Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Survey on Audio Steganography Techniques for Digital Data Security

**Ashima Wadhwa**
*Department of Computer Science and Applications,*
*Kurukshetra University, Kurukshetra, India*

***Abstract-The excessive use of digital data in various real life scenarios has been emerging the interest of scientists to ensure their security. Techniques such as cryptography, steganography and watermarking are used in this regard. Out of these, steganography proves to be an efficient technique which provides better confidentiality because it is the practice of hiding information and an effort to mask the existence of the embedded information. Four main trends of development of steganography are: digital media steganography; linguistic steganography; file system steganography and network steganography. In digital media steganography we mainly use text files, images, audio and videos as carrier. But in our study we focus on audio as a carrier. In this paper we present a comparison of all digital data security techniques. A comparison and evaluation of various digital audio steganography techniques are also studied.***

***Keywords-cryptography, steganography, audio steganography, LSB, watermarking.***

## I. INTRODUCTION

Today digital communication has become an extremely important area of concern and mostly applications are internet based. Excessive use of internet for communication purpose increases the possibility of attacks. Hence security during communication has become a fundamental issue. Security of information depends on the privacy of its existence and confidentiality of its decoding methods. Digital data security can be achieved in two ways-encryption and data hiding. Cryptography technique distorts the information in such a way that it cannot be recognized. Steganography and Digital watermarking are the popular data hiding techniques. Steganography prevents suspecting the existence of data by inadvertent recipient but digital watermarking provides copyright protection by hiding legal information.

### *A. Cryptography*

The art of securing information by scrambling it into unrecognizable format called cipher text. A secret key is used for encryption and decryption process. Cryptography only hides the content of message not the existence of message.

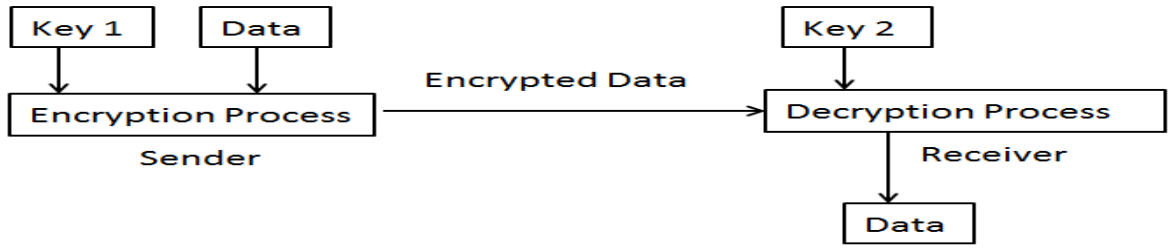



Fig. 1 Cryptography Technique

Two types of cryptography are there:

- Symmetric key Cryptography: In this same key is used by sender and receiver
- Asymmetric key Cryptography: In this different key is used by sender and receiver

### *B. Digital Watermarking*

It is the method of embedding information into digital file in such a way that its removal is hardly possible. In this digital file may be any text, audio, video or image. If someone tries to copy the watermarked file then information also copied. It may be used for authentication, certification and conditional access.

