# An Extensive Survey on Evaluation of Steganography Techniques

Priyanka Sharma[1], Dr. Amit Shrivastava[2], Dr. Kapil Chaturvedi[3]

*[1]M.tech. Student, [2]Guide and HOD, [3]Co-Guide*

*Department of Computer Science and Engineering, SIRT-S, Bhopal*

***Abstract- Most of today's steganographic systems use multimedia objects such as picture, audio, video, etc. as cover media because users frequently transmit digital images via email and other Internet communication or network packet level. There are so many important parameters to keep in mind while learning and applying steganographic models. Robustness, capacity and security are the significant steganographic parameters to be considered. This examination work presents an extensive survey of literature on evaluation of Steganography techniques based on LSB and latest trends in Steganography techniques are discussed for information security enhancement.***

***Keywords- Information Hiding, Steganography, LSB, Encryption, Secure Communication.***

## I. INTRODUCTION

In recent times, the need for digital communication has increased dramatically and as a result, the Internet has become essentially means more effective and faster communication to digital communication. At the same time, data on the Internet has become susceptible to copyright infringement, espionage, piracy, etc., which therefore requires secret communication. As a result, a new domain dedicated to information security has evolved and is known as data hiding. Steganography is a relatively novel addition to the area of data hiding but traces its origin to long ago in history.

The term steganography derives from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing". In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data.

A basic block diagram of steganographic model is depicted in Fig. 1.1. The information is inserted in a cover image by the stegonographic encoder, which may employ a key or password. Here the concept of symmetric key steganography having both side the same key (K1) is used. .Now the produced stego image is transmitted to the receiver and it is decoded by using the same key to get back the original message. As the stego image is carried over channel, it may be viewed by unintended persons but stego image will behave like an innocent medium without showing the hidden message inside it.

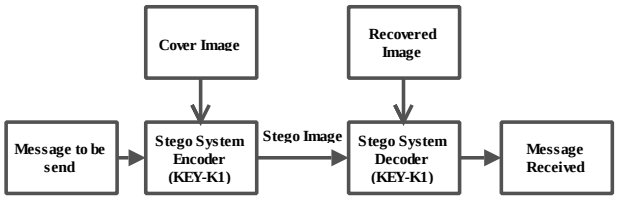



Fig.1.1 Basic block diagram of Steganography system

Steganography employs medium such as image, audio, video, or text file to conceal any information in it, so that does not draw any interest and looks like an innocuous medium. Cover medium such as digital image, video and photo became the obvious choice. Stego media are the media, which contain the secret information while cover media are the plain file. Recently, the images have been a popular choice as a means to cover mainly because of its redundancy in the representation and the ability to penetrate applications in daily life. Over the years, many algorithms have been proposed to hide data in images and developing new algorithms are a topic of current research. In this examination, some of the most popular and effective among image steganography algorithms are analyzed for their mechanisms, advantages and disadvantages, which could be a valuable guide for future research scope openings.

- Text Steganography: - hiding information in text file is the most common method of Steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.
- Image Steganography: -Images are used as the popular cover medium for Steganography. A message is embedded in a digital image using an

embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message.

- Audio Steganography:- Audio Steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. 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. Existing audio Steganography software can embed messages in WAV and MP3 sound files.
- Video Steganography: - Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.
- Protocol steganography:- the term protocol Steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

