IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 5, May 2024

A Novel Method of Hiding Audio Signal into Color Image using LSB Substitution

Shital Nivas Shinde[1], Komal Laxman Nikam[2], Bhagyashri Sampat Shinde[3],
Dr Arjun Ramchandra Nichal[4]
Students, Department of E&TC[1,2,3]
Associate Professor, Department of E&TC[4]
Adarsh Institute of Technology and Research Centre, Vita, India

Abstract: *Data security means protective digital privacy measure that are applied to prevent unauthorized access to computers, huge database and online data it is also protect data from security. Steganography is focuses on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is is used to hide the message and prevent the detection of hidden message. Various modern technique of steganography are: a) Video steganography b) Audio steganography. information. The propose method is to hide secret information and image behind the audio and video file respectively. Steganography, a method of concealing secret data within various media carriers, has gained prominence due to advancements in computational power and increased security awareness. This paper introduces novel techniques based on LSB manipulation and redundant noise inclusion for data hiding in images and audio. Experimental results demonstrate the effectiveness and imperceptibility of these methods. Evaluation parameters such as transparency, robustness, and capacity are crucial for assessing steganography techniques. Image steganography methods are categorized into spatial and transform domain techniques, with the latter offering higher robustness. LSB-based steganography methods, including LSBR and LSBM, manipulate pixel bits to hide data, while variants like LSB MR enhance capacity. Ongoing research aims to strike a balance between capacity, robustness, and transparency in steganography techniques*

Keywords: Steganography, LSB substitution, Image processing, Secret Key, etc

I. INTRODUCTION

Steganography technique employs a key ad a media called cover data. To hide the secret data. The main objective of a steganography method is to hide the sender, the receiver, and the content of the secret data. Which makes the secret data visible only to the receiver The steganography word is originally derived from two Greek words. Stego means hidden and grafia means writing steganography is a method to transfer secret data embedded withincover data through a public communication channel such as a Internet.in these methods an attacker cannot extract the secret data from the cover data. There are three important parameters for evaluating a secret data communication technique. Namely, capacity, robustness, and transparency. Increasing these three parameters raises the confidentiality of the data communication technique. However, increasing all these three parameters simultaneously is a very daunting task. Audio signal are used in this method as the cover to hide secret data. This embedment alters the binary sequence of the used file. This is a more difficult task when compared to image and text steganography. Audio steganography can be done using different method such as least significant bit encoding, phase coding and spread spectrum. This method hides the data in WAV, AU, and even MP3 sound files Information technique is a new kind of secret communication technology. Them majority of today information hiding systems uses multimedia objects like audio. Embedding secret message in digital sound usually a more different process. Varieties of technique for embedding information in digital audio have been established. In these paper we will attend the general principle of hiding secret information using audio technology and an overview of functions and technique. In order to improve the data hiding in all types of multimedia data formats such as image and audio and to make hidden message imperceptible. A novel method of steganography is introduced in these paper. It is based on Least Significant Bit [LSB]manipulation and inclusion of redundant noise as secret key in message. These method is applied to data hiding in images. For data hiding in audio, discrete cosine transform(DCT)and discrete wavelet transform(DWT) both are used. Also the algorithm tested for various number of bits. For those values of bits. Mean square error(MSE) andpeak signal to noise ratio(PSNR) are calculated and plotted

II. STRUTURE

- Embedding Process
- Extraction Process

III. OBJECTIVE

- Terrorists can also use audio data hiding to keep their communication secret and to coordinate attack.
- It is used for forensic application for inserting hidden data into audio file.
- In the business world audio data hiding can be used to hide a secret chemical formula or plans for new invention.
- Audio data hiding can be used anytime you want to hide data.

IV. LITERATURE REVIEW

R. Indryani, H. A. Nugroho, and R. Hidaka, [31] Least significant bit (LSB) are one of the classical methods commonly used for steganography audio because of its simplicity, many research errs have been interested to develop it. This investigation aims to determine the maximum limit of adding bits and its effects on audio quality based on the modified LSB method consisting of LSB□ 1, LSB□ 2, 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 accepted PSNR value. [1]

Vardhan, M. Vishnu, B. Rama Krishna." IWT Based Data. In Encrypted Images." 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE,2018. Steganography methods are expected to exhibit some levels of perceptual Invisibility. Hence, several visual quality metrics are used to determine the visual Quality measures of a stenographic process and most of the ones used are MSE, PSNR, SSIM, Q index matrices. Here, the cover image is modelled using a feature Extractor lightweight encryption method that can protect secret data in a cost Effective manner. [2]

