iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53692

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

A Comparative Study of Steganography Techniques: A Review

Sahil Raj[1], Harsh Tyagi[2], Devansh Mishra[3]
[1, 2, 3]*School of Computing Science and Engineering, Galgotias University, Greater Noida*

Abstract: ***Steganography and Digital Watermarking are two methods of information concealment in which the context can be interpreted as keeping the information hidden or making it subtle. Steganography is a means of disguising an information so that only the person(s) who placed it are aware of its existence. On the other hand digital watermarking is the technique of inserting a symbol of some form into a media file to differentiate it from others. Security authenticationis intended to be permanent, and it is applied by a process that involves changes to the media file. Other parties may be able to see or hide digital watermarking in plain sight. In this paper we are going to review the steganography techniques. This paper will do a whole comparativestudy of different steganography techniques also.***

I. INTRODUCTION

Steganography's goal is to conceal and deliberately mislead. It is a type of covert communication in which messages are hidden using any media. It isn't cryptography because it doesn't encrypt data or require the usage of a key. Instead, it's a type of data suppression thatcan be done in a variety of ways. Data hiding technologies have progressed from limited use to widespread adoption during the last decade. The necessity to preserve important intellectualinformation has spawned a profusion of innovative approaches and technologies for both goodand evil, thanks to the rapid evolution of smart mobile devices. Those that combine hiding methods with cryptography are the most dangerous, as they provide a mechanism to both disguise the existence of hidden information while also offering excellent protection for the information even if the channel is discovered.

II. RELATED WORKS

In the related work of “Image Steganography and it’s recent advances: A review” by authors Nandhini Subhramaniam, Somaya Al-Maadeed and others, they have reviewed the recent advances of steganography techniques. Our review paper aims at presenting a comparative study among all the steganography techniques present till date to help others establishing a better understanding of how it works and which way is most efficient to go with. As with the growing advances in every phase of communication and media, the need to secure information is also increasing. Traditionally where cryptography was most prominently used to encrypt data for security reasons, steganography has overcome the disadvantages that are linked with cryptography. Like we say encryption and decryption are the cryptographic mechanisms used,but when the attacker seizes the data and decrypts it anyhow then out data is at risk then. Any confidential information, which is why, is considered more safe with steganography as it makes the information undoubted for a hacker to pay attention on.

Steganography and it’s techniques:

Steganography is the art and science of encoding secret messages in a cover message so that no one save the sender and intended recipient suspects the message's presence. The various kinds of methods of steganography are:

1) *Text steganography:* It is the practise of concealing information within text files. It entails modifying the format of existing text, changing words within a text, producing random letter sequences, and constructing intelligible writings using context-free grammars. The following are some of the approaches used to hide data in text: Method based on format Statistical and Random GenerationLinguistic Approach
2) *Image Steganography:* Image steganography is the process of concealing data by using the cover object as an image. Because the digital representation of an image contains a large number of bits, photographs arecommonly employed as a cover source in digital steganography. There are numerous methods for concealing information within an image. The following are some examples of common approaches:

Masking and Filtering of the Least Significant Bit InsertionEncryption using Redundant Pattern Encoding
Encrypt and scatter
Coding and Cosine Transformation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

3) *Audio Steganography:*The secret message is embedded in an audio signal, which changes the binary sequence of therelated audio file in audio steganography. When compared to other methods, such as Image Steganography, hiding secret messages in digital sound is far more challenging. The followingare some examples of audio steganography techniques:

Spread Spectrum

Least Significant Bit EncodingParity Encoding

The data in WAV, AU, and even MP3 sound files is hidden using this method.

4) Video Steganography: You may use Video Steganography to hide any type of data in a digital video format. This kindhas the advantage of being able to store a vast quantity of data and being a moving stream of images and sounds. This is a hybrid of Image Steganography and Audio Steganography. Thereare two types of video steganography: Data is included in uncompressed raw video and then compressed later.Embedding data directly into the compressed data stream.

5) *Network Steganography:* It is the process of embedding data directly into a compressed data stream (Protocol Steganography). It's a method of embedding data within network control protocols like TCP, UDP, and ICMP, which are utilised in data transmission. In several covert channels found in the OSI model, steganography can be used. For example, in the header of a TCP/IP packet, youcan hide information in specific fields that are either optional or not.

