A codeword is assigned to all possible characters that can occur in the secret message.

B. LAYER 2: ENCRYPTION

Although a steganography technique is meant to withstand any steganalysis attack, if a technique breaks, the secret message becomes visible to the intruder, compromising privacy. An additional layer of encryption will increase the robustness and ensure that if an intruder is successful in steganalysis, the secret message is still protected.

Before the selection of an encryption scheme, one must make sure that the encryption scheme is not vulnerable to attacks. One such scheme is the Advanced Encryption Standard (AES) which has three possible key size choices; 128 bits, 192 bits and 256 bits. AES with the smallest key size of 128 bits is still un-breakable. The key size can decrease capacity, but if the secret message bits are large, key size becomes negligible.

The technique adopted for the process of encryption is the Advanced Encryption Standard (AES) with a maximum possible key size of 256 bits. Since, the AES algorithm is still unbreakable, it is impossible for the secret message to be leaked if it's transmitted in encrypted form. In AES-256, the plain text block and the cipher text block always have a length of 128 bits while the key length is 256 bits with the number ofrounds being 14. Since the plain text for applying

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

AES-256 should have a length equal to any multiple of 128 bits and secret message bits might not be a multiple of 128. Zeros are concatenated at the end of secret message bits to make its length a multiple of 128.

C. LAYER 3 :ENHANCED STEGANOGRAPHY

The conventional LSB modification technique for audio steganography is quite vulnerable to steganalysis. It simply embeds the secret message bits in fixed LSBs and any intruder who detects bit modification pattern, can retrieve the entire secret message.In an 8 bits sample of a cover message, the weight of the last three LSBs is much smaller than the other bits. Changing the first, second or third LSB of any sample of the cover message doesn't result in a detectable change, but the fourth LSB change becomes. Therefore, one or multiple bits from three LSBs can be used to embed a secret message.Conventionally, one way is to select one of the three LSBs of each sample and embed the secret message. Another way is to use all two or three LSBs to hide the secret message which will reduce the samples of the cover message. Both of these techniques are quite vulnerable to steganalysis.
The enhanced steganography technique proposes two simple and easy ways against steganalysis; bit election and sample selection. Due to bit selection and sample selection techniques, Layer 3 results in an increased transparency and robustness with a decreased capacity. As the main focus of this paper is confidentiality of the secret message, a compromise could be made to achieve higher transparency and robustness against lower capacity. Today, this trade-off seems reasonable because lower capacities can be overcome with advanced broadband networks, however, these networks don't help much to increase robustness or transparency.
Layer 3 deals with both the secret message and the cover message. After layer 2, the encrypted and compressed secret message in the form of bits is available. The secret message is now ready to be embedded.A cover message can be either an audio voice recording or any audio file selected from a hard disk. The audio file is passed through an Analog-to-Digital Converter (ADC) at a sampling rate of 8000 samples/second with each sample containing 8 bits.

The proposed scheme uses an image file as the secret data to be hidden in the audio file taken as cover object because the size of the image is generally quite small compared to the size of the audio file in which it must be hidden Captions should be Times New Roman 9-point bold. They should be numbered, please note that the word for Table and Figure are spelled out. Figure's captions should be centered beneath the image or picture, and Table captions should be centered above the table body. In order to hide secret information in the form of gray scale image file, we use cover file i.e. 16 bit CD quality wave audio file at 44.1 kHz which have best quality of sound characteristics. The proposed method is based on the basic design principle for hiding secret data in audio.to the proposed method, least significant bits up to three LSB positions are used as a stego-key to encode the image bits in stego-object. Thus, the image data can be embedded according to the following embedding algorithm.

D. *EMBEDDING ALGORITHM*

1. Input the gray scale image that is to be embedded and convert it into binary form.
2. Read the cover audio file. Leave the header of the audio file untouched.
3. Start with the first audio data sample and first bit of the image.
4. Do the following:

a. Compare the image bit to be embedded with the audio sample's 1st MSB to 7th MSB position till the first match is found.
b. If any MSB (from position 1 to 7) of audio sample matches with the image bit, replace the three LSBs of the audio sample with the binary equivalent of the MSB position (where match is found) else,
c. Insert all 0s into the three LSBs of the audio sample(indicating that this sample does not contain an image bit embedded into it.. Move to the next audio sample.

