International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

STEGNOGRAPHIC PROPERTIES BASED DATA HIDDEN IN MEDIA ELEMENTS USING CRYPTOGRAPHY

[1]Vandana Bhatia, [2]Kuldeep Kumar

[1.2]Department of computer Science, CDLU (Sirsa), (INDIA)

ABSTRACT

Steganography helps in communication of secured data in several carries like images, videos and audio. The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography and steganography can be combined. This paper proposes a secure communication system. It employs cryptographic algorithm together with steganography. The joining of these techniques provides a robust and strong communication system that able to withstand against attackers. In this paper, we have presented an Media Steganography concept for hiding the information in audio. The Storage of secret information is a constant security concern, and the reliability and integrity of this information is important. The proposed work will compute cipher text of message using cryptography algorithm, then LSB technique will hide the information in audio file. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR). The simulation results show that, the proposed system provides high level of security.

Keywords: *Audio Steganography, Cryptography, LSB, , PSNR, Steganography.*

I. INTRODUCTION

Steganography is a technique to embed the data in the content like images, audio and videos etc. by means of providing security to the data which has been sent over the internet or mail. The word steganography has its own meaning i.e. hidden writing. The word ―Steganography‖ is formed by the two Greek words that are ―Stegos means Hidden or Covered‖ and ―Grafia means writing‖. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by

Simmons in 1983. [**1**].We can use steganography over the cryptography, these are very closely related to each other. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message. 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. 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. There are many types of

steganography methods. In this paper, we are going to take a short look at different steganography methods. [1]. Fig. below shows the different steganography approaches.

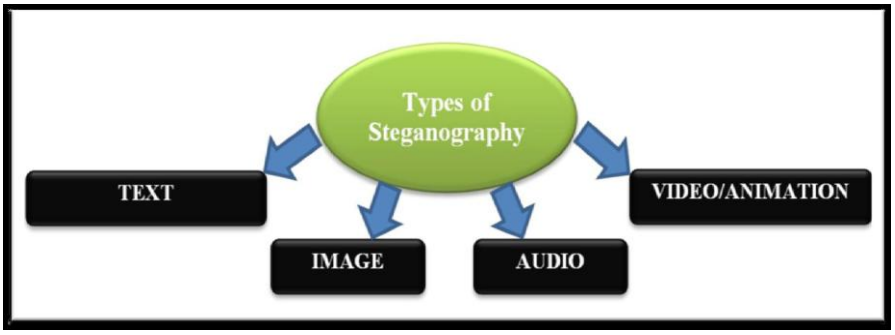
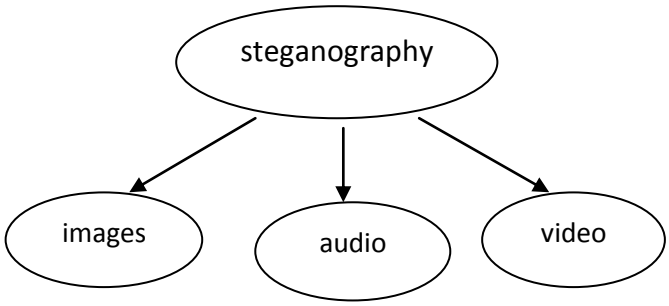


Fig. Different steganography approaches.

Different Kinds of Steganography

Figure below shows the three main categories of file formats that are used in current steganography technology.



Video Steganography

Video is used as medium for Hidden information. Video steganography can be done on the formats such as MP4, MPEG, AVI etc.