By comparing the stego-picture to the cover image, the efficiency of a steganographic methodcan be determined. The efficiency of a technique is determined by a number of elements. Theseare the factors:

a) Robustness: When stego data is subjected to attacks such as linear and nonlinear filtering, sharpening or blurring, random noise insertion, rotation and scaling, croppingor breaking, compression, and so on, the embedded data should not be corrupted.

b) Invisibility: Stego data should be indistinguishable from regular data. There should be no doubt in the minds of any user or software that the stego file contains additionalinformation.

c) Payload capacity: This is the maximum amount of sensitive data that can be stored in the cover data. The goal of the steganographic method is to transport the most amountof confidential data with the least amount of change in the cover data.

d) Peak Signal to Noise Ratio (PSNR): This rate compares the original and stego data for quality. The better the steganographic method, the greater the PSNR value.

e) Mean Square Error(MSE) : The average difference between a reference image and a changed image is denoted as the Mean Square Error (MSE). The lower the MSE, themore effective the steganography method.

A. Steganography Techniques

1) *LSB(Least Significant Bit):* We know that every information consists of binary data which are in the form called bits. Alsothere are two types of bits- the MSB and LSB. MSB stands for most significant bit while LSB stands for least significant bit. This can be understood better with an example

Let us say data bits are 11011010001

So in here the last two or three bits are called the LSB/ Least significant bit while the starting ones are the most significant bits. It is generally according to the way and purpose it follows. For the same reason the LSB are used to hide the secret code of information within images sothat they can be transferred without any suspicion. We know that every image consists of numerous number of pixels which are none other than in the form of data bits. Every image isa combination of colours with different colour models. Let us say the image follows the RGB Colour model.

RGB stands for Red Green Blue colour model and its representation in 8-bits is in the form like:

If image is red then: (255,0,0)

If image is green then: (0,255,0)If image is blue then: (0,0,255)

(0,11111111,0)
And then there is another image.

(0,11111100,0)

In this we can see that both the images are same but there is a difference in second image. In the second image its LSB are changed as a result though it is visible as green and as exactly asprevious one but in place of these LSB we can add our secured data bits to transmit over network safely. As a result only the known authorized user can access the decryption technique to get the hidden message as shown in figure1. In this way image steganography is highly spread over the world.

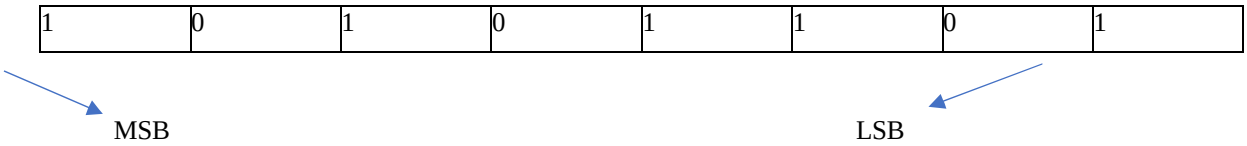


Figure 1.

8 bits of data representing colours; red, green, and blue are preserved for each pixel in a 24bit image file. By substituting the last bit of each 8-bit data with the confidential data bit, data canbe hidden in an image or audio file. Human senses will be unable to detect this shift since it will be so little. The RGB data of two pixels contains 6 bits of data, and the stego-data conversion of the cover data is presented on the right side. There is no discernible change in the cover data.
The cover data are the ones on the left side of the figure 1 if it is expanded two pixels. The RGB data of two pixels contains 6 bits of data, and the stego-data conversion of the cover datais presented on the right side 2.

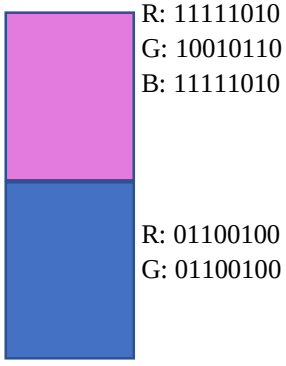


Figure 1

+110101=

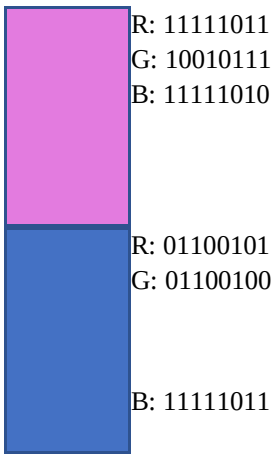


Figure 2

The best rate for LSB coding for audio steganography is 1kbps for 1kHz. To get the digital value of each sample, the cover audio data is sampled first, then digital quantization is performed as illustrated in the figure given below.