5. Repeat steps 4a - 4d till the match for the image bit is found in some MSB (from position 1 to 7) of an audio sample.
6. Move to the next image bit.
7. Repeat steps 4 - 6 till all the image bits are successfully hidden into the audio file.
8. Write the wave audio file with stego-key that contains number of samples used to embed secret image in the audio file and number of rows/columns in the image.
9. Output wave audio file is the stego-object.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

E. EXTRACTING ALGORITHM

The data extraction at the receiver's end follows the same logic asthe embedding algorithm.
1. Read the stego-object i.e. Cover audio after encoding.
2. Extract the stego-key from the stego-object that contains information about the number of samples used to embed the image in the audio and number of rows/columns in the image.
3. Do the following:
a. Select the audio samples one by one and extract the image bits from the MSB position of the audio samples with respect to the decimal equivalent of the value at three LSB positions.
b. If the value at three LSB positions is all 0s, move to next sample.
4. Repeat steps 3a – 3b till all the samples used to embed the image bits are used.
5. Store the image bits retrieved from the audio file into an array.
6. Divide the array into number of rows and columns and create the secret image.
7. Display the secret image.

IV. SIMULATION RESULTS

Simulation is done using MATLAB.Initially user is asked to enter the secret data.Secret data is entered as text in the base program. This text data is encoded using Huffman encoding.Huffman encoding is done to map characters into bits.More compression can be achieved as more frequently occurring characters are assigned smaller length code words.Encoding is done using Huffman dictionary.

After performing Huffman encoding,the Huffman encoded output is subjected to RC4 encryption.RC4 encryption is done to ensure more confidentiality.After RC4 ,AES encryption is also done.This is to make the data less prone to steganalysis. In the third layer enhanced steganography is done using bit selection mapping and sample selection mapping.The two algorithms can be changed according to the user. After AES encryption, the encrypted data is passed to the receiver side.On the receiver side the steps are done in the reverse order.

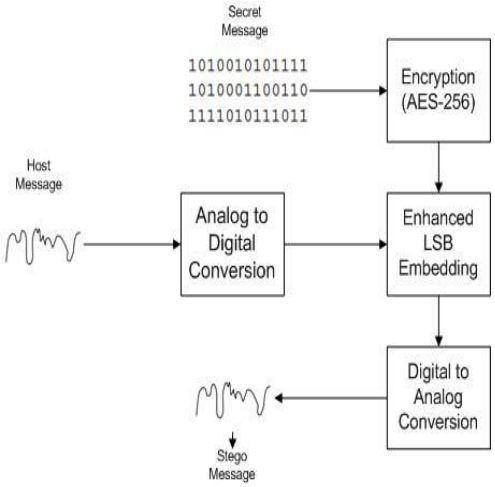

Fig 1. Enhanced Steganography Encoder

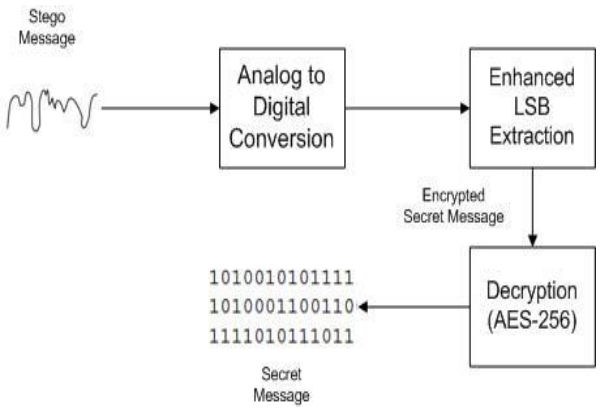

Fig 2. Enhanced Steganography Decoder

Fig 1 shows the enhanced steganography encoder which firsts converts the host message into digital form and then passes to enhanced LSB embedding unit where the AES encrypted data is also given .Processing is done in this unit and then passed to DAC unit which produces the stego output.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Fig 2 shows the enhanced steganography decoder where the stego message is given as input and it is passed to ADC then it is passed to enhanced LSB extracting unit which gives the encrypted secret message as output then it will undergo AES decryption then the secret message is extracted.

Bit Selection is a way to confuse the intruder by changing the secret message bit in every sample. In an 8 bits sample, only 1 bit of the secret message is embedded. Since any of the three LSBs can be used to contain a secret message bit, every sample has a secret message bit on a different LSB. The LSB selection can be done in many different ways. One possible way without any overhead of a key is to use first two Most Significant Bits (MSBs) of the same sample.

