A Brief Review on an Audio Steganography with LSB and Security Enhancements

Vinita Bhimte[1], Prof. Jeetendra Singh Yadav[2]

[1]*M.Tech Scholar,* [2]*Guide*

Department of Computer Science and Engg. Bhabha Engineering and Research Institute, Bhopal

Abstract-Recently the trading of data over the Internet wound up essential. it has turned out to be essential to utilize stowing away and encryption mechanics to keep up the security and privacy of information as it go over the system. Utilizing Steganography, you can insert a mystery message inside a bit of unsuspicious data and send it without anybody knowing the presence of the mystery message. In a general sense, audio Steganography is the workmanship and study of covering up computerized information, for example, instant messages, fundamentally, and parallel documents into audio records, for example, WAV, MP3, and RM documents. The output audio document is known as the transporter record and is the main middle of the road to be sent to the recipient.

Keyword- Steganography, Least Significant Bit, MP3, Cryptography.

I. INTRODUCTION

Information is shared globally through the Internet, in digital form. There are issues and challenges regarding the security of information in transit from senders to receivers. The major issue is the protection of digital data against any form of intrusion, penetration, and theft. The major challenge is developing a solution to protect information and ensure their security during transmission. Three components of information security are confidentiality, integrity, and availability. Confidentiality ensures that information is kept secret from any unauthorized access. This could be done through information hiding techniques, namely cryptography and steganography.

Cryptography involves the act of encryption and decryption of a digital data. The major weaknesses of such techniques are that even though the message has been encrypted, it still exists. Steganography dwells on concealing any digital data in an innocuous digital carrier; the word steganography is derived from an old Greek word which means covered writing.

Concept of Steganography

The general steganography system as: First, create a message on the cover media. The second, a stego message is created by hiding a secret message placed on the cover via message using a stego message, and then the receiver get the stego message from the channel that not secure. Lastly, a pre agreed stego key are uses for extracts secret message when receiver already receive the message.

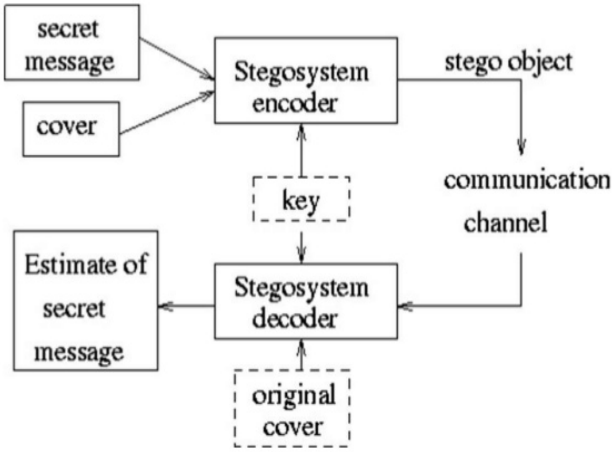

Figure 1.1 Basic Diagram of Steganography.

Steganography is one of the two techniques used for covert communication. However, watermarking is the second technique that can embed watermark into host cover to keep copyright for the hosts. Steganography typically establishes point-to-point data security. The strength of steganographic technique, in keeping the data in the carrier medium against attacks or alteration is weak during transmission, storage or format conversion is weak.

Steganography is an ancient art that has been reborn in recent years; this art hides the idea that there is communication happening. Here the aim is to have a communication channel that is convert between two parties, the two channel existence is to be hidden to a possible attacker. Steganography basically, takes single piece of information and then hides the information within another computer file (sounds recordings, images, and texts) containing insignificant or unused areas of data. It takes the advantage of the areas, where it replaces them with information. These files can later be transported or sent without anyone getting to know what really is inside it.

Cryptography

Cryptography is art and science of keeping messages secure. it is the practice and study of techniques for secure communication in the presence of third parties. Cryptography protects information by transforming it into unreadable format. Only those who possess a secret key can decipher the cipher text into plain text. Where different keys are used for encryption and decryption. In asymmetric or public-key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public.

In Cryptography systems following terms are used.

• Plaintext is message or data which are in their normal, readable form.

• Encryption: Encoding the contents of the message in such a way that hides its contents from outsiders.