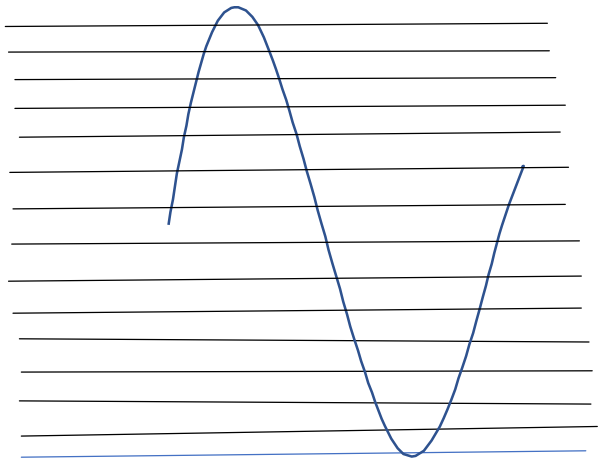


Figure: A sine representation

After quantization, a data can be encoded in the last bit of each of the produced data arrays. When the captured sequence is transformed back to an analogue signal, very slight variations in the stego sound data's amplitude values occur, which are undetectable by the human ear.

2) *Distribute the Spectrum:* This technique makes use of the spread spectrum notion. Confidential data is dispersed over a wide frequency spectrum in this manner. The signal-to-noise ratio in each frequency band should be so low that detecting the presence of data is difficult. Even if many frequency bands'data pieces are destroyed, there will still be enough buried data in the other groups to retrieve. As a result, completely deleting the data without also removing the cover is challenging. This is a highly reliable technology that is mostly utilised in military communications. Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and TimeHopping Spread Spectrum are some of the spread spectrum techniques employed (THSS).
3) *Statistical Methodology:* Confidential info is integrated in the cover by modifying several characteristics of the cover. Itentails slicing the cover into chunks and then inserting a data bit on each of them. Only when the value of the following concealed databit is '1' is the cover block modified; otherwise, no changes are necessary.

B. Technique for Transforming Domains

The cover's transform or frequency domain contains the concealed message. This is a more complicated method of picture transmission concealment. To hide the message in the cover, various methods and manipulations are utilised. The following are examples of conversion domain techniques:

1) Lossless or reversible approach (DCT)
2) Embedding in coefficient bits
3) Discrete Fourier Transformation (DFT)
4) Discrete Cosine Transformation (DCT)
5) Discrete Wavelet Transformation (DWT)

C. Coding for Parity

Parity is a mechanism that is based on bits. A parity bit is a bit that is added at the end of a bitsequence based on whether the sum of the bits is 0 or 1. For example, a 7-bit binary sequence can be converted to an 8-bit data sequence by adding a parity bit. After receiving the data sequence, the receiver side sums the first 7 bits and compares them to the parity bit. If the answer is wrong, the message is garbled during transmission and must be re-requested. Insteadof breaking a signal into distinct samples, steganography parity coding divides it into sample areas and codes each bit from the private message within the parity bit of each region. As a result, the sender has additional embedding possibilities, and the cover data can be changed inan imperceptible way.

D. Encoding of Phases

This approach is applicable to audio signals. The Human Auditory System (HAS) struggles todetect phase shifts and noise in audio signals.

This technique encodes secret signal bits as phase shifts in a digital signal's phase spectrum, resulting in an unnoticed change in signal-to-noise ratio. In a nutshell, this technology chunks the original audio stream or cover file into blocks and embeds the confidential message data sequence in the first block's phase spectrum. The load capacity is quite low because the secret data is only included in the first block. The sensitive data, on the other hand, does not transfer to the cover file, making it immune to attacks like cutting and clipping.

Algorithm in use:

1) Remove the cover data's header section.
2) The remainder of the data is separated into equal segments of the same size as the confidentaldata.
3) Each segment is subjected to the Discrete Fourier Transform (DFT) to create a phase matrix.
4) Private information is added to the first segment's phase vector.

