STEGANOGRAPHY A PRACTICAL APPROACH

[1]Ankur Mehta, [2]Shobha Bhatt
[1]Computer Science & Engineering,
[1]Ambedkar Institute of Advanced Communication Technologies & Research,, Geeta Colony, Delhi, India

Abstract : Today, in the digital world, all the things are available on the internet. The main concern is about privacy and security due to which steganography has experienced a great concentration by the researcher, as it has been an effective method to provide data security or secure communication. There are many modern and successful methods to secure digital data in a real-world application. Cost effective secrecy can be accomplished by doing the steganography methods.
This paper presents the Least Significant Bit Steganography method of embedding text data in an audio file. The text will be taken as a secret message, and in the second case, we are taking the text as a cover media and the secret message itself hidden in the cover media. The stego function is based on index location. The key is used to encrypt the stego function and send it to the receiver end the stego function is encoded in such a way that it can be sent to the destination safely and to give a better, extremely organized method for maintaining security.

Index Terms **- Steganography, Secret Message, Cryptography, LSB Method, Cover Media.**

I. INTRODUCTION

Today, digital contents are spreading over the internet very rapidly. Information Security is the main concern for the society to how to send the information securely over the insecure channel. Organization and individuals who seek covertness can use the cryptography and steganography as one who can help in avoiding supposition and protect privacy.

The Steganography can be used to hide data. According to the need when we know that the message is crucial, and we want it to send to another person keeping in mind that the message is sent in such a way that hacker does nothing the existence of message [1].

In Fig 1 the function F contains a cover media 'C', a message 'M' and a stego-key 'K' and a stego-object 'Z'. In this figure, the cover media 'C' is the original carrier in which we will hide the message 'M'. Message 'M' can be encrypted text or may be simple text, audio, and image. Stego-key 'K' is used as a password or pre-defined function which is used to provide more secrecy to message when it flows on an insecure channel to prevent it from hackers. Stego-object 'Z' is the output of the function which we applied for Steganography. Stego-object is the final result of the technique which we implemented. This is the process of hiding the message into the cover object. To get the message back, we have to need the stego-function and the stego-key 'K'. By using the key, we can decrypt the message, and with the stego-function helps to find out where the secret message has been hidden.

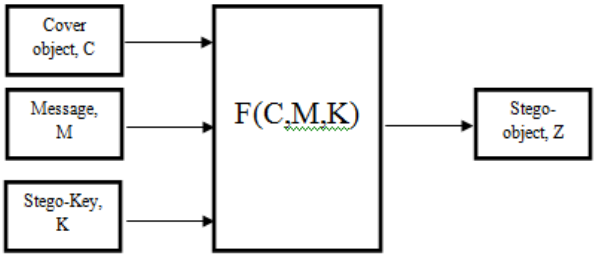

Fig.1. Steganography

Hiding Capacity, Perceptual Transparency, Robustness Tamper–resistance, Confidentiality, Imperceptibility, Accurateness, High capacity, Resistance, Visibility, Survivability, One-Way Hashing because of this all steganography is the prime choice of the user to secure their data. However, as many blessings in steganography, there is a limitation of steganography in this excess amount of memory required, time-consuming, based on an algorithm and if the algorithm is known to others, then this technique fails, required more attention and care to protect from hackers.

The nature of the Steganography is described below in the Fig.2[2]. There are three types of Steganography, i.e. Text, Image, and Audio/Video. We have to choose the cover medium and the secret message according to the need.

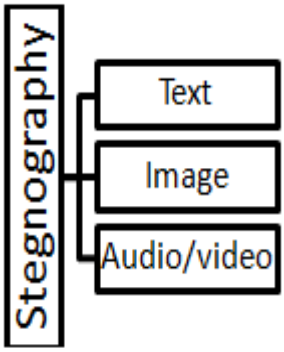

Fig.2. Types of Steganography

In section II, the previous work which has been done and their methods are discussed. In section III the steganography is discussed by taking the two cases in the first case, i.e., audio steganography with the least significant bit in which the cover medium is audio, and the secret message is text, and in the second case the text steganography we will send the secret message with the help of key which is the index location of the strings and the key is encrypted. In section IV, the algorithm is defined as how to implement the steganography. In section V, the implementation and the result are shown. In section VI, the conclusion and the future scope is discussed.