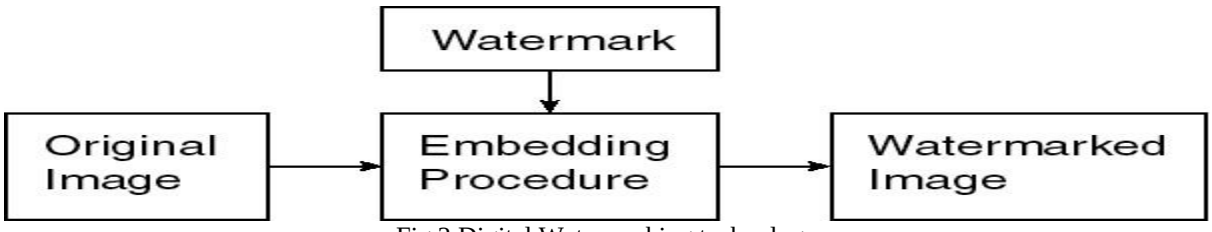



Fig.2 Digital Watermarking technology

*C. Steganography*

Steganography formally means "masked writing" and is proved to be a new alternative technique to ensure data security. It is a technique of hiding the existence of one message in the presence of another carrier message. Steganography technique requires a cover that will hold the data and a message that is to be transported. Cover may be any image, audio, video, text or other digitally representative code. Message may be plain text, images, audio, images or cipher text. It also needs a stego key for the embedding and extraction process. The message is embedded in the cover file in such a way that the quality of cover media is not lost. After the embedding of message in the carrier a stego file is generated this is transmitted over the channel. Receiver must have stego key to extract the secret message.

Modern Steganography Methods:

- Embedding Secret message in plain text
- Embedding Secret message in images
- Embedding Secret message in audio
- Embedding Secret message in video
- Embedding Secret message in ip datagram

*D. Audio Steganography*

Audio steganography is a technique of hiding secret message in the audio signal. In this case secret message can be audio or text. In order to make audio steganography successful the difference between audio carrier signal and stego audio signal should be undetectable. Capacity, transparency and robustness are the three parameters to define the audio steganography technique [8].

- Capacity → number of bits of secret message that can be embedded in carrier.
- Transparency→ how securely the information embedded.
- Robustness→ ability of the stego message to resist stegnalysis attacks.

## II. LITERATURE REVIEW

W. Bender D. Gruhl N. Morimoto A. Lu [1] describes both conventional and new approaches including low bit coding, phase coding, echo hiding ,spread spectrum for data hiding and evaluation of all the techniques is performed on the basis of copyright protection, temper proofing and augmentation data embedding.

Muhammad Asad, Junaid Gilani, Adnan Khalid [2] proposes two methods to improve the conventional LSB technique-Bit Selection and Sample Selection. The first method is to randomize bit number of secret message used for embedding. And second method is to randomize the sample number which is used for embedding the next message bit. Both the proposed algorithms work fine against steganalysis attacks. A successful test has been performed for proposed method on the .wav file with 8000 samples per second containing 8 bits per sample.

Harish Kumar, Anuradha[3] have presented a Steganography method of hiding text data in an audio file and proposed a technique which firstly sampled the audio file and then suitable modification is done at LSB.Experimental results are also given for the proposed technique

Pooja P. Balgurgi, Prof. Sonal K. Jagtap[4]presented the implementation of two level security by combining cryptography and steganography. And proposed an algorithm in which combination of LSB technique and XORing method is used to provide a better level of security. Brief description of all the audio steganography techniques is also presented.

Gunjan Nehru, Puja Dhar[5]describe different techniques of audio steganography using algorithmis like genetic algorithm and LSB method.

Mazdak Zamani,Rabiah Bt Ahmad.Azizah Bt Abdul Manaf,Akram M. Zeki[6]gives a new approach of substitution of audio steganography to increase the robustness. Robustness mainly enhanced against both intentional and unintentional attacks. In proposed technique Genetic algorithm is used and the message bit is embedded into higher LSB layers.

Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam[7] performs a comparative study of all the digital audio steganography techniques.

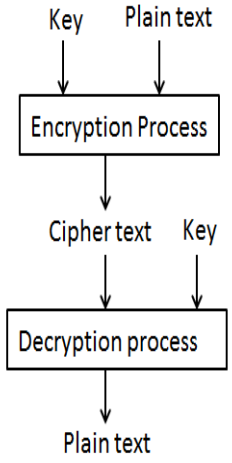
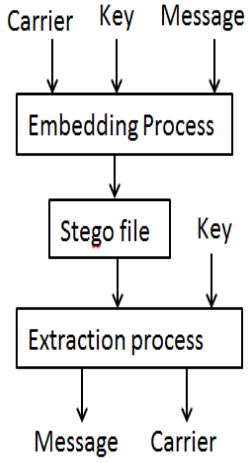
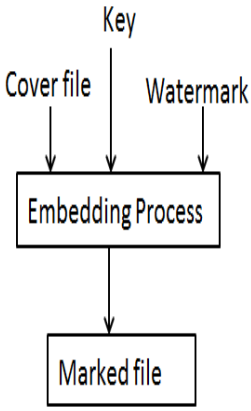
## III. PERFORMANCE REVIEW