New Phase =

Old Phase + (π/2) hidden message bit=0

Old Phase – (π/2) hidden message bit=1

5) With the new phase value and the first segment's original phase matrix, a new phase matrix is produced.
6) The heading segment is added to the phase matrix that has been constructed.
7) The audio signal is reconstructed using the inverse DFT.

E. Hiding Echoes

Echo concealing is the process of embedding secret data in an audio recording by adding an echo to a distinct signal. It is accomplished by overlaying delayed versions of the signal on top of the original signal. It has the same advantages as the common spectrum approach in that it allows for a high data transmission rate and improved robustness. Only one bit of information can be encoded if only one echo is generated from the original signal. As a result, before the encoding process begins, the original signal is separated into block as shown in figure 1 and 2in detail.The blocks are recombined to generate the final signal once the encoding is complete.

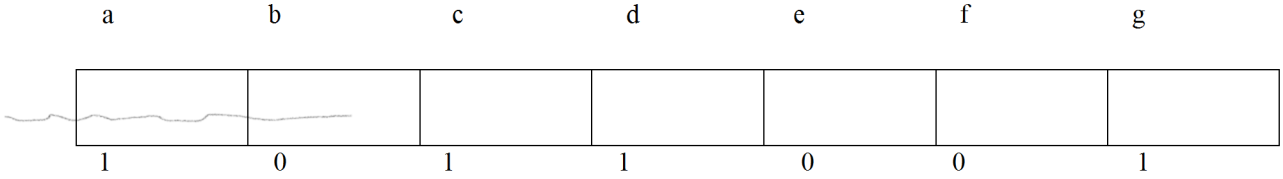


Fig.1 Original audio signal splitted into blocks before hiding the echo

The number of blocks is equal to number of bits in the confidential message and each block isequal in length.

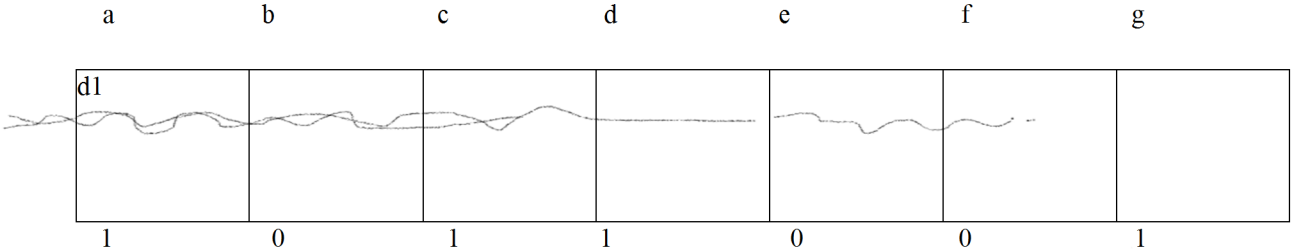


Fig.2 Audio signal in echo hyping process and the bit sequence hidden in the blocks

F. Filtering and Masking

As cover data, this approach simply employs grayscale photographs. Instead of being stored atthe noise level, hidden data is kept in more critical regions. The detection and removal of confidential data is more difficult since it is more integrated into the image.