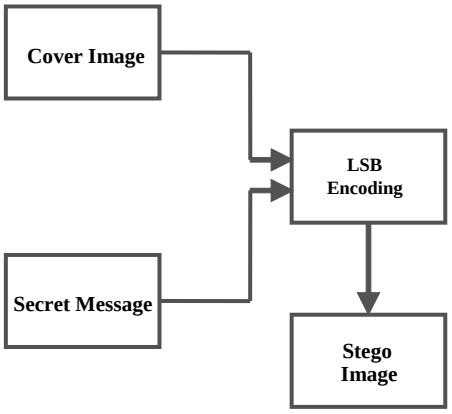
## II. LSB TECHNIQUE

This is the acronym used for least significant bit technique. Images consist of pixels. These pixels can be represented in binary format. This binary representation will have 0 or 1. So changing the least significant bit will either add 1 or subtract 1 to that pixel value. This change is so small that the result of change cannot be recognized by human eyes. So taking images as cover medium for Steganography can use LSB technique to hide any secret image or secret text data inside the cover image. In colour images there are 24 bits in each pixel while in gray images there are 8 bits in each pixel. In colour image each pixel consists of RGB components containing 8 bits each. So if using colour image as cover image have 3 bits per pixel to hide data while 1 bit for gray images. The extraction of secret message from the cover image is done using the LSB extraction method which is just the reverse one of the insertion method.

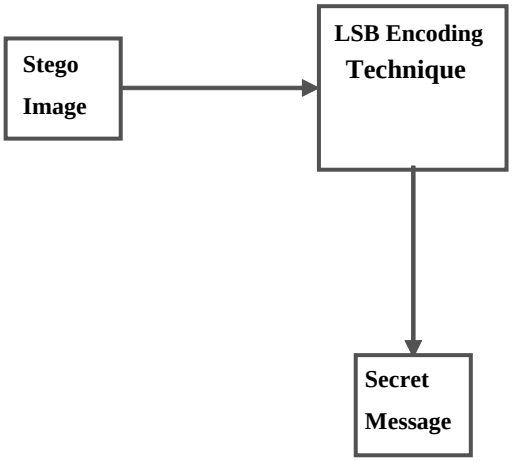
*a. Secret Message Embedding using LSB*

Input: Cover image, Secret message Output: Stego image

(i) Convert the secret message into corresponding binary encoded bit string
(ii) Measure the length of the binary string
(iii) Take the pixel values from gray images
(iv) Change the 8th bit of the pixel according to the binary string message
(v) Repeat step 3 and 4 binary string length times
(vi) Put the terminating symbol
(vii) Get the Stego image




(a) LSB Embedding Technique




(b) LSB Extracting Technique

Fig. 2.1 LSB embedding and extraction

*B. Secret Message Extraction using LSB*

Input: Stego image Output: Secret Message

(i) Extract the pixels from stego image.
(ii) Find the 8th bit value and store it in binary bit string
(iii) Repeat step 1 and 2 until terminating symbol found
(iv) Convert the binary bit string into character string and find secret message

## III. LITERATURE REVIEW

| 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 Efficient Audio Steganography Technique to Hide Text in Audio | S. P. Rajput, K. P. Adhiya and G. K. Patnaik | 2017 | This work introduces the new efficient audio steganography technique where two data bits of secret message are embedded at the time on LSB positions of carrier audio based on the compliment of 3 MSBs of carrier audio |
| 3 | A new approach to hide data in color image using LSB steganography technique | Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta and M. N. Islam | 2017 | A technique which adds double layer security to hide data in image using LSB algorithm, AES-128 encryption and a new approach of choosing index of image pixel are reported |
| 4 | A proposed implementation method of an audio steganography technique | M. Tayel, A. Gamal and H. Shawky | 2016 | Audio steganography uses different algorithms, but (LSB) least significant bit is applied in this examination. The quality of sound is depended on the size of the audio which the user selects and length of the message |
| 5 | Survey on steganography methods (text, image, audio, video, protocol and network steganography) | P. Johri, A. Mishra, S. Das and A. Kumar | 2016 | Here authors are discussing various types of steganography methods in this survey work |
| 6 | Applying AWGN MP3 Steganography Attack in BiLSB and SLSB Techniques | M. M. Salih and M. S. Atoum | 2015 | This examination aims to compare between two techniques SLSB and BiLSB to privew which one is more secure |
| 7 | The MP3 steganography algorithm based on linbits, | Yakun Dong, Ru Zhang, Jianyi Liu, Chenlei Cao and Di Xiao | 2014 | This work presents an improved LSB (Least Significant Bits) Steganography algorithm based on linbits by analyzing the structure of MP3 bitstream and the characteristics of the linbits of MP3 encoding |

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 examination 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.