Saini, Ravi, Kamal deep Joshi, and Rainu Nandal." An Adapted Approach of Image Steganography Using Pixel mutation and Bit Augmentation. "Analysis and detection attacks used in literature to evaluate the stenographic schemes. [3]

Kadhim, I. J., and Halloran, B. (2019). Comprehensive Survey of image steganography: Techniques, Evolutions, and trends in future Research. Neurocomputing, 335, 299-326. The introduction of ranges of visual Artifacts by stenographic schemes during an embedding process causes some Unusual variations in the features of the stego-image, such as imperceptibility. Such variations are exploited during steganalysis to detect the presence of secret Data. There are two common methods for steganalysis which are passive and Active steganalysis. during passive steganalysis, the aim is to identify the Presence or absence of the secret data or the embedding process. [4]

Dhawan, Sachin, and Rashmi Gupta. " Analysis of Various data security techniques of steganography: A survey. "Information Security Journal: A Global Perspective 30.2 (2021): 63-87. If any steganalysis Reveals and presence of hidden bits inside the embedded digital object, the basic Aim of steganography is defeated. These is another way of protecting the existing stenographic techniques from steganalysis. most of the modern steganalysis Methods deploy the method of computing the specific features of the cover and stego- images. [5]

Sharma & Thakur [34] noted that in the present scenario of extensive mediums for communication technologies, it has always been a challenging task to ensure the confidentiality of the sensitive information that is transmitted over a secured channel. They also noted that amongst various reliable and efficient techniques to secretly exchange information, audio steganography is considered very promising. The study then proposed a Random Key Indexing method to replace the LSBs of the carrier audio with a secret message. The bit replacement is guided by a primary key that is provided by TTP (Trusted Third Party) and a secondary key that will be generated at the encoder end during the embedding process and is supplied to the decoder end. The proposed method also uses message retrieval code that adds another layer of protection to the process. The method is successfully tested on various 32-bit & 16-bit stereo wave files with different payloads. The SNR dB values came out in the range of 139 dB to 142 dB for 32-bit and 67 dB to 85 dB for 16- bit stereo files. The Bit Error Rate (BER) was in the range of 0.23 to 0.32 % for 32-bit and 0.018 to 0.028 % for 16-bit files.[6]

Datta & Bandyopadhyay [32] stated that the embedment of secret "data in the same LSB position of consecutive samples help intruders to easily extract the hidden information. So, they proposed the introduction of a robust audio steganography technique for hiding secret data in multiple layers of randomly chosen LSB and in non-consecutive samples to improve the robustness and strength of the process. They solved the problem of data hiding at non-contiguous sample locations which causes loss of the capacity of stego audio by proposing the hiding of three bits in a target sample. They also increased the capacity by using "6 bits ASCII representation of the secret message" rather than 7. To evaluate the proposed technique, the authors embedded texts of different payloads in the cover audio and made comparisons with the other embedding methods in terms of capacity and" quality [7].

Abdelsatir & Abushama [35] proposed a new spatial domain-based audio steganography method using a transparent LSB matching approach. The scheme was evaluated using standard algorithms and other audio steganography tools. The proposed scheme achieved better transparency rates than the comparative tools based on image LSB matching methods. The hidden information in the proposed method also left no evidence of steganography use during the subjective listening tests; hence, there was no detectable auditable noise in the host audio signal. [8]

Binny & Koilakuntla [36] presented a stenographic method for text embedding in audio using LSB based algorithm. In this method, each audio sample is transformed into bits before embedding the text data. The first step of the embedding process is the conversion of the message character into the corresponding binary before using the proposed LSB-based algorithm to do the embedding; this improves the capacity of the stego system. The evaluation of the proposed algorithm was done using metrics like SNR values for different audio inputs. [9]

