IPEC Journal of Science & Technology, Vol. 02 (01), June 2023
ISSN: 2583-3286(Online)

Information Hiding Using ImageSteganography

Medhavi Bhardwaj, Arun Kumar, Nikhil Saini, Naveen Kr Varshney, Md. Sadique
Department of Information Technology
Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India

Abstract **The process of hiding data and information is known to be steganography it is done to provide secure communication, in present world there is a demand of sending and displaying data in a hidden format especially when the exchange of information and data is taking place publicly, and this is the reason because of which many methods have been proposed for data and information hiding.**

Keywords: **Data hiding, Digital Image.**

I. INTRODUCTION

The Internet is one of the most popular and the easiest medium for transmission of digital data among people, but one of the common threats during transmission is that anybody can access these data and Internet itself does not provide any protection on these data. [2].
The word Steganography, derived from the Greek word Steganos means covered or secret and graphic means writing or drawing. Its objective is to hide the secret data into some other unsuspected cover media. [3].
Steganography and Cryptography are the main areas of security and information hiding. [4]

II. STEGANOGRAPHY MEDIUMS

There are many Steganography technique listed below.

Image Steganography: To hide the information use of pixel intensities is done, if the cover object taken is image, then it is known as image steganography. A watermark diagram changes the cover of the object (for example, the identity of the owner). In other words, adding a watermark improves the cover source using only additional data. [5]

Video Steganography: Digital video format is used to hide any type of information in video steganography. In this technique for hiding information in images in the video the discrete cosine transform (DCT) adjusts the value which is not conspicuous through human eye. AVI, Mp4, etc video formats are used by video steganography.

Audio Steganography: Audio steganography is one of the most significant medium due to demand of Voice Over Internet Protocol (VOIP). As in this technique audio is chosen for information hiding, that's why it is called Audio Steganography. WAVE, MPEG, etc. digital audio formats are used in audio steganography.
Text Steganography: In this technique, for information hiding, capital letters, white spaces, number of tabs and many others are used.
Network Steganography: In this technique the cover object chosen is as network protocol, such as UDP, ICMP etc and these protocols are used as carrier.

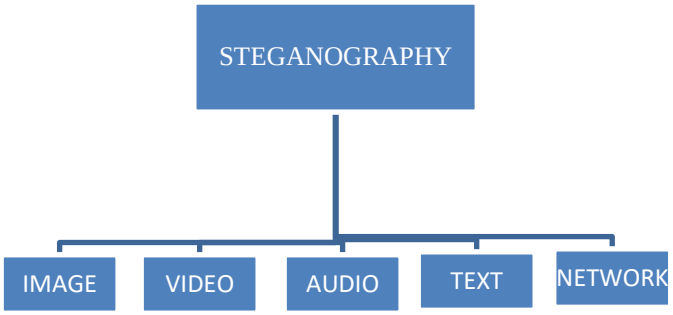


Figure 1 : Different Mediums to achieve steganography

III. PHASES OF STEGANOGRAPHY

For every hidden message exchanging process from sender to receiver, every Steganography algorithm must come through various stages
Sender: The prime objective of the sender is to embed the hidden message in the stego- medium and transmit it through the channel of communication.
Communication channel: A physical or wireless medium that holds an encoded cover picture across the network or some other distribution medium with a hidden.
Receiver: In this steganography process, it is the last stage where the cover medium is retrieved and extracted to see if the hidden text that was sent over the communication channel. [6]

Date of Submission: 01 May 2023
Date of Acceptance :20 June 2023
Corresponding Author: Arun Kumar
(E-mail: 1900300130018@ipec.org.in).