S. P. Rajput, K. P. Adhiya and G. K. Patnaik [2] Information security is the biggest challenge in recent digital communication era. Audio steganography is one of the information security techniques, which hides secret data in audio media. The traditional LSB based Audio steganography techniques are easy to implement but suffers from low embedding rate and low robustness. This examination introduces the new efficient audio

steganography technique where two data bits of secret message are embedded at the time on LSB positions of carrier audio based on the compliment of 3 MSBs of carrier audio. In proposed work, two algorithms have been proposed. In Proposed Algorithm-I two data bits of secret message are embedded at a time on LSB positions of carrier audio based on the 3 MSBs of carrier audio and in Proposed Algorithm-II those two data bits are embedded on LSB positions of carrier audio but based on the compliment of 3 MSBs of carrier audio. Proposed Algorithm-I improves the embedding capacity by embedding two data bits at a time and Proposed Algorithm-II increases the robustness against attacks, because in conventional algorithms the embedding of the secret bit value is in linear fashion, therefore a hacker can easily extract the secret message. As complement operation is used in Proposed Algorithm-II extraction of data bits from complement 3 MSB's is not that much of easy than extraction of data bits from traditional algorithm. Moreover, additional security is provided with the help of secret key without knowing the valid secret key it is difficult to access the data.

Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta and M. N. Islam, [3] With the advancement of information technology, almost everything in this digital world evolves with information and data. The importance of security and secrecy of data is also increasing enormously. Steganography presents the practice of hiding data or information in any sort of cover medium, e.g image, audio, video. In most of the existing procedures, with the exposure of the keys intruders get successful in picking their required bits. The objective of this examination is to propose and implement a tool for increasing the secrecy of data transmission using steganography. In this examination, firstly authors have proposed a technique which adds double layer security to hide data in image using LSB algorithm, AES-128 encryption and a new approach of choosing index of image pixel. Secondly, authors have developed a steganography tool using our proposed technique. Finally, authors have evaluated the performance of the proposed technique using Mean Square Error (MSE) method, Peak Signal to Noise Ratio (PSNR) and by measuring payload capacity. A comparative analysis of the developed tool with the some existing tools has showed that our tool performs better comparing with some other tools.

M. Tayel, A. Gamal and H. Shawky [4] Steganography is the art of science dealing with hiding secret data inside image, audio, video or text files. In audio steganography; secret message is embedded in the digital sound by slightly altering the binary sequence of the sound file. Existing audio steganography software deal with WAV, AU, and even MP3 sound files. Embedding secret messages in the digital sound is usually a more difficult process than embedding messages in other forms, such as digital images. Audio steganography uses different algorithms, but (LSB) least significant bit is applied in this examination. The quality of sound is depended on the size of the audio which the user selects and length of the message.

P. Johri, A. Mishra, S. Das and A. Kumar, [5] The growth of sharing information on the internet has arises the problem of security of digital data over the network. Steganography is a technique which protects the fact of concealment of message within a cover media i.e. it makes the secret message invisible for any unintended recipient. If anyone notices the secret information within the cover file then steganography is failed. Here authors are discussing various types of steganography methods.

M. M. Salih and M. S. Atoum [6]Steganography is considered as an advanced emerging method due to its ability to ensure secured data transmission based on embedding the required secret data in digital multimedia files. The most appropriate mediums for steganography is audio files because of its high rates of data transmission and high redundancy level. Various steganography methods have been introduced to ensure the transmission of data in a secured way. Nevertheless, some of those methods, such as the Standard Least Significant Bit (SLSB) technique have some problems concerning the verification of attacks in the secret messages. Thus, this examination aims to compre between two techniques SLSB and BiLSB to privew which one is more secure. The performance of the developed technique is evaluated based on Additive white Gaussian noise (AWGN) with two variance values, 0.3 and 0.5 bits/sec/Hz to the extracted messages and comparing the performance of this technique with that of the SLSB technique based on hiding the same secret message in the same cover messages. Results demonstrated that the Bi-LSB technique outperforms the SLSB one in terms of PSNR values with and withut adding the attack. In addition, there is a noticed degredation after adding the noise, where the percentage of the degredation is higher for noise with 0.3 variance than that with 0.5 variance for both techniques, Bi-LSB and SLSB.