Al-Bayati & Al-Jarrah [33] presented the Duo Hide as a model for hiding secret data in multimedia files irrespective of the type. The file is processed in an uncompressed form and "divided between two cover images of similar sizes. Before hiding the file in the multimedia file, the media is first split into two parts, one part containing the most significant half-bytes and the other containing the least significant half-bytes. Both parts are hidden in 2 RGB cover images (uncompressed) using a least significant 4-bit replacement method. The two stego images produced are transmitted via different channels to keep them from

being intercepted by an adversary. The secret file is extracted by combining the LSB half-bytes from the two stego files, in this way, the extracted file shares close similarity with the original secret file in terms of structure and content. The evaluation of the proposed Duo Hide system on public multimedia files of different sizes showed that there was a clear and visible difference between the cover and stego images even at the highest embedding ratio." Hence, the proposed Duo Hide model can ensure better security of the secret data because even if an attacker succeeded in intercepting one of the stego images, the information will still be incomplete since the attacker has not captured the other set of data from the other half-byte bits. The use of a pair of stego files also reduces the size of the required stego file by 50%; this avoids the issues surrounding the transmission of large files that cannot be compressed further. The performance of the Duo Hide system, in terms of security, can be enhanced by randomizing the storage locations within the 2 stego images. [10]

V. PROBLEM DEFINATION

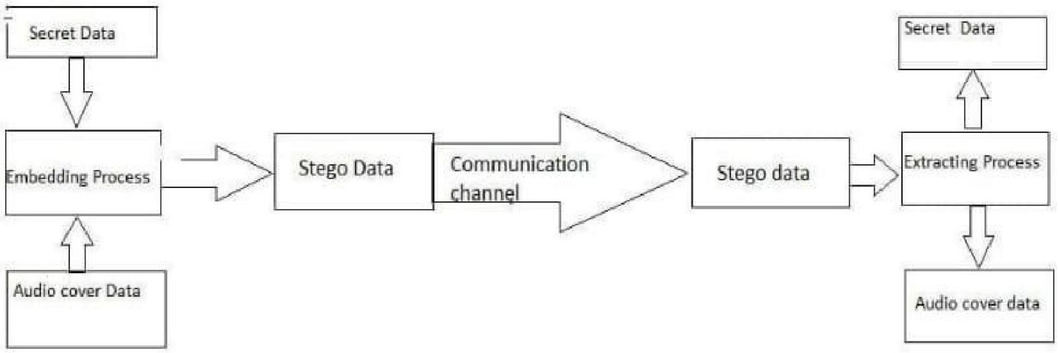
Steganography is an ancient art that has been reborn in recent year; these art hide ideas that there is a communication happening. Here the aim is to have a communication channel that is converting between two parties, the two channel existence is to be hide hidden to a possible attacker. Steganography basically, take a single piece of information and then hide the information within another computer file (sound recording, images, and texts) containing in significant or unused areas of data. It takes the advantages of areas, where it replaces them with information. This file 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. These study introduces the development an advanced least

DOI: 10.48175/568

significant bit (LSB) MP3 audio steganography method addresses the security problem of LSB. The security quality is still challenge for encryption and decryption of media data.

VI. METHODOLOGY

Block Diagram:



Flowchart:

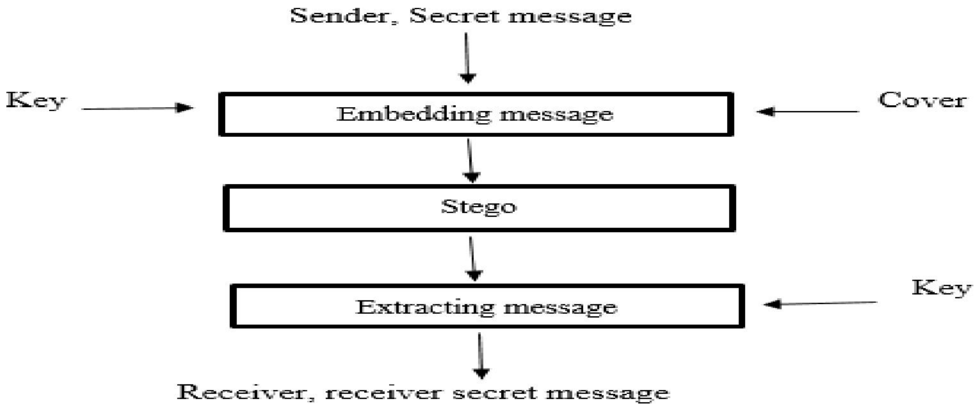


Figure 1 shows the general schema of steganography with the key

Figure 1 shows the general schema of steganography with the key. Todays, due to the wide variety of images, the image is used as a safe enclosure to conceal a message and is referred to as a cover. The image, which is produced after the enclusion of confidential data, is called stego. In steganography methods, we obtain use a key to clutter the message show that the content of the message message won't be discovered clearly if the secret message is compromised or is being exposed. This system consists two modules. The module are as follows:

- Embedding
- Extracting

Now we will discuss above module in detail

Embedding-

First module of our embedding system is hiding audio in image. This method uses LSB coding technique for data hiding in audio. However instead of directly replacing LSBs of digitized sample with the message bit, first check the parity of samples and then carries out data embedding. The process of data embedding are explained as follows:

1. Read the cover audio for signal.
2. Read the audio signal to be embedded its size less than the size of the cover audio signal an convert it into binary sequence of message bit.

3. Depending upon the value of message bit to be embedded (0/1), the LSB of the sample of cover audio signal is modified or unchanged
4. If the message bit to be embedded is 0, then the LSB of the sample of cover audio signal is modified unchanged such that the parity of the sample after embedding of this message bit is even.
5. If the message bit to be embedded is 1, then the LSB of the sample of cover audio signal is modified
6. unchanged such that the parity of the sample after embedding of this message bit is odd.
7. The modified cover audio samples are then return to the file forming the stego audio file.

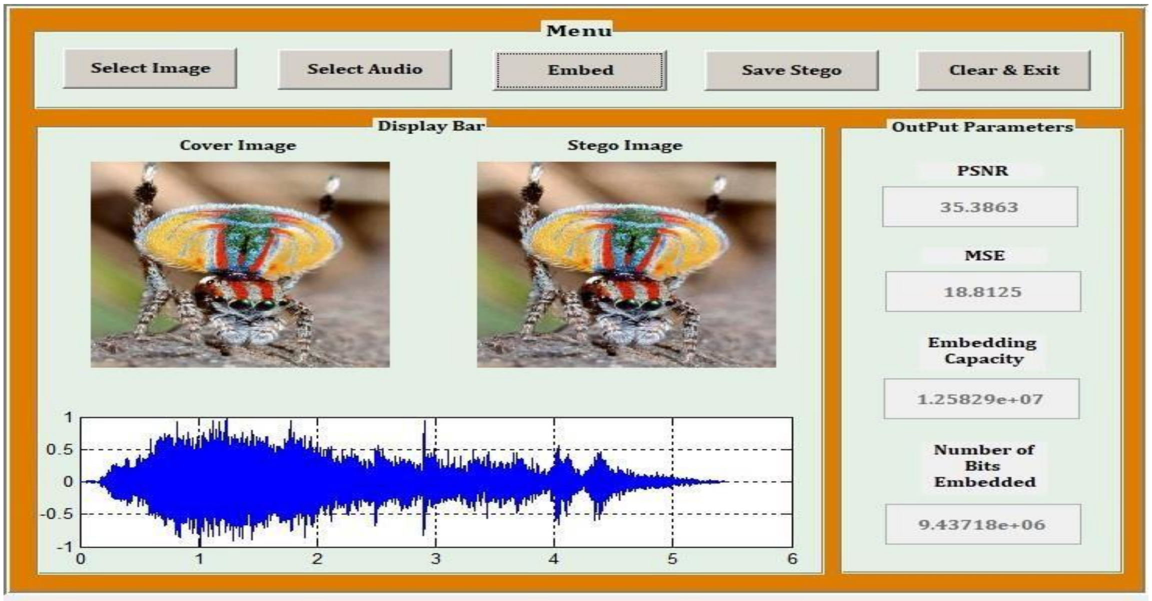
Extracting

In the extracting phase, we only need of perform the mapping function over each group of four coefficients from the received Image as a result, we obtain a secret message. In extracting phase, we perform the following steps;

1. The stego audio file is read.
2. After every such 16 message bit are retrieved, they are converted to their decimal equivalent.
3. We first extract pixels of the cover image based on the key in the embedding phase.
4. We divide the pixels into a set of group with four pixels in each group.
5. We extract secret message according to the four pixel and equation nine for each group.
6. We add the secret message to each other and thus we obtain a bit stream of secret message as the result of these step.
7. Finally, the secret signal is reconstructed