Sample selection is another way to confuse the intruder by randomly selecting samples that will contain the secret message bits. This means not all consecutive samples of the cover message will contain the secret message bits. There are a number of ways one can achieve this goal, for example, a table with different values indicating the sample numbers that will contain the secret message bits, but this requires maintaining a table and transmitting it to the other end as well. A simple solution to this problem lies again in the MSBs of the same sample. Assume the first secret message bit is embedded in sample i, the next sample containing the second secret message bit depends on the first three MSBs of sample i. The last column of Table II indicates the next sample where the next secret message bit will be embedded. For example, if the first three MSBs are 011, then the next sample containing the secret message bit will be i+4. The solution is very simple and neither requires a key nor the transmission of any table to the receiver.

1st MSB	**2nd MSB**	**Secret message bit**
0	0	3rd LSB
0	1	2nd LSB
1	0	1st LSB
1	1	1st LSB

Table I: Bit selection mapping

1st MSB	**2nd MSB**	**3rd MSB**	**Sample containing next secret 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

Table II: Sample selection mapping

Table I represents bit selection mapping .1st MSB and 2nd MSB of the sample is chosen and according to the table the secret message is embedded.The next sample which contains the secret data is determined by sample selection mapping.According to the 1st ,2nd and 3rd MSB of the current sample the next sample in which the secret message is embedded is determined from the Table II.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

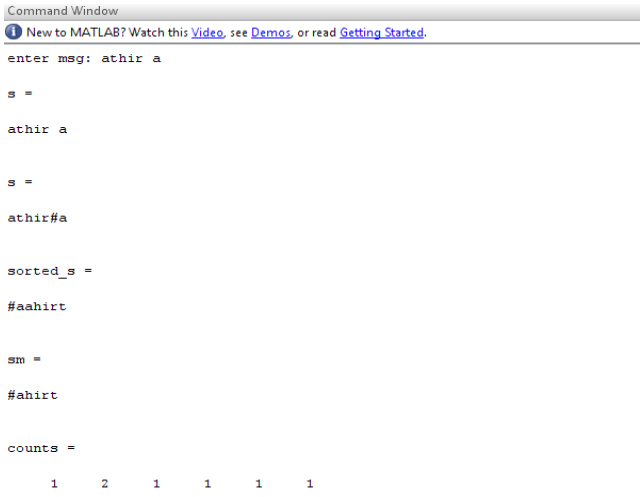

Fig 3. Secret Data

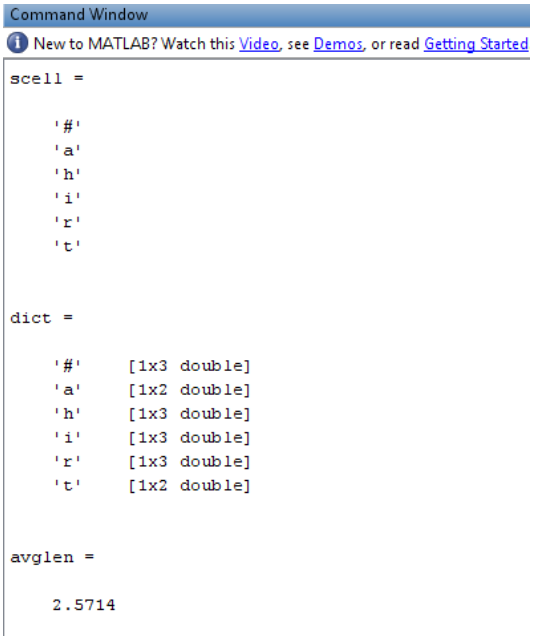

Fig 4. Huffman Dictionary

Fig 3 shows the secret message to be embedded and Fig 4 shows the Huffman dictionary for the secret message.

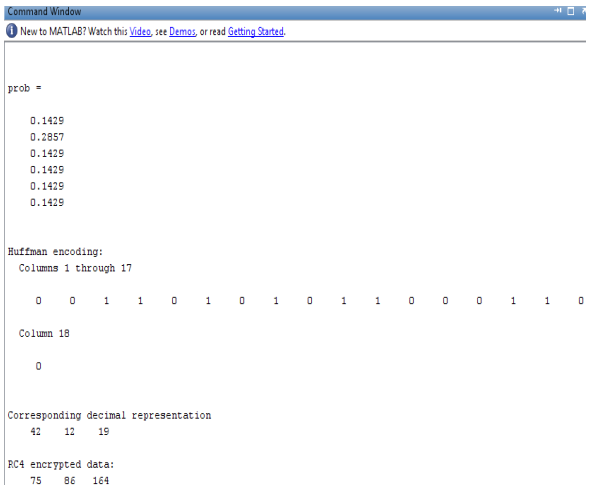

Fig 5. RC4 Encryption

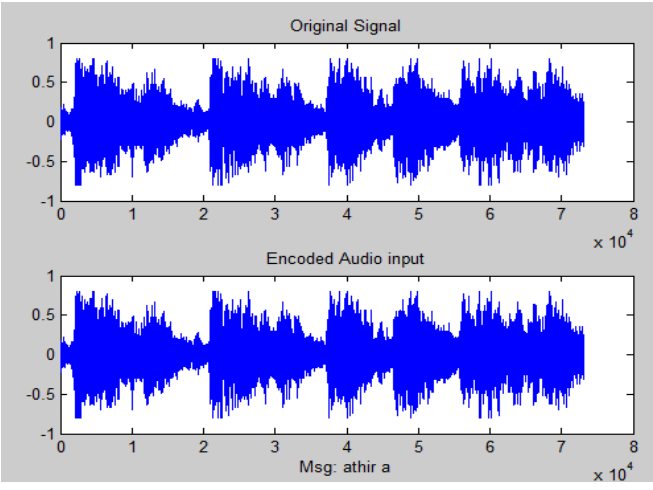

Fig 6. Secret message hidden in audio cover

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Fig 5 shows RC4 encryption which is performed on Huffman encoded data.Fig 6 shows the secret message embedded in the audio cover and the orginal audio signal.There is no notable difference between them.

For the enhancement section an image is used as the secret data. The proposed method is based on the basic design principle for hiding secret data in audio.According to the proposed method, least significant bits up to three LSB positions are used as a stego-key to encode the image bits in stego-object. Thus, the image data can be embedded according to the embedding algorithm and retreived using the retrieving algorithm. Fig.7 shows the image file which is used as the secret image.Fig 8. shows the orginal signal and the signal in which secret image is embedded.Both signals look alike.

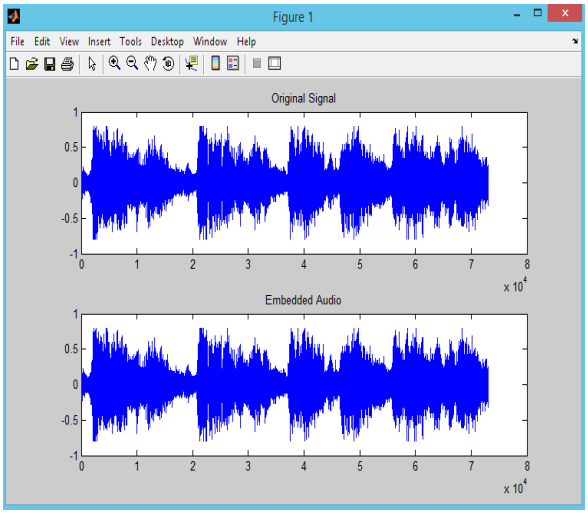

Fig 7. Orginal Signal and Encoded Audio Output

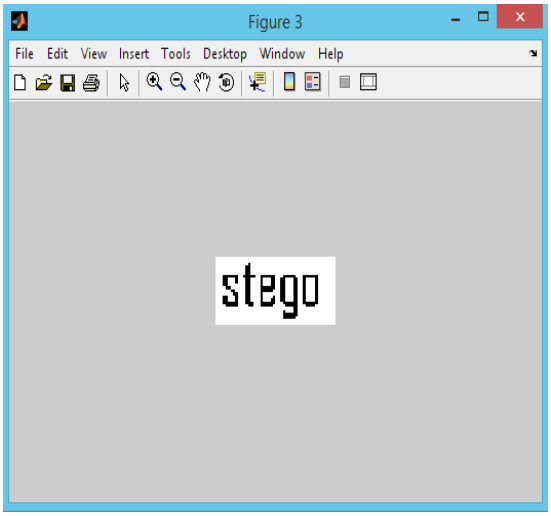

Fig 8. Secret Image

Fig 7 shows the orginal signal and the encoded audio output.Fig 8 is the secret message which is embedded in the audio signal.

V. CONCLUSION AND FUTURE WORK

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. ill order to make sure the secret message is completely embedded, the samples of host message shouldbe eight times the number of bits of secret message.Samples of Host Message== 8 * Bits of Secret Message. 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.