Yakun Dong, Ru Zhang, Jianyi Liu, Chenlei Cao and Di Xiao [7] This examination presents an improved LSB (Least Significant Bits) steganography algorithm based on linbits by analyzing the structure of MP3 bitstream and the characteristics of the linbits of MP3 encoding. The algorithm is improved by considering the distribution of MP3 frequency coefficient and the selection of block type in MP3 decoding. Experimental results show that the algorithm keeps transparency and has good real-time performance. In addition, it has high steganographic

capacity with low complexity and is easy for embedding and extraction.

## IV. PROBLEM STATEMENT

Constantly communicated through the Internet are flows of information generated from many diverse applications such as e-commerce transactions, audio and video streaming or online chatting. The security of such data communication, which is required and vital for many applications nowadays, has been a major concern and ongoing topic of study given that the Internet is by design open and public in nature. Many techniques have been proposed for providing a secure transmission of data. Data encryption and information hiding techniques have become popular and generally complement each other. The general idea of hiding secret information in media has a wider range of applications that go beyond Steganography. Due to the high proliferation of digital images and the high degree of redundancy present in digital images, there is an increased interest in the usage of images as the cover object in Steganography. The Least-Significant-Bit (LSB) technique is one of the most widely used scheme for image Steganography. This technique involves the modification of the LSB planes of the images. Desirable modification in LSB improves the performance of Steganography in terms of robustness and security.

## V. CONCLUSION

In this research work an extensive survey of literature has reported various recent works in the field of Steganography. The approaches proposed by various authors are examined based on their advancement and drawbacks. The various kinds of Steganography strategies are transform domain, spread spectrum, substitution, distortion and statistical systems and cover generation methods. Substitution systems replace the LSB (least significant bits) of every pixel in the cover file with bits from the secret document. The transform domain technique hides secret information in the transform space (like frequency domain) by modifying the least significant coefficients of the cover file. Most of the present Steganography frameworks utilize interactive media objects like video, audio, images and so on as cover media since individuals regularly transmit digital pictures over email and other Internet communication. Current Steganography approaches provide the opportunity of hiding data into digital multimedia media files.

## 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]. S. P. Rajput, K. P. Adhiya and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-6.

[3]. Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta and M. N. Islam, "A new approach to hide data in color image using LSB steganography technique," 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), Khulna, 2017, pp. 1-6

[4]. M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, 2016, pp. 180-184

[5]. P. Johri, A. Mishra, S. Das and A. Kumar, "Survey on steganography methods (text, image, audio, video, protocol and network steganography)," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2906-2909

[6]. M. M. Salih and M. S. Atoum, "Applying AWGN MP3 Steganography Attack in BiLSB and SLSB Techniques," 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, 2015, pp. 62-67

[7]. Yakun Dong, Ru Zhang, Jianyi Liu, Chenlei Cao and Di Xiao, "The MP3 steganography algorithm based on linbits," ICINS 2014 - 2014 International Conference on Information and Network Security, Beijing, 2014, pp. 134-151

[8]. H. B. Kekre, A. Athawale, B. S. Rao, and U. Athawale, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding," in 2010 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 196-201

[9]. R. Sridevi, A. Damodaram, and S. Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security," Journal of Theoretical & Applied Information Technology, vol. 5, 2009

[10]. M. S. Atoum, M. Suleiman, A. Rababaa, S. Ibrahim, and A. Ahmed, "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III," Journal of Computer Science, vol. 11, pp. 184-188, 2011

[11]. B. Datta, P. Pal, and S. K. Bandyopadhyay, "Robust multi layer audio steganography," in 2015 Annual IEEE India Conference (INDICON), 2015, pp. 1-6

[12]. K. Srinivasan, V. Ramamurthi, and K. S. Chatha, "A technique for energy versus quality of service trade-off for MPEG-2 decoder," in IEEE Computer society Annual Symposium on VLSI, 2004, 2004, pp. 313-316