To improve the security of digital data over internet encryption and data hiding techniques are used. Various criteria are used to compare security techniques in tabular form (Table1)

Table I Comparison Between different Data Security Techniques

| **Digital Data Security Techniques** | | | |
|---|---|---|---|
| **Criteria** | **Encryption** | **Data Hiding** | |
| **Technique** | **Cryptography** | **Steganography** | **Watermarking** |
| **Goal** | Garble the contents of communication | Hiding the actuality of communication | Protection of carrier Or copyright |

| | | | | |
|---|---|---|---|---|
| **Methodology** | |  |  |  |
| **Features** | *Confidentiality* | Cipher text is unreadable | Embedded information is imperceptible to the unknowing observer | Invisibility or visibility depends on requirements |
| | *Robustness* | A complex encryption algorithm gives assurance of robustness | Protection against detection of embedded data | Robustness against removal of embedded data |
| | *Security* | It depends on the secrecy of the key | It depends on confidentiality of the method of embedding | It also depends on privacy of embedding method used |
| | *Visibility* | Communication is visible | Invisible and Inaudible | Visible<br>Invisible |
| | *Type of Carrier* | No need of carrier | • Carrier may be any service, protocol, file, environment employing digital representation of data<br>• There is no relation between message and carrier | • Digital files like audio, video, text or images<br>• Embedded data is used to secure the carrier |
| | *Effect of compression* | | May lead to loss of hidden data | Must not lead to loss of watermark |
| | *Attacks* | Easy detection and complex extraction | Detection and Extraction both are complex | Extraction is much complex |
| **Requirements** | | Robustness | • Undetectability<br>• Capacity | Robustness |

Many techniques for audio steganography have been presented over time. Some of the well-known techniques are low bit coding, echo hiding, spread spectrum, phase coding and many more. The advantages and disadvantages of some of techniques are discussed in tabular form (Table2)

Table: II Comparison Between different Audio Steganography Techniques

| **Audio Steganography Techniques** | | | | |
|---|---|---|---|---|
| **Technique** | | **Embedding Approach** | **Strong Points** | **Weak Points** |
| | *Lowest Bit Coding* | This method embeds the data in the Least significant bit of each sample. | • Low computational complexity<br>• High bit rate<br>• Easier implementation | • Less prone to attacks<br>• Filtering, amplifying, noise addition and compression of audio will destroy the data<br>• Extraction is easy |
| | *Parity Coding* | This method breaks down signal into different region of samples and the region's parity bit is used for embedding. | It provides more choices in encoding the secret bit | Easy to extract and destroy |