ISSN: 2583-3286(Online)

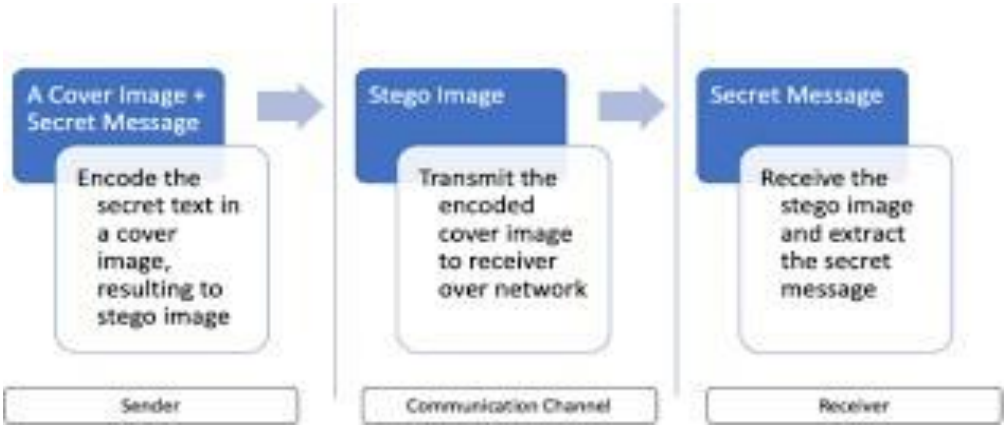


Figure 2: Phases of Steganography

IV. LITERATURE REVIEW

YEAR	AUTHOR	NAME	DESCRIPTION
2015	G. Prashanti and K. Sandhyarani	"A New Approach for Data Hiding with LSB Steganography"	Authors have done survey on a new approach for data hiding using LSB (Least Significant Bit) steganography. The aim of the study is to enhance the security and robustness of data hiding in LSB steganography by using a new embedding algorithm. [7]
2015	M .Nursrati et al.	"Steganography in image Segments using Genetic Algorithm"	They present a method for hiding secret messages in image segments using genetic algorithm (GA) which find optimal location in cover image to hide data efficiently. [8]
2015	Ajaya Shrestha,Arun Timalsina	"Color image steganography technique using daubechies discrete wavelet transform"	In this research, steganography technique using Daubechies Discrete Wavelet Transform (DWT) is implemented. First the cover image is transformed using Daubechies DWT and secret information is embedded in coefficients of Daubechies DWT which gives a stego image. Reverse process is applied to obtain secret information from stego image. The performance of the proposed approach is evaluated using PSNR and MSE. [9]
2015	M. M. Emam, A. A. Aly, and F. A. Omara	"A Modified Image Steganography Method based on LSB Techniques"	The message is expressed in 6 binary bits using the LSBraille method, rather than ASCII format. Three message bits are embedded in one pixel as follows: two bits are embedded in blue layer, and one bit is embedded in the green layer.
2015	Sahar A. El_Rahman	"A Comprehensive Image Steganography Tool using LSB Scheme"	The authors provide a detailed explanation of the tool's architecture and functionality, as well as experimental results that demonstrate its effectiveness

ISSN: 2583-3286(Online)