II. LITERATURE REVIEW

Researchers presented the comparative study of digital audio steganography techniques in the survey paper. They discussed the merits and demerits of the various methods like Eco Hiding, Tone Insertion, Spread Spectrum, Low bit encoding and also mentioned the application and trends of the steganography in the market [3].

Dutta, Poulami, Debnath Bhattacharyya, and Tai-hoon Kim presented a method in which the least significant bit of the audio file is replaced by the secret message which we want to hide. In this method, the size of the audio file is the same after implementing the Steganography [4].

Muhammad Asad, Junaid Gilani, and Adnan Khalid gave a three-layered model for audio steganography based on least significant bit replacement [5]. In the first layer, they encoded the secret message into hexadecimal format after that in the second layer, the hexadecimal message is encrypted, and in the last stage, the message in the original audio file. In this approach, the three parameters were taken, i.e. transparency, capacity, and robustness and also compared the SNR as compared to the conventional Least Significant Bit method.

Binny, Anu, and Maddulety Koilakuntla used Steganographic technique to compute the SNR values for various audio files by using the LSB method in which they converted their secret message into binary form and embedded in the least bit of original audio file [6].

Por, Lip Yee, and B. Delina proposed a new method of text steganography in which the hybrid method is used consisting of inter-word spacing and inter-paragraph spacing is used. The Stego-text is also generated dynamically using the six parameters in this new method [7].

III. STEGANOGRPAHY

Steganography is a technique to hide the data within the data, and it can also be used with the cryptography to provide extra security to your context which you send over the insecure channel to increase the security.

Case 1

Audio Steganography is a method used to send the secret message by embedding it in the audio cover signal in an impalpable manner. The original file before the steganography and the stego file have the same characteristics. Fig.3 shows the workflow of the Audio Steganography is depend on the cover medium, which is audio in this case. The secret message is encrypted with the help of key and stego function is used to hide the secret message at the place where we want to hide the message and then sends it to the other user. At the receiver ends they used the key and the stego function to get the secret message back.

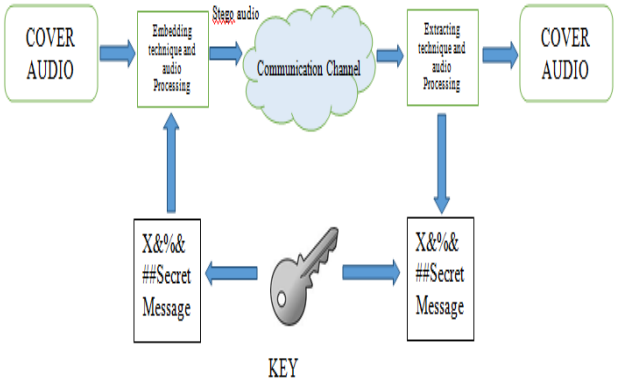

Fig. 3. Audio Steganography Workflow

Case 2

In the Text steganography method, the message was embedded in a cover medium. The stego function is based on index location, and the pre-defined algorithm is designed, which is used for encryption and extraction process, and both the sender and receiver used the same algorithm for this. The workflow of the Text Steganography is shown in the "Fig.4" below

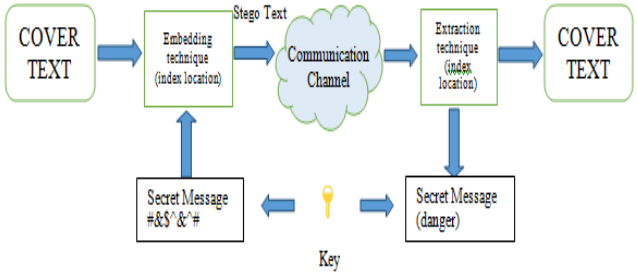

Fig. 4. Text Steganography Workflow

3.1 LEAST SIGNIFICANT BIT METHOD

The Least Significant Method is one of the traditional methods which are used for hiding the information. In this method, the last bit of the cover file is replaced by the secret message. If we take an audio file as a cover medium for secret communication, then it has high embedding capacity as compared to take the other cover medium like image and text [8]. LSB is used because the changes we made is not much visible compared to the other bits in a binary sequence. The main advantage of this process is facile to use, but it is more vulnerable to attacks. To prevent it from attack we can use cryptography which we are using in our method.

IV. METHODOLOGY

In our model, we will implement 2 cases in which first is audio steganography in which cryptography is also used for encrypting the secret message, and in the second case, text steganography is used

Case 1 *Embedding Algorithm for Audio Steganography*

Step1:- Select or Record .wav file as Carrier and a text as a secret message.
Step2:- Read the audio file and secret message in binary.
Step3:- Prepare secret message text as a binary column vector 8.
Step4:- Prepare carrier as a matrix of 8 columns.
Step5:- Replace the least significant bit of audio file with the corresponding element of secret message.
Step6:- After getting the binary stego audio file convert that file into an audio file.

Extraction Algorithm for Audio Steganography

Step1:- Read the stego audio and convert it into the binary.
Step2:- Extract the secret message which is hidden in the LSB of stego audio by stego function.
Step3:- Convert extracted binary code into text.
Step4:- Display the secret message.

Case 2 *Algorithm for Text Steganography*

Step1:- Select or Text file as Carrier and a text as a secret message.

Step2:- Create a stego function based on index location where the message is hidden.

Step3:- Encrypt the stego function using the substitution cipher.

Step4:- Send the cover audio to the receiver, and the receiver will know the key and stego function.

Step6:- At the receiver end, the extraction process used stego function and the key to get the secret message.

V. IMPLEMENTATION

The text steganography can be implemented in mat lab software by encrypting the secret message and then hide it in the cover medium, which is also text using the LSB method. The audio steganography is also implemented in Matlab. The algorithm is mentioned above. The implemented result is shown in the figures and graph. The graph is shown in "Fig. 5" is the original audio file which is recorded in the Matlab at run time. The "Fig.6" shown is the graph after replacing the least significant bit in the original audio. When we compare, both graphs are similar, that means the steganography technique is implemented successfully.

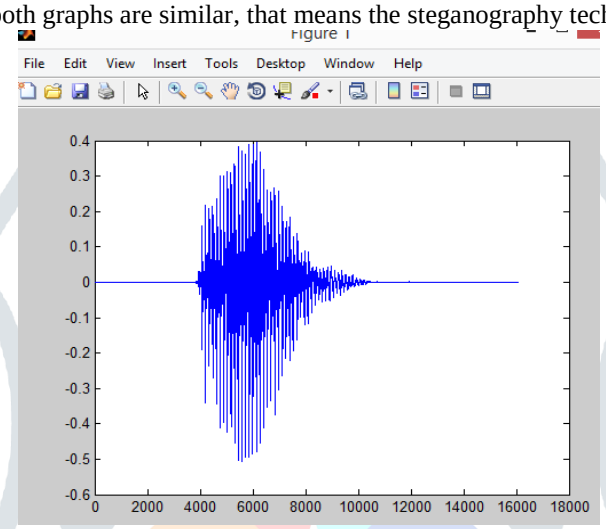

Fig5: Original Audio

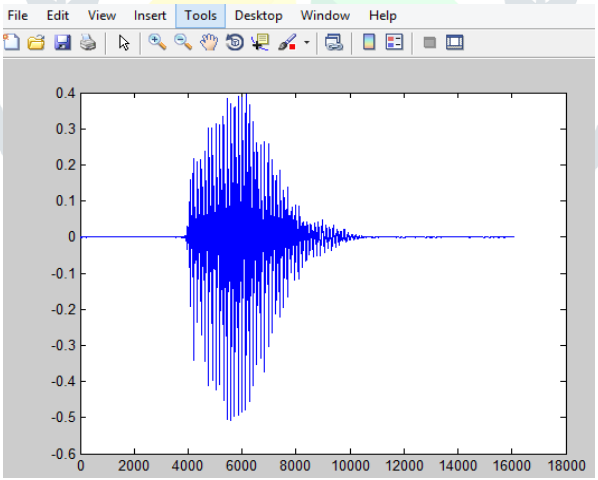

Fig6: Stego Audio

The comparison is shown in the table in which the Mean Squared Error value is shown. In the method where both cryptography and steganography implemented has lower MSE value as compared to the method on which the only steganography implemented. "Table 1" shows the comparison between both the methods on the parameters discussed earlier.