| | | | | |
|---|---|---|---|---|
| **LSB Encoding** | *XORing of LSB* | In this XOR operation is performed on least significant bits. Modification of LSB depends on the result of XOR operation and bit to be embedded. | • Easy to implement and increase the security of conventional LSB<br>• Extraction is not that much easy | • Addition of noise can destroy the data<br>• Used for single audio format: .wav |
| | *Bit Selection* | This method selects different bits for embedding in every sample. First 2 MSB bits of a sample are used to select the bit. In this only first 3 LSB's are used for embedding. | Randomness in the bit selection is used to confuse the intruder thus providing more security. | Compression will destroy the data |
| | *Sample Selection* | This method does not use all the samples for data hiding and selects the different samples for embedding. The selection of next sample for embedding depends on the first 3 MSB's of sample. | More secure than bit selection | Compression will destroy the data |
| | *Variable Low bit Coding* | This is an improved version of Lowest Bit Coding method. In this method two threshold values are calculated. Assume threshold1<threshold2<br>• If Amplitude range<threshold1→Secret data not embedded<br>• If Threshold1<Amplitude range<Threshold2→1 bit is embedded<br>• If Amplitude range>threshold2→2 bits are embedded | • It increases the embedding capacity.<br>• It provides more secure embedding than conventional LSB | Complex than conventional LSB |
| | *Average Amplitude Method* | Average amplitude data of neighbouring audio data except own audio data is used as threshold. If amplitude level is greater than threshold than 2 binary digits are used for embedding else no embedding take place. | This method will increase the capacity and secrecy of embedding | • Computational Complexity is high<br>• Embedding is limited to 2 binary bits |
| | *Embedding At $4^{th}$ and $5^{th}$ LSB Layer* | This method embeds the message bit at $4^{th}$ and $5^{th}$ LSB of every audio sample. | Distortion of host audio is reduced thus making steganography more secure | Easy to extract |
| | *Genetic Algorithm Based Audio Steganography* | This algorithm consists of 4 steps<br>• Alteration<br>• Modification<br>• Verification<br>• Reconstruction | This method supports different file formats and message length is increased | Computational Complexity is high |
| **Echo Hiding** | | This method introduces the echo for embedding data in audio signal. Data hiding depends on 3 parameters of echo:<br>• Initial Amplitude<br>• Offset<br>• Decay Rate | • Compression of audio will not destroy the data<br>• All parameters are set below threshold value of human hearing so echo is not easily resolved. | Low embedding capacity and security |
| **Phase Encoding** | | This method performs modulation of cover audio | • It is an effective technique in terms | Low Capacity |

| | | | |
|---|---|---|---|
| | signal for embedding data signal. | of signal to perceived noise ratio.<br>• Robust to the manipulation of audio signal. | |
| **Spread Spectrum** | In this method the confidential data is distributed over frequency spectrum of audio signal. | Highly Robust | Unprotected to time scale modification |
| **Tone Insertion** | This method inserts tones with low power level at known frequencies. | Invisibility of embedded data | Lack of clarity and security |
| **Wavelet Coefficient** | In this method data is embedded in LSB's of wavelet coefficients. | Embedding capacity is high | Extracted data may be lossy |

## IV. CONCLUSION

Security has a great importance and application in large areas. Cryptography and steganography are widely used methods to provide data security. Steganography provides better security than cryptography because steganography secretly transmits the messages without the fact of communication being discovered. Among all the steganography techniques audio steganography is more challenging. In this paper all the digital data security techniques are compared and also a comparison of all the steganography techniques is given.

## REFERENCES

[1] W. Bender D. Gruhl N. Morimoto A. Lu, "Techniques for Data Hiding", IBM Systems Journal, vol. 35, no. 3 and 4,pp. 313-336, 1996.

[2] Muhammad Asad, Junaid Gilani, Adnan Khalid," An Enhanced Least Significant BitModification Technique for Audio Steganography", IEEE978-1-61284-941-6/111$26.00 ,2011.

[3] Harish Kumar, Anuradha" Enhanced LSB technique for Audio Steganography" ICCCNT'12 26th_28th July 2012, Coimbatore, India,IEEE-2012

[4] Pooja P. Balgurgi, Sonal K. Jagtap(2012) "Intelligent Processing : An Approach of Audio Steganography" 2012 IEEE International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India

[5] Gunjan Nehru, Puja Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[6] Mazdak Zamani,Rabiah Bt Ahmad.Azizah Bt Abdul Manaf,Akram M. Zeki "An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography" IEEE-2009,978-1-4244-4520-2/09.

[7] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam" Comparative study of digital audio steganography techniques" Djebbar *et al. EURASIP Journal on Audio, Speech, andMusic Processing* 2012

[8] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, "A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009,Page(s): 1 – 6.

[9] Arvind Kumar, Km. Pooja(2010), "Steganography- A Data Hiding Technique", Research paper, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November

[10] Tanmaiy G. Verma, Zohaib Hasan, Dr. Girish Verma(2013),"A Unique Approach for Data Hiding Using Audio Steganography",International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 4, Jul - Aug. pp-2098-2101