2015	Indu Nehra, Rakesh Sharma	"Review Paper On Image Based Steganography"	The authors describe the different types of image-based steganography techniques, including spatial domain, frequency domain, and transform domain techniques. [12]
2015	Vipul Shanna and Madhusudan	"Two New Approaches for Image Steganography Using Cryptography"	In this paper tells about the, Chaotic Map-Based Cryptography and Genetic Algorithm for Image Steganography.Discrete Wavelet Transform and Chaos-Based Cryptography for Image Steganography. [13]
2016	Rupali Jain,Jayshree Boaddh	"Advances in digital image steganography"	The paper provides a comprehensive overview of recent advancements in digital image steganography and steganalysis. [14]
2016	Essam H. Houssein,Mona A. S. Ali, Aboul Ella Hassanien	"An image steganography algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System"	This paper proposes an advanced technique for encrypting data using Advanced Encryption System (AES) and hiding the data using Haar Discreet Wavelet Transform (HDWT). HDWT aims to decrease the complexity in image steganology while providing less image distortion and lesser detectability. [15]
2016	Sadaf Bukhari, Muhammad Shoaib Arif, M.R. Anjum, and Samia Dilbar	"Enhancing security of images by Steganography and Cryptography techniques".	Enhancing security of images by Steganography and Cryptography techniques". These studies have explored various steganography and cryptography techniques and their performance in terms ofsecurity and robustness. [16]
2017	Azizah Bt Abdul Manaf1 & Akram M. Zeki	"PSW statistical LSB image steganalysis"	These methods use a range of statistical and correlation-based features to train a classifier that can detect the presence of hidden information in images.is paper proposes an adaptive steganalysis method based on MLE for LSB
2017	Radoslav Forgáč; Roman Krakovský	"Contribution to image steganography using pulse coupled neural networks"	The paper is focused on use of Pulse Coupled Neural Network (PCNN) in the image steganography based on the research in the field of invariant image recognition. [18]
2017	Nishant Madhukar Surse,Preetida Vinayakray-Jani	"A comparative study on recent image steganography techniques based on DWT."	In this paper DWT are used as different transformations for providing a higher security and privacy of the information. [19]
2017	Y.-L. Wang,J.-J. Shen,M.-S. Hwang	"An Improved Dual Imagebased Reversible Hiding Technique Using LSB Matching, International Journal of Network Security"	evaluate the proposed technique's performance using several metrics, including peak signal-to- noise ratio (PSNR), structural similarity index (SSIM).In conclusion, the proposed technique provides an improved and efficient approach for reversible image hiding using LSB matching. [20]
2018	H. Y. Chen, I. S. Fang, and W. C. Chiu	"Self-contained stylization via steganography for reverse and serial style transfer"	The paper introduces a novel method for stylizing images, called self-contained stylization, which uses steganography to embed style information within the image itself. [21]
2018	Wu S., Zhong S., Liu Y.	"Deep residual learning for image steganalysis, Multimedia tools and applications"	The authors propose a residual convolutional neural network (CNN) that consists of several residual blocks. Each residual block includes multiple convolutional layers, followed by a shortcut connection that allows the network to learn residual mappings instead of directly learning the underlying mappings [22].

ISSN: 2583-3286(Online)

2018	Yiwei Zhang, Weiming Zhang,Kejiang Chen, Jiayang Liu, Yujia Liu, Nenghai Yu	"Adversarial examples against deep neural network based steganalysis, In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security"	The paper highlights the vulnerability of DNN-based steganalysis systems to adversarial examples and proposes a method for generating such examples using the FGSM method. [23]
2019	Sahu A. K., Swain G	"Dual Stego-imaging based Reversible Data Hiding using Improved LSB Matching"	The author proposed technique uses two cover images, namely Cover Image 1 (CI1) and Cover Image 2 (CI2), to hide the secret data. The authors use LSB matching to embed the secret data in the cover images. [24]
2019	Hameed M. A., Hassaballah M., Aly S., Awad A. I.	"An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques"	The paper provides an efficient and secure adaptive steganography technique that combines the HOG and PVD-LSB techniques. [25]
2019	Arshiya Sajid Ansari, M ohammad Sajid Moham madi, Mohammad Tanvi r Parvez	"A Comparative Study of Recent Steganography Techniques for Multiple Image Formats"	The paper compares and analyzes recent steganography techniques for multiple image formats, including BMP, GIF, JPEG, and PNG. The aim of the study is to evaluate the strengths and weaknesses of each technique and identify the best-performing techniques for each image format.[26]
2019	I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran,	"Comprehensive survey of image steganography: techniques, Evaluations, and trends in future research"	LSB-based techniques Transform domain techniques Statistical techniques Evaluations:Evaluated based on several factors such as embedding capacity, imperceptibility, robustness, and security Trends in future research: area of research is to increase the embedding capacity of steganographic systems while maintaining the imperceptibility of the stego image. [27]
2020	Srushti S Yadahalli, Shambhavi Rege, Reena Sonkusare	"Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques".	The paper deals with understanding and implementation of steganography on different images using two different techniques: Least Significant Bit method(secret image is hidden using the bits at least significant level of the cover image) and Discrete Wavelet Transform method(secret image is hidden by modification of the wavelet coefficients of cover image). [28]
2020	Adnan Gutub & Maimoona Al-Ghamdi	"Hiding shares by multimedia image steganography for optimized counting-based secret sharing, Multimedia Tools and Applications"	The authors use the least significant bit (LSB) modification technique to embed the shares in the cover images' pixel values. The use of multimedia images for hiding the shares reduces the number of shares required for reconstruction, thus optimizing the CBSS scheme. [29]