VII. RESULT

Embed



PSNR: 35.3863

MSE: 18.8125

Embedding Capacity: 1.25829e+07

Number of Bits Embedded: 9.43718e+06

Figure 1. Stego Image

Extract

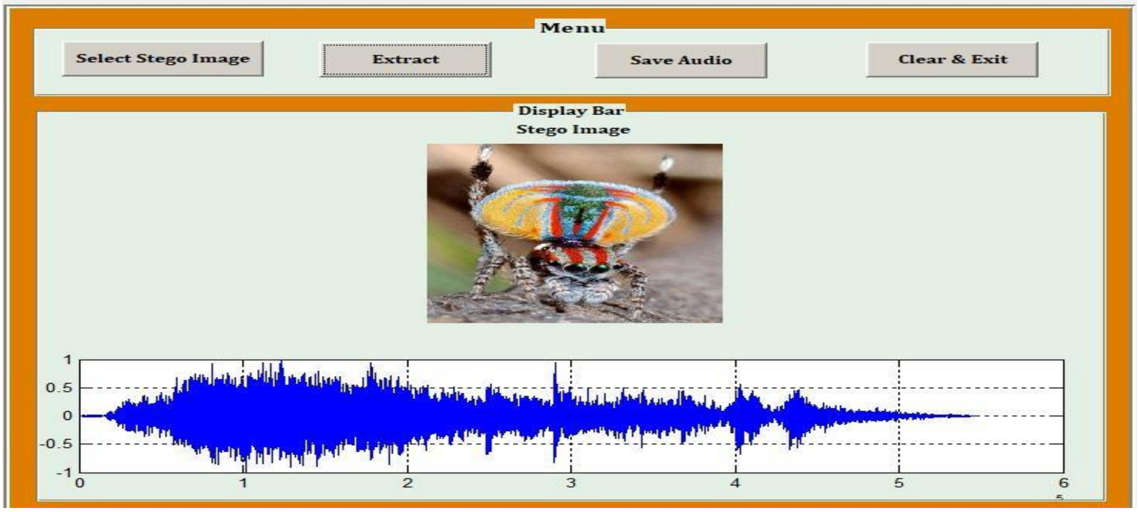


Figure 2. Extract Image

VIII. CONCLUSION

In these examination work and extensive literature review on evolution of MP3 steganography based on modified LSB method has reported. Recently the trading of data over the internet wound up essential. It has turned the 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 secret mes sage inside a bit of non-secret data and send it without any body knowing the presence of the secret message. In a general sense, audio stega nography is the work manship and study of covering up computerized information, for example, Text messages, fundamentally and parallel formats into audio records, for examples, 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. The host signal in the basic version of these methods need to be done, this algorithm has a very small algorithmic delay. This permits the use on these LSB in real time applications. These algorithm is a good basis for stegano graphy application for audio signal and a steganalysis

REFERENCES

[1] R. Indrayani, “An evaluation of MP3 steganography based on modified LSB method.” 2017 International Conference on Information Technology Systems and Innovation (ICTSI), Bandung, 2017, pp. 257-260.

[2] Vardhan, M. Vishnu, B. Rama Krishna, and V. Thanikaiselvan. "IWT Based Data Hiding in Encrypted Images." 2018 Second Intern ational Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2018.

[3] Saini, Ravi, Kamaldeep Joshi, and Rainu Nandal. "An Adapted Approach of Image Steganography Using Pixel Mutation and Bit Aug mentation." Smart Computing Techniques and Applications. Springer, Singapore, 2021. 217-224.

[4] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Eva luations, and trends in future research. Neurocomputing, 335, 299-326.

[5] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." Information Sec urity Journal: A Global Perspective 30.2 (2021): 63- 87.

[6] Sharma, Vipul, and Ravinder Thakur. "LSB modification based audio steganography using trusted third party key indexing method ." 2015 Third International Conference On Image Information Processing (ICIIP).

[7] Datta, Biswajita, Prithwish Kumar Pal, and Samir Kumar Bandyopadhyay. "Multi-bit data hiding in randomly chosen LSB layers an audio." 2016 International Conference on Information Technology (ICIT). IEEE, 2016.

[8] Abdelsatir, El-Tigani B., Narayan C. Debnath, and Hisham Abushama. "A multilayered scheme for transparent audio data hiding. " 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2015.

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

[10] Al-Bayati, Marwa Tariq, and Mudhafar M. AlJarrah. "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images." 2016 9th International Conference on Developments in eSystems Engineering (DeSE). IEEE, 2016.