The conventional LSB modification techniques used are prone to steganalysis. A new three layered model for audio steganography is presented in this paper. On the sender side,the first layer maps characters of the secret message to bits.The compression provided by this layer increases capacity. The second layer applies encryption to secret message bits, thus changing representation of the secret message. The change in representation increases robustness, but the transmission of key decreases capacity. However, the decrease in capacity becomes negligible for longer secret messages. The third layer samples the cover message, embeds the secret message in it and transmits the resultant stego message over the network to the receiver. The third layer increases transparency and robustness,but decreases capacity which can be easily overcome by advance broadband networks. The receiver retrieves the stego message from the network and passes it through all three layers but in reverse order with each layer performing reverse operations. At the end, the same secret message is available to the receiver.

A new method of embedding an image data into the host audio file using LSB based audio Steganography has been successfully developed and implemented as discussed in this paper. Proposed method is found to be better than the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

3LSB and4LSB insertion methods.The main aim of this research work was embedding of image into audio as a case of audio steganography. In test cases, the image data has been successfully embedded and extracted from the audio file.

Future research direction is to explore the possibilities of improvements in audio steganograhy system with respect to each technique of data hiding in audio. One of the areas is to enhance the storage capacity of the system. This focuses on improving the maximum capacity of the audio signal to carry hidden data into it and making it robust to steganalysis. Further, the methods can be improved by applying mixed approaches, making the system more secure towards detection by using the combination of various techniques of data hiding in audio signals.

REFERENCES

[1] KaliappanGopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, Page(s): 1 – 5,2009
[2] KaliappanGopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, Page(s): 1 – 5,2009
[3] KaliappanGopalan., "Audio steganography using bit modification", IEEE International Conference on Acoustics, Speech, and Signal Processing,vol-2, Page(s): II - 421-4,2003
[4] MazdakZamani, "A secure Audio Steganography Approach",InternationalConference for Internet Technology and Secured Transactions ,Page(s): 1 – 6,2009
[5] Muhammad Asad, JunaidGilani, Adnan Khalid, "An enhanced least significant bit modification technique for audio steganography", International Conference on Computer Networks and Information Technology, Pages: 143 – 147,2011
[6] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu,"Techniques for Data Hiding", IBM Systems Journal, Volume: 35,Pages: 313 - 336,2011
[7] Avi Kak, "Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on Computer and Network Security", May 1, 2015. 8 Kriti Saroha , Pradeep Kumar Singh "A Variant of LSB Steganography for Hiding Images inAudio" International Journal of Computer Applications ,Volume 11– No.6, December 2010
[8] Nedeljko Cvejic, TapioSeppanen, "Increasing the capacity of LSBbased audio steganography", IEEE Workshop on Multimedia Signal Processing, Pages: 336 – 338,2002
[9] KaliappanGopalan, Qidong Shi, "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", 19th International Conference on Computer Communications and Networks, Pages: 1 – 6,2011
[10] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, "An audio steganography by a low-bit coding method with wave files", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pages: 530 – 533,2010
[11] Krishna Bhowal, AnindyaJyoti Pal, Geetam S. Tomar, P. P. Sarkar, "Audio Steganography using GA", International Conference on Computational Intelligence and Communication Networks, Pages: 449 -453,2010
[12] Nede Gko Cvejic, Tapio Seppanen, "A wavelet domain LSB insertion algorithm for high capacity audio steganography", IEEE 10thDigital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop, Pages: 53 – 55,2002.
[13] Muhammad Asad, "Text Steganography Using Huffman Coding",International Conference on Intelligent and Information Technology, Volume: 1, Pages: 445 – 447,2010

BIOGRAPHY

Athira M Joshyreceived B.Tech degree in Electronics and Communication Engineering from SNMIMT, underMahatma Gandhi University, Kerala, India in 2013. Currently pursuing M.Tech in Communication Engineering from SNGCE, under Mahatma Gandhi University, Kottayam, Kerala, India. Her area of interest is Steganography, Cryptography and Image Processing.

Priyanka Udayabhanu, is an Assistant Professor in the Department of Electronics and Communication Engineering, SNGCE. Secured M.Tech in Computer Vision and Image Processing from Amrita School of Engineering, Coimbatoreand B.Tech in ECE from Caarmel Engineering College, under Mahatma Gandhi University, Kottayam. Working areas includes Image Processing, and Watermarking.