ISSN: 2583-3286(Online)

2021	Qu, Z.; Sun, H.; Zheng.M	"An efficient quantum image steganography protocol based on improved EMD algorithm"	The paper "An efficient quantum image steganography protocol based on improved EMD algorithm" proposes a novel quantum image steganography protocol that utilizes an improved Earth Mover's Distance (EMD) algorithm. [30]
2021	Nandhini Subramanian; Omar Elharrouss; Somaya Al-Maadeed; Ahmed Bouridane	Image Steganography: A Review of the Recent Advances	This paper tells about CNN-based image steganography methods and GAN-based image steganography methods. Traditional methods are frameworks which use methods that are not related to machine learning or deep learning algorithms. Many traditional methods are based on the LSB technique. [31]
2022	Wenjie Lin, Xueke Zhu, Wujian Ye, Chin-Chen Chang, Yijun Liu, Chengmin Liu	"An Improved Image Steganography Framework Based on Y Channel Information for Neural Style Transfer"	In this an improved image steganography framework based on Y channel information for neural style transfer. The proposed framework uses the Y channel of the YCbCr color space to hide the secret information. The Y channel contains the luminance information of the image, and it is less sensitive to noise and compression compared to the other two channels (Cb and Cr). [32]
2021	Xinliang Bi, Xiaoyuan Yang, Chao Wang, Jia Liu,	"High-Capacity Image Steganography Algorithm Based on Image Style Transfer"	In this a high-capacity image steganography algorithm based on image style transfer, proposed in the paper "High-Capacity Image Steganography Algorithm Based on Image Style Transfer" [33]
2022	Pratap Chandra Mandal , Imon Mukherjee , Goutam Paul , B.N. Chatterji	"Digital image steganography: A literature survey"	The paper begins by introducing the basic concepts of steganography, including the various types of steganography techniques such as substitution, transform, and spread spectrum techniques for digital image. [34]
2022	Nasro Min-Allah , Naya Nagy, Malak Aljabri, Mariam Alkharraa, ashael Alqahtani ,Dana Alghamdi,Razan Sabri and Rana Alshaikh	"Quantum Image Steganography Schemes for Data Hiding: A Survey"	The authors discuss the various quantum image steganography techniques, such as the least significant qubit (LSQ) method, the quantum-dot cellular automata (QCA) method, and the quantum genetic algorithm (QGA) method. [35]
2022	Noor Alhuda F. Abbas, Nida Abdulredha, Raed Khalid Ibrahim Adnan Hussein Ali	"Security and imperceptibility improving of image steganography using pixel allocation and random function techniques"	The authors evaluate the performance of their proposed technique using various metrics such as peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM), and compare the results with existing techniques. [36]

ISSN: 2583-3286(Online)

V. RESEARCH OBJECTIVE

A. To Develop novel image steganography techniques that can achieve high security and robustness while maintaining low embedding distortion.

B. Develop efficient and secure steganalysis techniques to detect the presence of hidden data in images.

C. Study the applicability of image steganography in different domains such as medical imaging, military, and law enforcement.

D. Exploring the potential applications of steganography in various fields such as forensics, military, and healthcare.

E. Investigate the impact of different image properties such as color space, image size, and format on the embedding and extraction processes.

F. Analyzing the impact of steganography on the storage, transmission, and processing of digital images.

VI. METHODOLOGY

The framework of image steganography refers to the general steps involved in embedding secret information into an image while maintaining the image's perceptual integrity. The framework typically includes the following steps:

i. Image selection: The first step in the framework is to select an appropriate cover image that will be used to hide the secret information. The cover image should be large enough to accommodate the secret message and should not have any noticeable visual changes after the message is embedded.

ii. Message selection: The second step is to select the message to be hidden in the cover image. The message can be any form of digital data, including text, audio, or video.

iii. Embedding: The next step is to embed the message into the cover image using a steganography algorithm. The steganography algorithm should ensure that the message is hidden securely and that the image's perceptual integrity is not compromised. proposing solutions for optimizing their performance and efficiency

Overall, the research objective on image steganography is to advance the state-of-the- art techniques in this field and provide solutions that can enhance the security and privacy of image data.

i. Encryption: In some cases, encryption may be added to the message before embedding to enhance its security. his step involves using a cryptographic algorithm to convert the message into an unintelligible form that can only be decrypted with the correct key.

ii. Steganalysis resistance: To ensure the embedded message is resistant to steganalysis attacks, various steganalysis methods can be applied to detect the presence of a hidden message in the image.

iii. Extraction: The final step is to extract the hidden message from the stego image using a steganography extraction algorithm. The extraction algorithm should be able to retrieve the hidden message without causing any visual changes to the cover image.

The above steps provide a high-level overview of the image steganography framework. The specific details of each step will depend on the steganography algorithm used and the requirements of the specific application.

VII. IMPLEMENTATION

Least significant bit (LSB) : is very simple method to embed data in digital image, audio or video file. The technique works by altering the least significant bits of the pixels in an image, which have little impact on the overall appearance of the image. [37]

For example, consider a grayscale image where each pixel is represented by an 8-bit binary value. The value of each pixel ranges from 0 (binary 00000000) to 255 (binary 11111111). By using the LSB technique, we can replace the least significant bit of each pixel with a bit from the secret message, without significantly altering the appearance of the image. This means that we can hide up to 1 bit of secret data within each pixel of the image.

Here is an example of how the LSB technique can be used to hide the binary message "01010101" within a grayscale image:

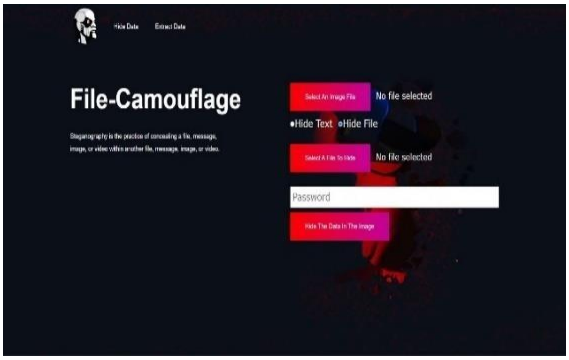
1. Convert the binary message into individual bits: "0 1 0 1 0 1 0 1".
2. Take the first pixel value of the image and convert it into binary. For example, if the pixel value is 187, its binary representation is "10111011".
3. Replace the least significant bit of the pixel value with the first bit of the message. In this case, we replace the last bit of "10111011" with "0", giving us "10111010".
4. Repeat this process for each subsequent pixel in the image, using the next bit of the message each time.
5. Once all the bits of the message have been hidden within the image, the modified image can be sent to the recipient.

ISSN: 2583-3286(Online)

6. The recipient can extract the hidden message by extracting

the LSB of each pixel in the image and combining them into a binary message.

BPCS-steganography (Bit-Plane Complexity Segmentation steganography) Digital steganography can hide confidential data (i.e. secret files) very securely by embedding them into some media data called "vessel data. [38]". The BPCS steganography algorithm works by dividing an image into bit-planes, and then selecting the high complexity bit-planes to hide the secret data. The secret data is then embedded into the selected bit-planes by replacing some of the pixels in the bit-plane with the secret data.



Here is an example of how the BPCS steganography technique can be used to hide a secret message within an image:

1. Select the bit-planes with the highest complexity. This can be done by calculating the complexity measure of each bit-plane and selecting the ones with the highest values.

2. Divide the secret message into binary format and create a bit-stream of the message.

3. Divide the selected bit-planes into non- overlapping blocks. Each block is usually a small square region of the image.

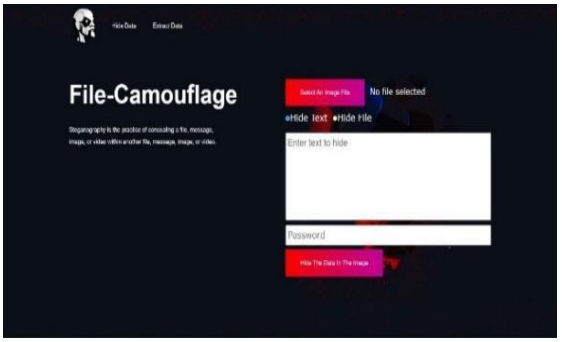
4. For each block, calculate the complexity of the block by comparing it to a reference pattern. If the block has a complexity above a threshold value, then it is considered a candidate block for embedding the secret data.

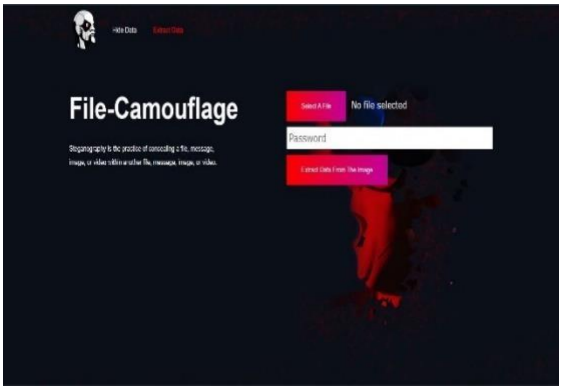
5. In each candidate block, select a number of pixels to embed the secret data.

6. The selected pixels are replaced with bits from the secret message, one bit per pixel.

7. Repeat this process for all candidate blocks until all of the secret data has been embedded.

8. Finally, the modified image can be sent to the recipient, who can extract the secret data by using a similar algorithm to the embedding process.





ISSN: 2583-3286(Online)

REFERENCES

[1] P. S. Ritu Sindhu, “Information Hiding using Steganography,” Vols. Volume-9, 2020.

[2] S. W, “ Cryptography and Network Security, ”2007.

[3] “Steganography,” https ://en.wikipedia.org /wiki/ Steganography.

[4] P. Chandarana and a. P. Ahirao, “"Advanced Image Steganography.",” *International Journal of Innovative Research in Information Security (IJIRIS),* 2018

[5] N. Singh, “"Survey Paper on Steganography.",” vol. Volume 6, pp. 68-71,2017

[6] J. R. Jayapandiyan and C. K. a. K. Sakthivel, “Multi Image Steganography Using Distributed Lsb Algorithm and Secret Text Recovery On Stego Image Corruption,” 2020.

[7] K.Sandhyarani and G.Prashanti, “A NewApproach for Data hiding with LSB Steganography,” 2015.

[8] A. H. K. Masoud Nosrati, “Steganography in Image Segments Using Genetic Algorithm,” 2015.

[9] A. Shrestha and A. Timalsina, “Color image steganography technique using daubechies discrete wavelet transform,” 2015.

[10] A. A. A. a. F. A. O. M. M. Emam, “A Modified Image Steganography Method based on LSBTechnique,” vol. 125, p. 5, 2015.

[11] S. A. El_Rahman, “A Comprehensive ImageSteganography Tool using LSB Scheme,” 2015.

[12] R. S. Indu Nehra, “Review Paper On Image Based,” *International Journal of Scientific &Engineering Research,* vol. Volume 6, no. Issue 6, 2015.

[13] V. S. a. Madhusudan, Two New Approaches, vol. IEEE XPLORE Digital Library, 2015.

[14] R. Jain and J. Boaddh, “Advances in digital image steganography,” 2016

[15] E. H. Houssein, M. A. S. Ali and A. E. Hassanien, “Essam H. Houssein; Mona A. S. Ali; Aboul Ella Hassanien,” *2016 Federated Conference on Computer Science and Information Systems (FedCSIS),* 2016.

[16] M. S. A. M. A. a. Sadaf Bukhari, “Enhancing security of images by Steganography and Cryptography techniques,” 2016.

[17] A. B. A. M. &. A. M. Zeki, “PSW statistical LSB image steganalysis,” 2017.

[18] R. Forgáč and R. Krakovský, “Contribution to image steganography using pulse coupled neural networks,” 16 November 2017.

[19] N. M. Surse and P. Vinayakray-Jani, “A comparative study on recent image steganography techniques based on DWT.,”2017.

[20] J.-J. S.-S. H. Y.-L. Wang, “An Improved Dual Image based Reversible Hiding Technique Using LSB Matching, International Journal of Network Security,” *International Journal of Network Security,* 2017

[21] I. S. F. a. W. C. C. H. Y. Chen, “Self-contained stylization via steganography for reverse and serial style,” Conference on Applications of Computer Vision, pp. 1-15, March 2018

[21] I. M. ,. G. P. ,. B. C. Pratap Chandra Mandal.""Digital image steganography: A literature survey",2022

[22] Z. S. L. Y. Wu S., “ Deep residual learning for image steganalysis, Multimedia tools and applications,” pp. 10437-10453, 2018

[23] W. Z. C. Yiwei Zhang, ““Adversarial examples against deep neural network based steganalysis, In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security”,” 2018.

[24] S. G. Sahu A. K., ““Dual Stego-imaging based Reversible Data Hiding using Improved LSB Matching”,” *International Journal of Intelligent Engineering and Systems,* 2019.

[25] H. M. A. S. A. A. I. Hameed M. A., “An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques,” 2019.

[26] A. S. Ansari, M. S. Mohammadi and M. T.Parvez, “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats,” *MECS,* 2019.

[27] P. Kadhim, “Comprehensive survey of image steganography: techniques, evaluations, and trends in future research,” in *Neurocomputing,* 2019, p. 299–326

[28] S. S. Yadahalli, S. Rege and R. Sonkusare, “Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques,” 2020.

[29] A. G. &. M. Al-Ghamdi, ““Hiding shares by multimedia image steganography for optimized counting-based secret sharing, Multimedia Tools and Applications”,” 2020.

[30] Z. Qu, H. Sun and Zheng.M, ““An efficient quantum image steganography protocol based on improved EMD algorithm”,” p. 1–29, 2021.

[31] N. Subramanian, O. Elharrouss, S. Al- Maadeed and A. Bouridane, “Image Steganography: A Review of the RecentAdvances,” 2021

[32] 1. Z. Y. Wenjie Lin, “An Improved Image Steganography Framework Based on Y Channel Information for Neural Style Transfer,” vol. Volume 2022, p. 12 pages,2022.

[33] X. Y. C. W. J. L. Xinliang Bi, “High-Capacity Image Steganography Algorithm Based on Image Style Transfer,” vol. 2021, p. 14, 2021

[34] P. C. Mandal, Mukherjee, Imon, G. Paul and B. Chatterji, “Digital image steganography: A literature survey",” 2022.

[35] N. Min-Allahv, N. Nagy, M. Aljabri, M. Alkharra, ““Quantum Image Steganography Schemes for Data Hiding:,”2022.

[36] N. A. F. Abbas, N. Abdulredha and R. K. Ibrahim, ““Security and imperceptibility improving of image steganography using pixel allocation and random function techniques”,”2022.

[37] “https://www.tutorialspoint.com/what-is- least-significan t- bit-algorithm-in-information- security”

[38] “https://en.wikipedia.org/wiki/BPCS-steganography”.

[39] N. Subramanian, O. Elharrouss, S. Al- Maadeed and A. Bouridane, “Image Steganography: A Review of the recent Advance,” vol. Volume: 9, 2021