• Cipher text: encrypted plaintext

• Decryption: The process of retrieving the plaintext back from the cipher text.

II. MP3 AUDIO STEGANOGRAPHY

Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

Steganography audio is the improvement of science from stenography. The audio document can be utilized to shroud data or mystery messages. audio Steganography strategies can implant any messages in MP3 sound records. The steganography of audio, mystery messages are embed into computerized audio signal which comes about into modifying parallel succession of comparing audio documents. The essential model of steganography on sound comprises of transporter (Audio document), message and watchword. Bearer or normal called a cover document, which stores private data.

The information revolution is the key technology in which the information has been gathered, processed and distributed as an interface between users, and many of the offices in this world. The development of communication makes the source of information to be more valuable and content with active speed like the International Network (Internet). The security issue is the main requirement for every system or protocol, which deals with information.

One of the methods used to compress audio to digital form is MP3; it tries to consume the minimum space possible, and at the same time keeps the quality of the audio with as good as possible. This method in this area is one of the best achievements.

Least Significant Bit Steganography Technique

Basically, the computer was created due to binary numbers, known as two numbers, namely 0 and 1. Both of these numbers are often referred to as bits. Then, these bits will continue to form a composite sequential and binary structure into a set of information. Set of information is composed of 8-bit or often referred to as 1 byte. A Steganography method is admirably secure only when the statistics of the cover information and the stego information are similar with each other. In other words it conveys the meaning that the relative entropy between the cover information and the stego information is zero. The LSB embedding technique suggests that data can be hidden in such a way that even the naked eye is unable to identify the hidden information in the LSBs of the cover file.

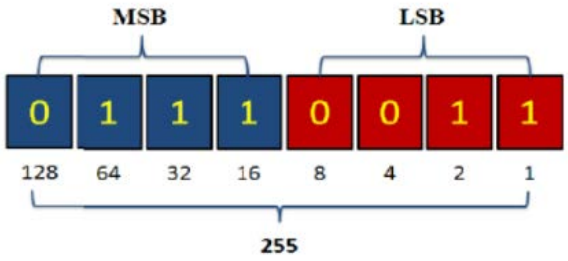

Fig. 2.1 Bit Representation in LSB.

Least Significant Bit (LSB) is part of the binary data row that has the lowest value and is located to the right of the bits. LSB is the opposite of MSE (Most Significant Bit), which is the bit that has the highest value in the binary sequence. For the example there are as follows. The easiest way to embed secret information within the cover file is called LSB insertion. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used, then the quantity of modification will be small.

The compressed encrypted secret message are taken. Then the encrypted secret data has to be converted into binary format. Binary conversion is done by taking the American Standard Code of Information Interchange values of the character and converting them into binary format and generating stream of bits.

III. LITERATURE SURVEY

Sr. no.	Title	Author	Year	Approach
1	An evaluation of MP3 steganography based on modified LSB method	R. Indrayani, H. A. Nugroho and R. Hidayat	2017	it. This paper aims to determine the maximum limit of adding bits and its effects on audio quality based on modified LSB method consisting of LSB+1, LSB+2 and LSB+3.
2	LSB-steganography framework for stereoscopic images based on BJND	L. R. Noriega-Galeana, R. Reyes-Reyes, V. Ponomaryov and C. Cruz-Ramos	2017	This paper proposes a new method to hide information into stereoscopic images using a LSB-Steganography technique and a Binocular Just Noticeable Difference model (BJND) embedding the maximum payload capacity avoiding visual artifacts and inaccurate 3D generation
3	A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution	M. Kalita and T. Tuithung	2016	This paper presents a novel steganographic method based on Least Significant Bit (LSB) substitution and 8-neighboring Pixel Value Differencing (8nPVD) for gray scale image in order to improve the embedding capacity with an imperceptible stego image.
4	An enhanced and secure image steganographic technique using RGB-box mapping	T. Bedwal and M. Kumar	2013	This paper presents a new algorithm to hide a RGB image in another RGB image based on LSB insertion technique. The concept of mapping is applied on RGB images for making it more secure.
5	A Steganography Method for AAC Audio Based on Escape Sequences	Y. Wang, L. Guo, Y. Wei and C. Wang	2010	An information hiding method on escape sequences of Huffman coding which can embed a great deal of secret information into AAC files is proposed based on the research of AAC coding standard.
6	LSB-based Audio Steganography Method Based on Lifting Wavelet Transform	M. Pooyan and A. Delforouzi	2007	In this paper we present a novel method for digital audio steganography where encrypted covert data is embedded into the wavelet coefficients of host audio signal

R. Indrayani, H. A. Nugroho and R. Hidayat [1] Least significant bit (LSB) is one of the classical methods commonly used for steganography audio. Because of its simplicity, many researchers have interested to develop it. This paper aims to determine the maximum limit of adding bits and its effects on audio quality based on modified LSB method consisting of LSB+1, LSB+2 and LSB+3. Then, this method is evaluated by counting steganography capacity, peak signal to noise ratio (PSNR) and bit error rate (BER) values. Evaluation results show that LSB+3 has the best performance by obtaining the maximum bit of steganography capacity and acceptable of PSNR value.

L. R. Noriega-Galeana, R. Reyes-Reyes, V. Ponomaryov and C. Cruz-Ramos [2] Nowadays, stereoscopic images are commonly used for 3D image generation, these are composed by a pair of images viewed independently by each eye, which creates a feeling of immersion and in depth perception. 3D vision technologies have multiple applications in many different areas such as medicine, entertainment, computer vision, etc.; being accessible to a wider group of people. However, there is so few researches that seek to hide information in this type of 3D content. This paper proposes a new method to hide information into stereoscopic images using a LSB-Steganography technique and a Binocular Just Noticeable Difference model (BJND) embedding the maximum payload capacity avoiding visual artifacts and inaccurate 3D generation. Results demonstrate that it is possible to embed up to 1.87 Mb into the stereoscopic images keeping high imperceptibility, obtaining average values for PSNR and SSIM between the original stereoscopic pair and the modified of 31.12 dB and 0.9693, respectively. Quantity Bad Pixels (QBP, δd= 0. 5) and SSIM are calculated for evaluating accurate 3D generation, obtaining average values of 41.26% and of 0.7721 between the ground-truth and the disparity map of the modified stereoscopic pair.

M. Kalita and T. Tuithung [3] This paper presents a novel steganographic method based on Least Significant Bit (LSB) substitution and 8-neighboring Pixel Value Differencing (8nPVD) for gray scale image in order to improve the embedding capacity with an imperceptible stego image. The proposed method partitions the cover

image into some 3×3 non-overlapping pixel blocks in row major order. k-bits of the secret bit stream are embedded in the center pixel of the block using modified LSB substitution. The difference between the center pixel and 8-neighboring pixels are employed to find out the number of bits that can be embedded in the difference value. The method divides the gray levels [0-255] into five different continuous ranges. The number of bits to be embedded is calculated from the range table. The experimental results show that the proposed method has a higher embedding capacity and Peak Signal to Noise Ratio (PSNR) value of the stego image against the cover image. This work also presents a comparison of the embedding capacity and PSNR value of the proposed method with the existing scheme.

T. Bedwal and M. Kumar [4] Image steganography is a technique of masking secret information (e.g. text, image, audio, video etc.) in a cover image in order to protect the information from being modified or destroyed. Owing to its simplicity and hiding capacity, Least Significant-Bit (LSB) insertion in spatial domain techniques is a very popular approach of hiding information in a cover image. This paper presents a new algorithm to hide a RGB image in another RGB image based on LSB insertion technique. The concept of mapping is applied on RGB images for making it more secure. Two different key-boxes for each channel are used for mapping. Each of these two key-boxes for a channel have 4 different values which are used to map the pixel values of that channel of secret image to 3 LSB bits of corresponding channel of cover image. The proposed method provides extra security as without the knowledge of mapping technique, it is not possible to extract the secret information. Further, the hiding capacity is good and the quality of stego-image is improved by using fewer number of LSB bits for hiding the secret information.

Y. Wang, L. Guo, Y. Wei and C. Wang [5] An information hiding method on escape sequences of Huffman coding which can embed a great deal of secret information into AAC files is proposed based on the research of AAC coding standard. The proposed algorithm first unpacks the cover AAC file to search for the escape sequences, and then modifies least significant bit (LSB) of the escape sequences with the approach of matrix encoding, to improve the embedding efficiency. This method is low in computational complexity without any changes of the length of AAC coding. Experimental results reveal that the proposed algorithm can achieve higher hidden data capacity for AAC audio at the bitrate of 128kbps or above, furthermore, it has good imperceptibility and can resist the steganalysis to some extent.

M. Pooyan and A. Delforouzi [6] In this paper we present a novel method for digital audio steganography where encrypted covert data is embedded into the wavelet coefficients of host audio signal. To avoid extraction error we use lifting wavelet transform. For using the maximum capacity of audio signals, we calculate hearing threshold in wavelet domain. Then according to this threshold data bits are embedded in the least significant bits of lifting wavelet coefficients. Inverse lifting wavelet transform is applied to modified coefficients to construct stego signal in time domain. Experimental results show that proposed method has large payload, high audio quality and full recovery.

IV. PROBLEM IDENTIFICATION

Audio steganography is an efficient method to secure embedded data and sent it through internet. Unfortintully the integrity message method is not focuses in steganography technique as well as LSB technique is not introduced encrypted method before embedding secret message. this work introduces the development of an advanced Bi Least Significant Bit (Bi- LSB) MP3 audio steganography method to addresses the security problems of LSB. Furthermore, an integrity part is added at the receiver to ensure the integrity messages is received correctly or not.

V. CONCLUSION

In this survey paper we can study of MP3 steganography based on modified LSB methods. One of the techniques, that is utilized to conceal data in audio records, is LSB. In this strategy, the bits of a message are put away in cover successively which makes it simple for assailants to separate the concealed message. In this study LSB has been enhanced by utilizing hopping methods to store bits of message in cover without influencing the cover estimate. The new LSB technique upgrades the estimation of PSNR more than Standard LSBs. This makes the new technique fruitful in the realm of sound Steganography.

Steganography can be used a large amount of data formats in the digital world of today. The most popular data formats are .bmp, .doc, .gif, .jpeg, mp3, .txt and .wav. Steganography technologies are a very important part of the future of Internet security and privacy on open systems such as Internet.

REFERENCES

[1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, 2017, pp. 257-260.

[2] L. R. Noriega-Galeana, R. Reyes-Reyes, V. Ponomaryov and C. Cruz-Ramos, "LSB-steganography framework for stereoscopic images based on BJND," 2017 14th

International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, 2017, pp. 1-6.

[3] M. Kalita and T. Tuithung, "A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution," 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), Bratislava, 2016, pp. 1-5.

[4] T. Bedwal and M. Kumar, "An enhanced and secure image steganographic technique using RGB-box mapping," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 385-393.

[5] Y. Wang, L. Guo, Y. Wei and C. Wang, "A Steganography Method for AAC Audio Based on Escape Sequences," 2010 International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, 2010, pp. 841-845.

[6] M. Pooyan and A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform," 2007 IEEE International Symposium on Signal Processing and Information Technology, Giza, 2007, pp. 600-603.

[7] Feruza, Y., & Kim, T. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering, 2(2), 17¬32.

[8] Neeta, D., Snehal, K., & Jacobs, D. (2006). Implementation of LSB Steganography and Its Evaluation for Various Bits. International Conference on Digital Information Management. 173¬178

[9] Francia, G. A., & Gomez, T. S. (2006). Steganography Obliterator: An Attack on the Least Significant Bits. Information Security Curriculum Development Conference. 85-91

[10] Sivathanu, G. Wright, C. P and Zadok, E. (2005). Ensuring Data Integrity in Storage: Techniques and Applications. a report submitted to Stony Brook University

[11] Santosa, R. and Bao, P. (2005). Audio to image wavelet transform based audio steganography. Proceeding of 47th International Symposium, ELMAR, pp. 209- 212

[12] Cvejic, N., & Seppanen, T. (2004). Reduced Distortion Bit-Modification For LSB Audio Steganography. International Conference on Signal Processing.3. 2318-2321

[13] Dunbar B. (2002). “A detailed look at Steganographic Techniques and their use in an Open Systems Environment”, SANS Institute.