III. CONCLUSION

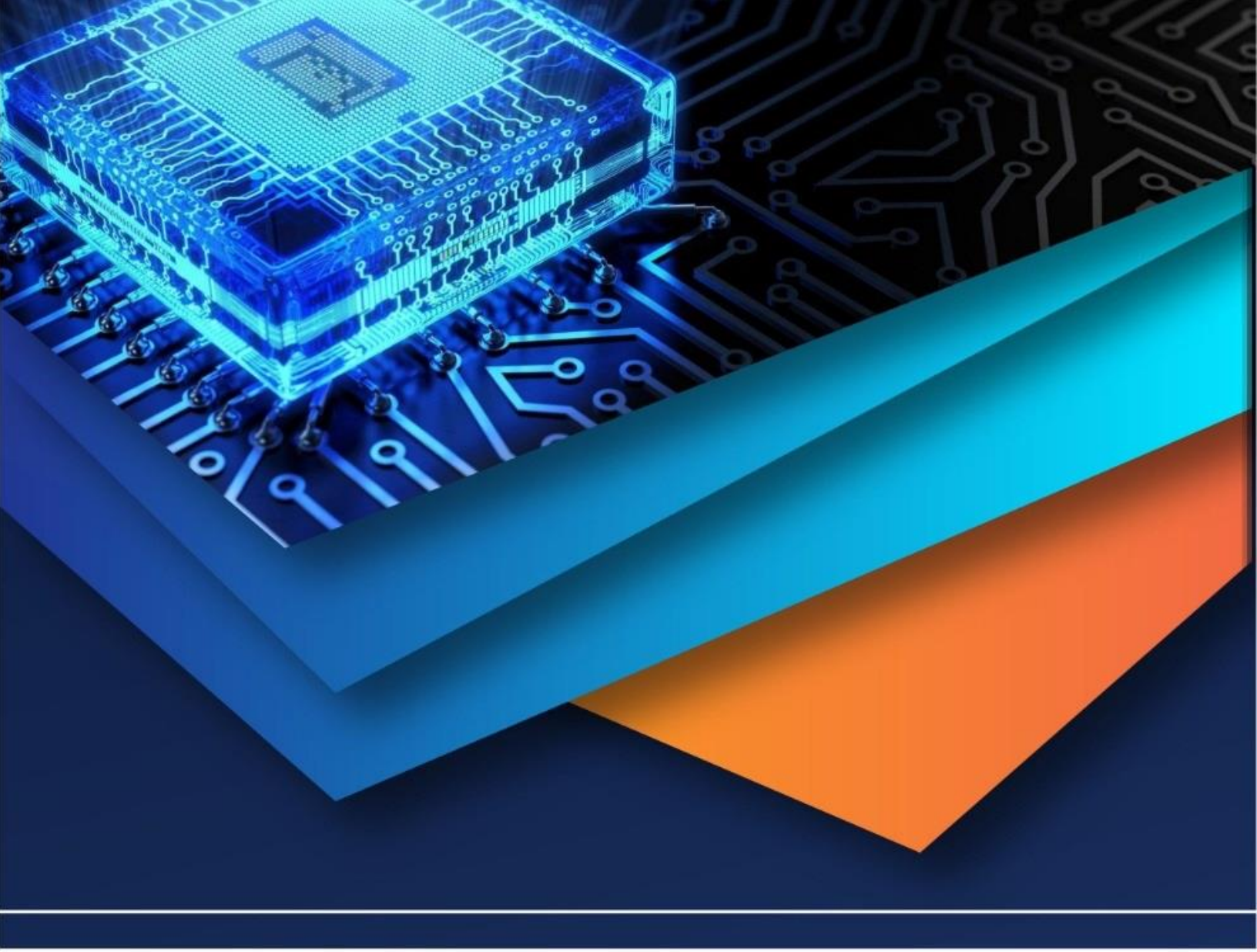
Steganography is the art and science of concealing information within another piece of information. Different steganography approaches are described in this study according on the sort of cover data they are dealing with. The benefits and drawbacks of the described methodsare listed in Table 1:

Technique	Robustness	Imperceptibility	Payload Capacity	Complexity
LSB	LOW	HIGH	HIGH	LOW
Spread Spectrum	MEDIUM	LOW	LOW	MEDIUM
Statistical Technique	MEDIUM	HIGH	LOW	MEDIUM
Transform Domain	HIGH	HIGH	MEDIUM	HIGH
Parity Coding	HIGH	HIGH	LOW	HIGH
Phase Coding	HIGH	MEDIUM	LOW	MEDIUM
Echo Hiding	HIGH	MEDIUM	MEDIUM	MEDIUM
Masking & filtering	LOW	MEDIUM	LOW	MEDIUM

With the current technologies being developed, steganography is becoming more prevalent andsecure. Several criteria, including as the quantity of the data to be embedded, security needs, and the context in which the data will be conveyed, can be used to determine the most acceptable steganography approach. Steganography and cryptography can be used together to meet higher security needs.

REFERENCES

[1] https://ieeexplore.ieee.org/abstract/document/9335027/authors#authors
[2] https://www.tandfonline.com/doi/abs/10.1080/09720529.2021.1962025
[3] https://iopscience.iop.org/article/10.1088/1742-6596/1751/1/012039/meta
[4] https://www.annalsofrscb.ro/index.php/journal/article/view/5779



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY