An Extensive Literature Review on Audio Steganography Methods

Madhuri Kumari[1], Prof. Komal Tahiliani [2]

[1]M.tech. Scholar, [2]Guide

Department of Computer Science & Engineering, School of Research & Technology, People's University, Bhopal (M.P.)

Abstract- In this ever changing and evolving environment, establishing secure communication is an important objective for researchers. Communication of secret information is a critical factor in information technology that continues to create challenges with increasing levels of sophistication. When communication takes place between peoples that are located on the same secure network, these challenges can be considered as manageable. In these situations where the involved parties are spatially separate, the security of secret information cannot rely only on the advanced technologies of secure networks, and additional security mechanisms should be incorporated. Steganography is the ability of hiding messages inside an image file/Audio file or a Video file such that the very existence of the message is unknown to third party. Cryptography is used to encrypt the data so that it is unreadable by a third party. Such techniques will facilitate various secret information sharing strategies. In this examination and extensive survey of literature of MP3 Steganography Based on Modified LSB Method has been reported.

Keywords- Steganography, Cryptography, Image Encryption, LSB Method, Information Hiding.

I. INTRODUCTION

Information is shared universally through the Web, in computerized shape. There are issues and difficulties in regards to the security of information in travel from senders to collectors. The real issue is the assurance of computerized information against any type of interruption, entrance, and robbery. The significant test is building up an answer for ensure information and guarantee their security amid transmission. Three parts of information security are privacy, trustworthiness, and accessible. Privacy guarantees that information is kept mystery from any unapproved get to. This should be possible through information hiding systems, to be specific cryptography and steganography. Cryptography includes the demonstration of encryption and decryption of a computerized information. The significant shortcomings of such methods are that despite the fact that the message has been scrambled, regardless it exists. Steganography harps on disguising any computerized information in a harmless advanced transporter; the word steganography is gotten from an old Greek word which implies secured composing.

Steganography is an old workmanship that has been reawakened as of late; this craftsmanship conceals the possibility that there is communication happening. Here the point is to have a correspondence channel that is changing over between two gatherings, the two channel presence is to be covered up to a conceivable assailant. Steganography essentially, takes single snippet of information and afterward shrouds the information inside another PC document (sounds accounts, images, and messages) containing irrelevant or unused territories of information. It takes the benefit of the zones, where it replaces them with information. These records can later be transported or sent without anybody becoming more acquainted with what truly is inside it.

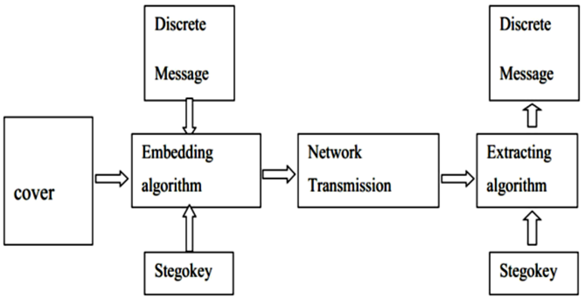

Fig. 1.1 The Basic Steganography Model.

Steganography is worried about techniques for guaranteeing that mystery message is embedded (which can be serial number or a clandestine communication or a copyright check) in a cover message (like a sound chronicle or a video film, or significantly PC code). Parameterization of the embedding is finished by a key; without the learning of presence of this key. It is hard for an outsider to expel or identify the embedded material, when cover protest has material embedded in it, this is called stego question. For example, it may implant a content in a cover image or a stamp in a cover content to give or giving a stego-image or stego content, and soon.

In a stego framework that is impeccable, the stego image isn't being discernable from the first cover. A cover can without much of a stretch distinguish and after that perhaps remake the message. So as to maintain a strategic distance from coincidental reuse, both receiver and sender ought to wreck all spreads they as of now have utilized for exchange of information.

Electronic communication is liable to capture attempt and mediation, particularly amid the Information Age. With regards to issues of security and protection, a great many people's first idea would turn towards encryption. By and large, just the planned beneficiary would have the capacity to decode the message. The thought is that regardless of whether somebody caught a scrambled message, the message would be absolutely garbled. The field of cryptography is an all around created field sponsored by an orderly scientific establishment. Then again, sending an encoded message is a barefaced demonstrate that the message was intended to just be shared between particular gatherings. Steganography exhibits an approach to secretively exchange a message between planned gatherings with nobody else thinking about it. Steganography will enable somebody to shroud messages in harmless protests with a specific end goal to maintain a strategic distance from location. The capacity to conceal messages can be exceptionally significant in territories where an encoded message may draw undesirable consideration. Just as cryptanalysis is utilized to check cryptography, so too is steganalysis used to neutralize steganography. So as to build up any great security conspire, one must invest energy and exertion endeavoring to break said plot. The requirement for steganalysis turns out to be more articulated when a gathering presumes another gathering would have motivation to transmit messages clandestinely.

II. TYPES OF STEGANOGRAPHY

Almost all advanced interactive media records - content, image, sound, video and convention can be utilized as cover mediums for Steganography to conceal mystery information .yet the organizations that are more appropriate are those with a high level of excess. Excess can be characterized as the bits of a question that give exactness far more prominent than would normally be appropriate for the protest's utilization and show. The excess bits of a question are those bits that can be adjusted without the modification being identified effortlessly. Image and sound documents particularly follow this necessity. Figure 2.1 demonstrates the four primary classifications of document arranges that can be utilized for Steganography.

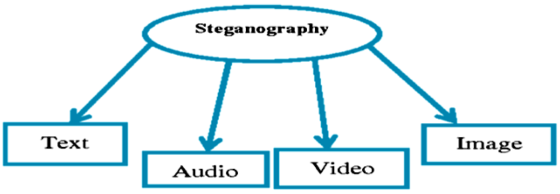

Fig. 2.1 Types of Steganography.

a. Text Steganography

Hiding information in content is the most essential technique for Steganography. The technique was to shroud a mystery message in each n th letter of each expression of an instant message. In the wake of blasting of Web and diverse kind of advanced record designs it has diminished in significance. Content stenography utilizing computerized records isn't utilized regularly on the grounds that the content documents have a little measure of repetitive information.

b. Image Steganography

Images are utilized as the prevalent cover objects for Steganography. A message is embedded in a computerized image through an embedding algorithm, utilizing the mystery key. The subsequent Stego image is send to the beneficiary. On the opposite side, it is prepared by the extraction algorithm utilizing a similar key. Amid the transmission of stego image unauthenticated people can just notice the transmission of an image however can't figure the presence of the shrouded message.

c. Audio Steganography

Audio stenography is concealing, which abuses the properties of the human ear to shroud information unnoticeably. A capable of being heard, sound can be unintelligible within the sight of another louder perceptible sound .This property permits to choose the divert in which to conceal information.

III. PRIOR WORK

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	This examination work 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	An approach towards novel video steganography for consumer electronics	M. C. Sushmitha, H. N. Suresh and J. Manikandan	2017	In this work, a novel attempt is made to conceal a secret video in a cover video using the concepts of steganography and discrete wavelet transform, thus achieving the best of both worlds.

3	Performance evaluation parameters of image steganography techniques	A. Pradhan, A. K. Sahu, G. Swain and K. R. Sekhar	2016	This work illustrates the various performance evaluation parameters of image steganography techniques. The performance of a steganographic technique can be rated by three parameters; (i) hiding capacity, (ii) distortion measure and (iii) security.
4	Enhancing security of images by Steganography and Cryptography techniques	S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar	2016	This examination provides a technique for the protection of image in open wireless channel. It depends on steganography and cryptography (double random phase encoding).
5	Photographing-decodable steganography by use of a high-frame-rate LED display	M. Takahashi and H. Yamamoto	2015	This work reported a kind of steganography that features decoding by photographing an LED screen. Our proposed steganography employs a high-frame-rate LED display to embed a secret image in successive 4 fields that are changed at 480 Hz.
6	Performance evaluation of LSB and LSD in steganography	D. Yadav, M. Agrawal and A. Arora	2014	In this work implemented and discussed the performance evaluation of Least Significant Bit (LSB) and Least Significant Digit (LSD) on various formats of multimedia data.
7	Performance evaluation of feature-based steganalysis in steganography	D. Majercak, V. Banoci, M. Broda, G. Bugar and D. Levicky	2013	The objective of this examination is performance testing of Feature-based Steganalysis methods for detection of steganography tools that are used for hiding a secret message in still images.

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 research work 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.

M. C. Sushmitha, H. N. Suresh and J. Manikandan [2] Videos have proven themselves to be the best medium to demand consumer attention. This has motivated the sharing of videos on Whatsapp, Facebook and other social media. Consumer electronics such as mobile phones, tablets and laptops are mainly used for video sharing. In this research work, a novel attempt is made to conceal a secret video in a cover video using the concepts of steganography and discrete wavelet transform, thus achieving the best of both worlds. Also, the proposed work is extended towards concealing two secret videos in a single cover video. The performance evaluation of proposed technique is reported in the research work. It is observed that the reconstructed videos have PSNR ranging from 74.30-90.12 dB and the PSNR of stego videos ranges from 68.66-70.80 dB. It is also observed that both, stego videos and reconstructed secret videos are visually indistinguishable from the original video.

A. Pradhan, A. K. Sahu, G. Swain and K. R. Sekhar [3] This research work illustrates the various performance evaluation parameters of image steganography techniques. The performance of a steganographic technique can be rated by three parameters; (i) hiding capacity, (ii) distortion measure and (iii) security. The hiding capacity means the maximum amount of information that can be hidden in an image. It can also be represented as the number of bits per pixel. The distortion is measured by using various metrics like mean square error, root mean square error, PSNR, quality index, correlation, structural similarity index etc. Each of these metrics can be represented mathematically. The security can be evaluated by testing the steganography technique with the steganalysis schemes like pixel difference histogram analysis, RS analysis etc. All these metrics are illustrated with mathematical equations. Finally, some future directions are also highlighted at the end of the research work.

S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar [4] this research work provides a technique for the protection of image in open wireless channel. It depends on steganography and cryptography (double random phase encoding). In this method primary step is to cover a message image inside an another image through steganography to make a stego image and then a simple encoding technique; double random phase encoding (DRPE) is perform on stego image. For the evaluation of proposed technique, statistical tests like entropy, time analysis and peak to signal noise ratio (PSNR) with and without noises (Gaussian, salt n pepper and speckle) are performed which illustrate that the proposed technique provide better security to the transmitted image in wireless channel than the other techniques.

M. Takahashi and H. Yamamoto [5] author propose a kind of steganography that features decoding by photographing an LED screen. Our proposed steganography employs a high-frame-rate LED display to embed a secret image in successive 4 fields that are changed at 480 Hz. Author have investigated display sequences of the encoded images by changing the exposure time of a camera. Experimental results show the displayed sequence that contains three black secret images is the most decodable with a single shot. Furthermore, Author has conducted a photographing-decodable steganography by using a higher frame rate LED display that shows full-color images at 960 Hz. Experimental results show the displayed sequence that contains fifteen secret images is the most decodable with a single shot. In addition,authorfound that the 960-Hz LED display performs a higher decoding rate and shorter exposure time than the 480-Hz LED display.

D. Yadav, M. Agrawal and A. Arora, [6] In this work author have implemented and discussed the performance evaluation of Least Significant Bit (LSB) and Least Significant Digit (LSD) on various formats of multimedia data. Author have shown the performance variation on different formats for which these two techniques have been applied to hide the messages. Implementation of both the algorithms has been done to explore the security and distortion level in different formats. Based on the implementation and exhaustive testing of the methods on documents, it was found that they help in proper hiding of messages so that it is not recovered by the intruder during the transfer of data from sender to the receiver.

D. Majercak, V. Banoci, M. Broda, G. Bugar and D. Levicky [7] The objective of this examination is performance testing of Feature-based Steganalysis methods for detection of steganography tools that are used for hiding a secret message in still images. Many of those tools, which can be used publicly, cause statistical changes in original images during embedding process. The features represent those statistically calculated changes, where feature extraction in this examination was applied in spatial domain and also directly in transformation domain of DCT in JPEG files what helps to obtained relevant statistical data. The results of this examination identify the selection of statistical feature vector that is used during training phase of classifier in order to distinguish between cover and stego image. The reliable detection of selected steganography methods were presented in relation to length of feature vector. Moreover, contribution to design of blind steganalysis system was proposed for the purpose of unveiling a secret communication via completely new steganography methods.

IV. PROBLEM STATEMENT

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 converting 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. Audio steganography is an efficient method to secure embedded data and sent it through internet. This study introduces the development of an advanced Least Significant Bit (LSB) MP3 audio steganography method to addresses the security problems of LSB. The security quality is still challenge for encryption and decryption of media data.

V. CONCLUSION

In this examination work an extensive literature review on evaluation of MP3 steganography based on modified LSB method has reported. 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, enables to insert a secret message inside a bit of non secret data and send it without anybody knowing the presence of the secret message. In a general sense, audio Steganography is the workmanship and study of covering up computerized information, for example, text messages, fundamentally, and parallel formats into audio records, for example, WAV, MP3, and

RM files. The output audio document is known as the transporter record and is the main middle of the road to be sent to the recipient.

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] M. C. Sushmitha, H. N. Suresh and J. Manikandan, "An approach towards novel video steganography for consumer electronics," 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Bangalore, 2017, pp. 72-76.

[3] A. Pradhan, A. K. Sahu, G. Swain and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques," 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), Bangalore, 2016, pp. 1-8.

[4] S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 531-534.

[5] M. Takahashi and H. Yamamoto, "Photographing-decodable steganography by use of a high-frame-rate LED display," 2015 14th Workshop on Information Optics (WIO), Kyoto, 2015, pp. 1-3.

[6] D. Yadav, M. Agrawal and A. Arora, "Performance evaluation of LSB and LSD in steganography," 2014 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), Noida, 2014, pp. 515-520.

[7] D. Majercak, V. Banoci, M. Broda, G. Bugar and D. Levicky, "Performance evaluation of feature-based steganalysis in steganography," 2013 23rd International Conference Radio elektronika (RADIOELEKTRONIKA), Pardubice, 2013, pp. 377-382.

[8] Y. Zheng, F. Liu, C. Yang, X. Luo and K. Zhao, "Identification of Steganography Software Based on Core Instructions Template Matching," 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, 2011, pp. 494-498.

[9] K. Alla and R. S. R. Prasad, "A New Approach to Hindi Text Steganography Using Matraye, Core Classification and HHK Scheme," 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, 2010, pp. 1223-1224.

[10] S. Sarreshtedari, M. Ghotbi and S. Ghaemmaghami, "One-third probability embedding: Less detectable LSB steganography," 2009 IEEE International Conference on Multimedia and Expo, New York, NY, 2009, pp. 1002-1005.

[11] Boulis, A. et al. (2003) Aggregation in Sensor Networks: An energy-accuracy trade-off. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications.

[12] Castelluccia, C., Mykletun, E. and Tsudik, G. (2005) Efficient Aggregation of Encrypted Data Wireless Sensor Network, Proc. ACM/IEEE Mobiquitous, San Diego, CA.