Audio Steganography

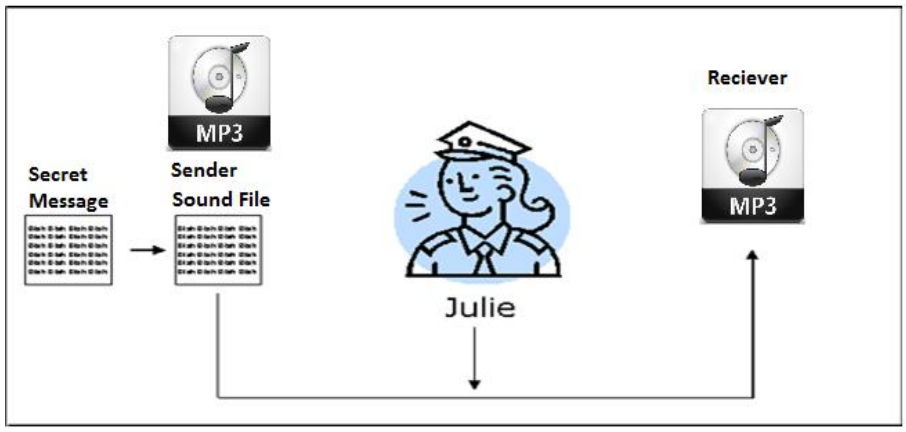


Figure: Secret Message behind MP3

Related Work

Andreas Westfeld (2001), proposed a algorithm, combines both preferences: resistance against visual and statistical attacks as well as high capacity. Matrix encoding and permutative straddling enable the user to decrease the necessary number of steganographic changes and to equalize the embedding rate in the steganogram. Pooyan, M.;Delforouzi,(2007), they present a novel method for digital audio steganography where encrypted covert data is embedded into the wavelet coefficients of host audio signal. Experimental results show that proposed method has large payload, high audio quality and full recovery. Gopalan, K., (2010),proposed some results of the tradeoff between the conflicting requirements of data robustness, payload and imperceptibility. Experimental results on both clean and noisy host audio signals indicate that while the payload can be as high as over 3000 bits/s much higher rate than common audio data embedding techniques notice ability of embedding is decreased and noise tolerance increased by using higher bit indices than the traditional least significant bit. Bit error rates of below one percent were observed for data retrieved from noise-added stego audio signals with 39 dB of SNR for an embedded payload of over 10 Kbits in a 3.3 s host audio. Usha, S. (2011), they proposed an encrypting system which combines techniques of cryptography and steganography with data hiding. Instead of using a single level of data encryption, the message is encrypted twice. Traditional techniques have been used for this purpose. Then the cipher is hidden inside the image in encrypted format for further use. It uses a reference matrix for selection of passwords depending on the properties of the image. The image with the hidden data is used for further purposes. Shahadi, H.I.; Jidin,R.(2011), they propose a new high capacity audio steganography algorithm based on the wavelet packet transform with adaptive hiding in least significant bits. The adaptive hiding is determined depend on the cover samples strength and bits block matching between message and cover signals. The results show that message can be embedded up to 42 % of the total size of the cover audio signal with at least of 50 dB signal to noise ratio. Balgurgi;Jagtap,S.K,(2012), The author provides implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography. The combination of LSB technique with XORing method is described in this paper, which gives additional level of security.

PROPOSED SYSTEM

Audio Steganography Techniques

There are number of techniques for data hiding in audio. Hiding data in audio can be done a number of ways like: Phase coding, Spread spectrum, Echo data hiding, Patchwork coding, Low-bit encoding. After analysis of these techniques for information hiding in digital audio, the Low-bit encoding technique has the highest quality bit rate but with low robust.

Low-bit encoding

This technique embeds the information into the least significant bit (LSB) of the audio file.

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Figure: Steps of Low Bit-Encoding

Working: Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. The LSB Technique is widely used for protecting the information. In this, the sampled output of the Audio file will be generated which will be substituted by the least significant bit of each sampling point with a binary message. Lease Significant bit (LSB) technique allows for a large amount of data to be encoded. The message 'HEY' is demonstrated by the below diagram:

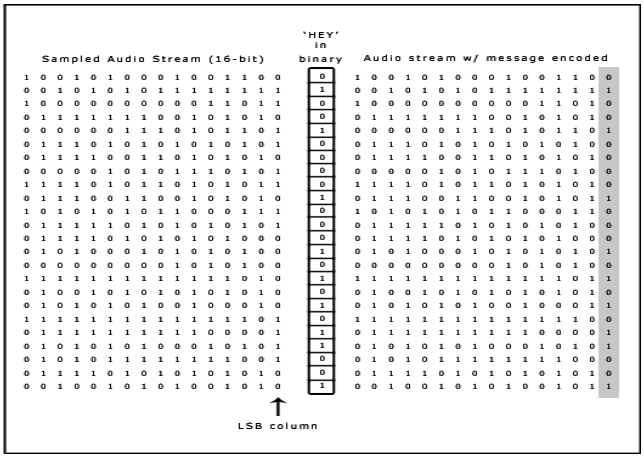


Figure: Low-Bit Encoding Technique

Echo Hiding

Echo data hiding embeds data into a host audio signal by introducing an echo. The data are hidden by varying three parameters of the echo: initial amplitude, decay rate and offset. As the offset (or delay) between the original and the echo decreases, the two signals blend. At a certain point, the human ear cannot distinguish between the two signals. The coder uses two delay times, one to represent a binary one (offset) and another to represent a binary zero (offset + delta).

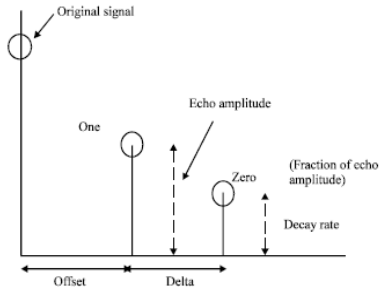


Figure: Echo Coding

To hide the data successfully, three parameters of the echo are varied: amplitude, decay rate, and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

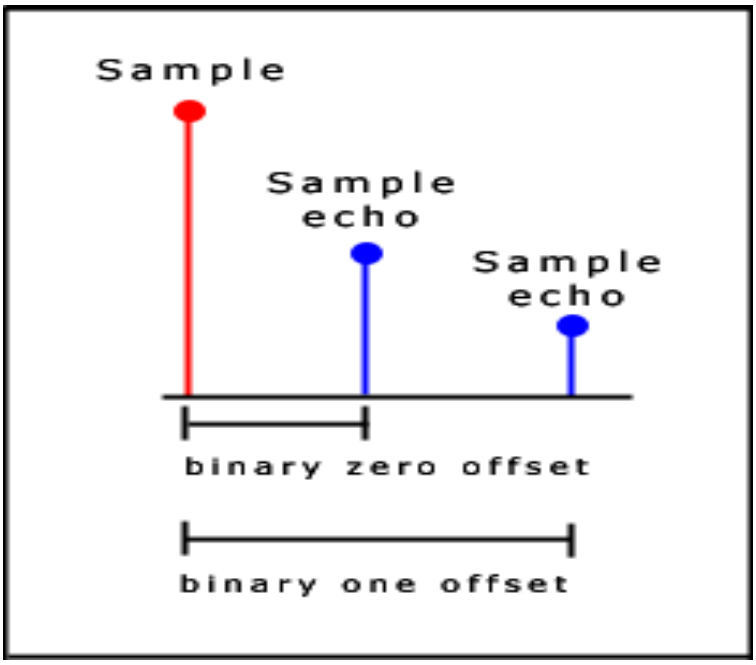


Figure: Offset Sample in Echo Coding

If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

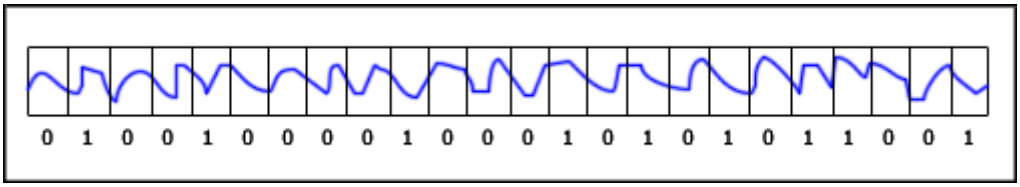


Figure: Binary Equivalent of HEY

There is simple form of the echo hiding process using the message 'HEY'. For briefness, there is need to divide the signal completely up into blocks, although under normal circumstances a random number of samples between each pair of blocks should remain unused to reduce the probability of detection. First the signal is divided up into blocks, and each block is assigned a one or a zero based on the secret message. In this case, the message is the binary equivalent of 'HEY'. Then the following algorithm illustrated through pseudo code is used to encode each block.

```
init(Block blocks[]) {
   for (int i=0; i < blocks.length; i++) {
      if (blocks[i].echoValue() == 0)
         blocks[i] = offset0(blocks[i]);
      else
         blocks[i] = offset1(blocks[i]);
   }
}

Block offset0(Block block) {
   return (block + (block - OFFSET_0));
}

Block offset1(Block block) {
   return (block + (block - OFFSET_1));
}
```

Figure: Pseudo Code of Echo

The blocks are recombined to produce the final signal. Using that implementation of the echo hiding process can usually result in a signal that has a fairly noticeable mix of echoes, thus increasing the risk of detection. A second implementation of the echo hiding process addresses this problem. First an echo signal is created from the entire original signal using the binary zero offset value. Then a second echo signal is created from the entire original signal using the binary one offset value. Thus the "one" echo signal only contains ones, and the “zero” echo signal only contains zeros. To combine the two echoes together to get the final encoding, two mixer signals are used. The mixer signals have a value of either one or zero, depending on which bit is to be encoded in the block. In our example using the message ‘HEY’, we would get the following two mixer signals.

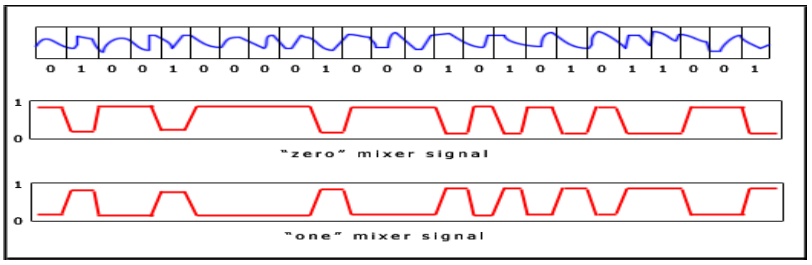


Figure: Blocks Recombined

The “one” echo signal is then multiplied by the “one” mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes. The following diagram summarizes the second implementation of the echo hiding process.

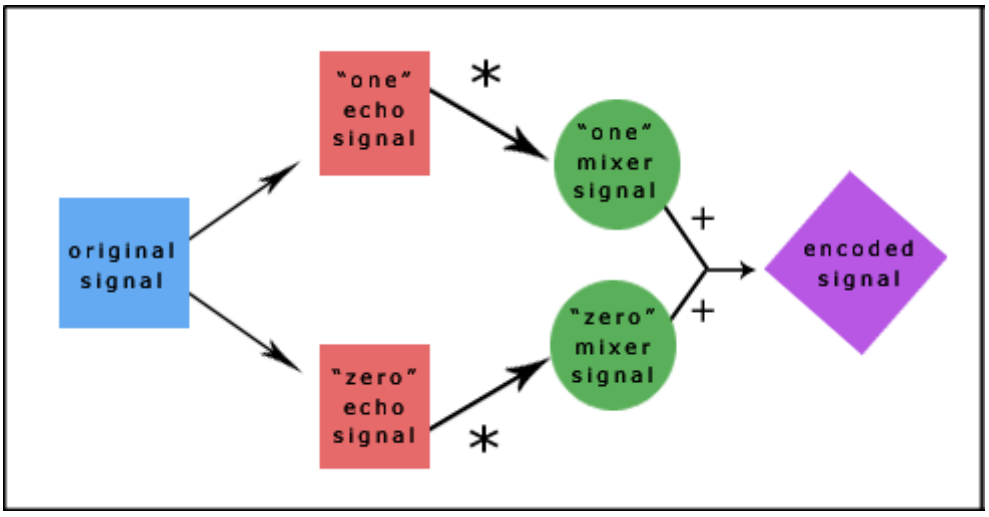


Figure: Echo hiding implementation

To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's cepstrum and the cepstrum is the Forward Fourier Transform of the signal's frequency spectrum, can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed.

Algorithm

Algorithm is used for solving the problem step by step which can be implemented with help of programming in any language.

1. Start
2. Initialize Secure Information
3. Read Data and Input Bytes
4. Setup Cryptographic Function
5. Implement Cryptographic technique T
6. Initialize Stegnaographic Algorithm
7. Selection of Audio Wave File
8. Implement Data Hiding Scheme in Audio
9. Hide Byte by Bite Information
10. Is All Hidden Successful
    Then Jump to 11
    Else Jump to 9
11. Generate Audio File

12. Generate Output Result and Comparison Audio Graphs
13. Stop

EXPERIMENTAL RESULTS AND DISCUSSIONS

The Proposed work has been implemented in the MATLAB Tool with Crytography and Steganography Concepts. The Inputs has been provided to the algorithm is Text file with Text information i.e. Confidential information, Media File and retrieved the output in form of the media file. The graph has been shown of audio steganography shows that there is no loss in quality of sound and resulted sound file will be accurate in terms of memory. The number of steps has been analyzed to secure the information. The Substitution cryptography and Data Hiding steganography techniques has been implemented for encrypt, decrypt information and steganography for hiding of information. The Least Significant bit (LSB) replaces the wav LSB with the encrypted Information.

The Proposed work has been practical worked out on the simulator and results are described as following diagrams.

Figure: Running Simulator

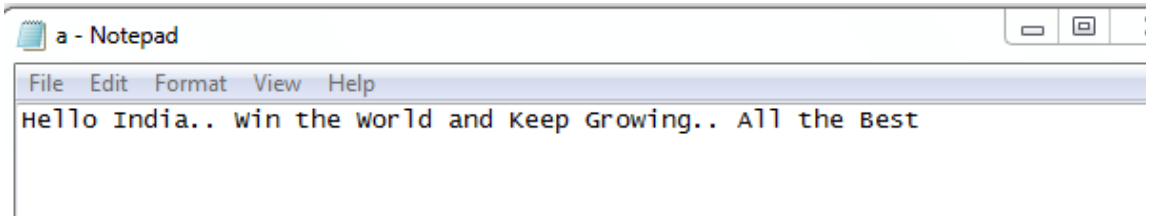


Figure: Input 1

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

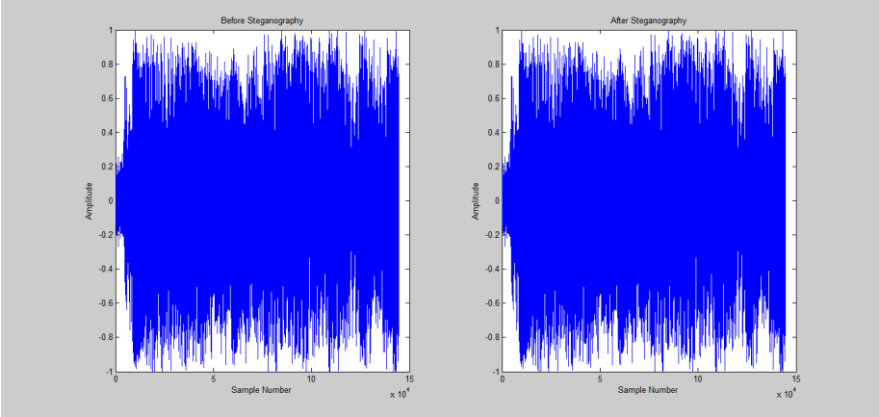


Figure 1: Output 1

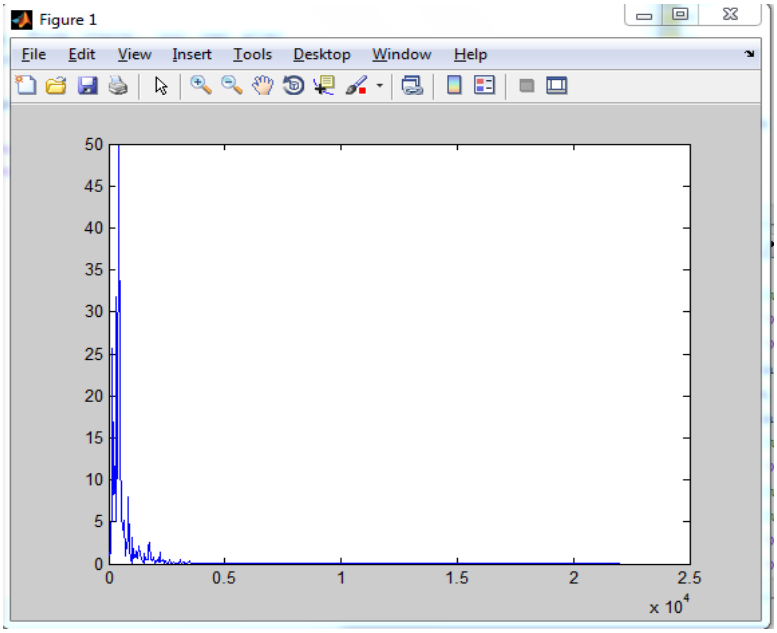


Figure 2: Output 2

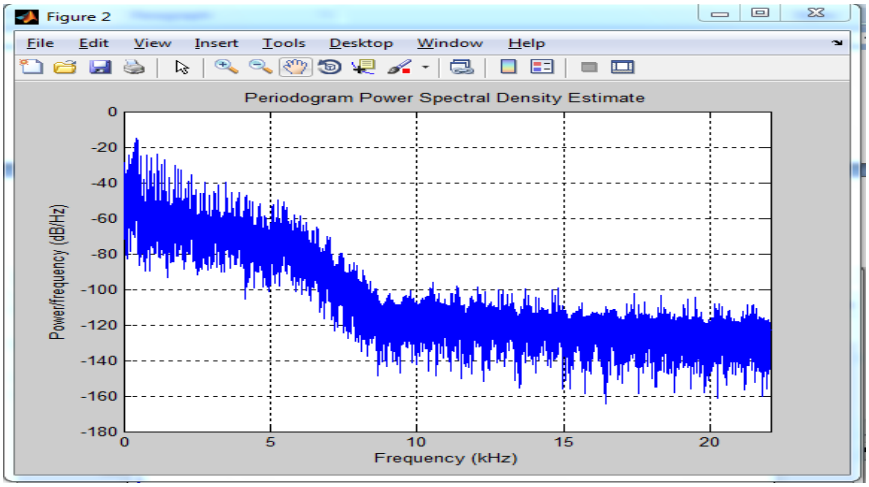


Figure: Output 3

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

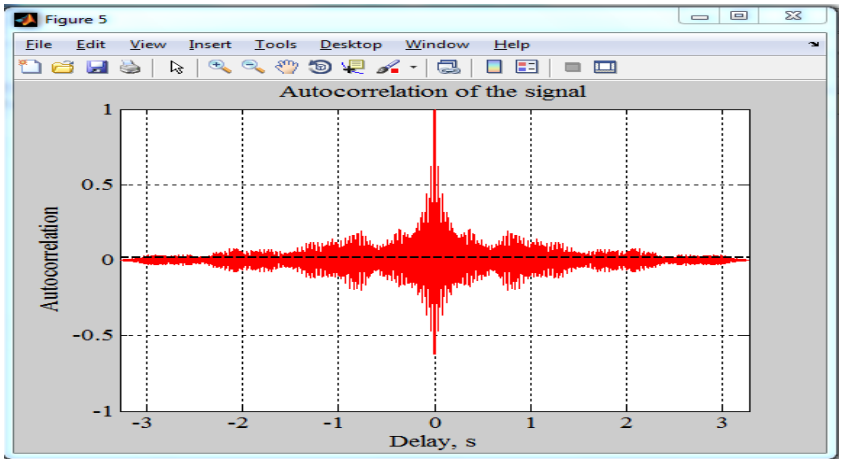


Figure: Output 4

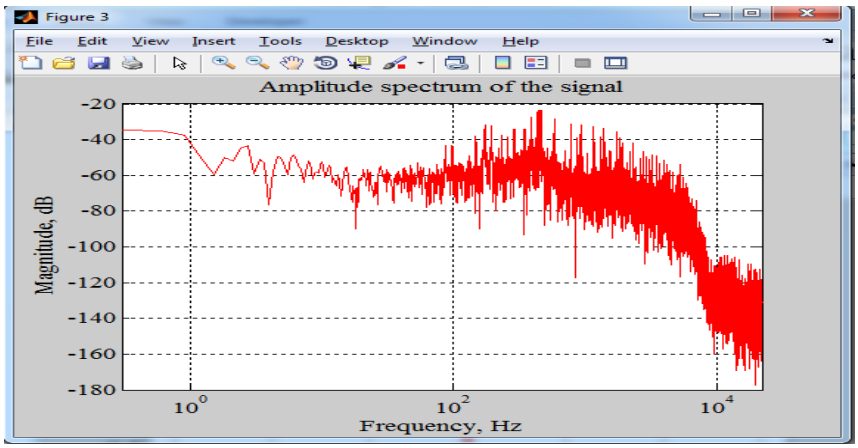


Figure: Output 5

```
ans =

  HI.trden hl ldWedKlii  eoanWae . onp nl   GglB  r. e  o.ts  w ht  iAe


cipher_data =

Hello India.. Win the World and Keep Growing.. All the Best


Original =

Hello India.. Win the World and Keep Growing.. All the Best
```

Figure: Output 6

The below figures shows the PSNR values of the proposed work.

```
>> run('D:\thesis\2015-2016\Vandana CDLU\Final Implementation\MPSNR.m')
mse=0.27692 PSNR=107.4823 BER=0
```

Figure: Peal Signal to Noise Ratio

CONCLUSION

In this paper, The proposed work will compute cipher text of message using cryptography algorithm, then LSB technique will hide the information in audio file. The corruption of the secret data's host means the corruption of the secret data. This article proposed a simple application of threshold sharing and information hiding in mp3 audio files. The sound file will be modified and keep the information inside it. The experimental results show the accuracy of system and will be beneficial for organization. Finally high perceptual transparency is accomplished by LSB of host audio signal which are used for data hiding and method has improved the capacity and robustness of data hiding in the audio file.

REFERENCES

[1] Y.K.Lee and L.H.Chen(2000), "High capacity image steganographic model".

[2] Andreas Westfeld (2001), "A Steganographic Algorithm High Capacity Despite Better Steganalysis".

[3] Kevin Curran (2003), "An Evaluation of Image Based Steganography Methods".

[4] Chang-Chou Lin, Wen-Hsiang Tsai (2004)," Secret image sharing with steganography and authentication".

[5] Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon(2004), "Image Steganography and Steganalysis: Concepts and Practice".

[6] Andrew D. Ker (2004)," Improved Detection of LSB Steganography in Grayscale Images".

[7] Delforouzi, A. ; Pooyan, M., "Adaptive Digital Audio Steganography Based on Integer Wavelet Transform" ,Intelligent Information Hiding and Multimedia Signal Processing. IIHMSP 2007. Page(s): 283 - 286

[8] Pooyan, M. ; Delforouzi, A., "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", Signal Processing and Information Technology, 2007, Page(s): 600 - 603

[9] Shah, P. ; Choudhari, P. ; Sivaraman, S., "Adaptive Wavelet Packet Based Audio Steganography using Data History", Industrial and Information Systems, 2008. ICIIS 2008. IEEE, 2008 , Page(s): 1 – 5

[10] Arvind Kumar , Km. Pooja (2010), "Steganography- A Data Hiding Technique".

[11] Gopalan, K., Qidong Shi, "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference

2010 , Page(s): 1 – 6.

[12] Sujay Narayana and Gaurav Prasad (2010)," Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions".

[13] Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan (2010), "New Design for Information Hiding with in Steganography Using Distortion Techniques".

[14] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi (2010)," Overview: Main Fundamentals for Steganography".

[15] Usha, S. (2011), "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), 2011 International Conference, Page(s):1017 - 1020

[16] Djebbar, F. ; Ayad, B. ; Hamam, H. ; Abed-Meraim, K, "A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011 International Conference on 2011 , Page(s): 409 - 414

[17] Nugraha, R.M., "Implementation of Direct Sequence Spread Spectrum steganography on audio data", Electrical Engineering and Informatics (ICEEI), 2011 International Conference 2011 , Page(s): 1 – 6

[18] Asad, M. ; Gilani, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011 International Conference, 2011 , Page(s): 143 - 147

[19] Shahadi, H.I. ; Jidin, R., "High capacity and inaudibility audio steganography scheme Information Assurance and Security (IAS)", 2011 Page(s): 104 - 109

[20] Balgurgi, P.P. ; Jagtap, S.K., "Intelligent processing: An approach of audio steganography", Communication, Information & Computing Technology (ICCICT), 2012, Page(s): 1 – 6