Table 1 Comparison of MSE and Size

Stego Audio File	**Method**	**MSE**	**SIZE**
Final1.wav	Steganography only	1.1548e-13	32KB
Final2.wav	Cryptography and Steganography	1.8005e-09	32KB

Case2 In the second case, we will take the cover media as a text in our case we are taking as shown in Fig7. Now the secret message in our case "danger" is hidden in the cover medium at a different location. We used the index locations to hide the secret message. In this, we used an index location, and this is our stego function.

```
ambedkar institute geeta colony rohini
```

Fig. 7. Cover Medium

After that encrypt the encrypt the stego function by using the substitution cipher as shown in Fig. 8.

```
5     7     11     20     21     33
```

Fig. 8. Stego-key

Send the cover media to the receiver and share the stego function and key with it after that the receiver used the same and extract the message hidden in the cover media. The extracted message is shown in the "Fig.9"

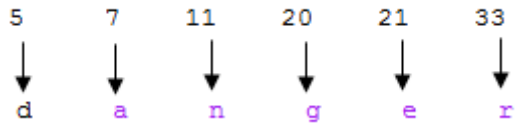

Fig. 9. Extraction of Secret Message

This is the implementation of the text steganography using both cover medium and the secret message as a text.

VI. CONCLUSION AND FUTURE WORK

To transmit the data secretly, which is hidden, steganography methods have been used. The use of audio signals has made them an essential choice to convey secret information. We discussed the basics of steganography, including its models, nature, characteristics, and some issues. Further, we proposed a new approach in audio steganography in which the secret message is first encrypted in the same level before hiding the secret message at the least bit of the cover medium to embed a message in the audio file. Finally, the message was received correctly at the receiver end by using the cryptography technique to encrypt the secret message, and the method is also verified using the parameters like MSE and size. In text steganography, we used a new technique in which we used the secret message is hidden at index location in the cover text. We generate the stego function and encrypting it with the help of substitution cipher and send it to the receiver. The receiver will extract the stego function using the key and get the message This provides high-level security and privacy over the insecure channel. The future work should be focused towards to enhance the security and robustness and also calculate the SNR ratio.

REFERENCES

[1] Doshi, Pratik Jain, and Lalit Gupta. "Steganography and its Applications in Security." International Journal of Modern Engineering Research (IJMER) 2.6 (2012): 4634-4638.

[2] Kanhe, Kanhe, Aniruddha, et al. "Robust Audio steganography based on Advanced Encryption standards in the temporal domain." Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015.

[3] Fatiha Djebabr, Beghdad Avad, Karim Abed Meriam and Habib Hamam Fatiha. "Comparative study of digital audio steganography techniques." EURASIP Journal on Audio, Speech, and Music Processing 2012.1 (2012): 25.

[4] Dutta, Poulami, Debnath Bhattacharyya, and Tai-hoon Kim. "Data hiding in audio signal: A review." International journal of database theory and application 2.2 (2009): 1-8.

[5] Asad, Muhammad, Junaid Gilani, and Adnan Khalid. "Three layered model for audio steganography." Emerging Technologies (ICET), 2012 International Conference on. IEEE, 2012.

[6] Binny, Anu, and Maddulety Koilakuntla. "Hiding secret information using LSB based audio steganography." Soft Computing and Machine Intelligence (ISCMI), 2014 International Conference on. IEEE, 2014.

[7] Por, Lip Yee, and B. Delina. "Information hiding: A new approach in text steganography." WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. No. 7. World Scientific and Engineering Academy and Society, 2008.

[8] Gupta, Shailender, Ankur Goyal, and Bharat Bhushan. "Information hiding using least significant bit steganography and cryptography." International Journal of Modern Education and Computer Science 4.6 (2012): 27.