Virtual Data Hiding and Extraction for carrier object using Image Steganography

Sachin More
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering
Navi Mumbai, India

Dayanad Ingle
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering
Navi Mumbai, India

***Abstract*— Hiding secret information inside other images will essentially be a fundamental technique for safe data communication using the proposed method that combines the compression algorithm called Deflate and LSB in order to increase the effectiveness of image steganography. Such an approach shall result in minimal changes to the host image when keeping the message being embedded confidential. The proposed method will be using the Deflate algorithm based on LZ77 and Huffman coding for LSB to compress the secret message before embedding. From the test results in MSE and PSNR for all images used within this experiment, it can be seen that the proposed method outperformed the baseline. The results suggest a close relation between applying data compression by the Deflate algorithm and the quality of outcomes for steganography. Thus, the innovation may possibly be applied to several spheres where confidentiality in communication-for example, in military operations or financial transactions-is necessary. Further studies may look into the performance of this method using images of any type and secret text size, and may also analyze the effects of varying compression levels on the results obtained in steganography.**

Keywords—***Steganography, Huffman Coding, LZ77, MSE, PSNR***

I. INTRODUCTION

The safeguarding of information is crucial in modern technologies.. The swift progress in network and data communication technologies has introduced numerous methods for transmitting, exchanging, and storing data; however, these advancements have also brought about security risks and vulnerabilities. Ensuring the authenticity and privacy of critical data requires a secure information exchange. Cryptography plays a fundamental role in ensuring security via protected channels. A subset of cryptography, known as steganography, involves concealing data within multimedia files such as videos and images. This technique provides an alternative method for transmitting encrypted data, allowing only the intended sender and recipient to access the hidden information. An example is image steganography, in which a secret message and key are embedded within a carrier image, making concealed content inaccessible to unauthorized parties. Most steganographic techniques use either sound or images as the carrier files. A common steganographic method, called Least Significant Bit (LSB) substitution, involves encoding information in the lowest-value position of binary data, such as 10010101 00001101 11001001 10010110 00001111 11001011 10011111 00010000. However, this LSB substitution technique is considered too basic for effectively hiding messages from human detection. The main goal of steganography is to conceal hidden information from the human awareness. Modern steganography detection tools have expanded this objective to protect covert messages not only from human discovery but also from digital analysis programs.

The main goal of steganography is to conceal hidden messages from human awareness. However, modern steganography detection systems have expanded this aim to include the protection of concealed messages from both human and digital discoveries. Virtual data hiding involves creating an illusion of hidden data behind a carrier object when no actual data are concealed. This method requires the extraction of secret information from the carrier at the recipient end. The term "virtuality," which denotes something that exists only in appearance but not in reality, aptly describes this concept. The virtual data-hiding mechanism allows for the concealment of an unlimited quantity of secret data behind any type of carrier object. It is crucial to note that no alterations can be made to the citations, references, or in-line citations in the text, and strict adherence to American English spelling, terms, and phrases is required. The success of image steganography depends on concealing a hidden message by altering pixel values, where any detectable differences between the original and modified images can jeopardize the confidentiality of the message [1]. Achieving maximum security depends heavily on the length of the encrypted message and the chosen encryption technique [2][3]. Encryption techniques can inadvertently reveal sensitive information. Significant progress in image steganography has resulted in the creation and improvement of various approaches [4][5][6]. [7] proposed a technique that combines LSB with the wavelet Faber-Schauder matching method, Ease of Use, to improve message extraction. [8] employed the Fisher-Yates shuffle to randomize a secret message's order before encoding, ensuring unbiased permutations. [9] concealed hidden messages within the green layer of images by utilizing the most significant bits for accurate tracking. Researchers have

also utilized metaheuristic approaches to obtain near-optimal outcomes in steganographic images. [10] developed an algorithm to detect optimal image regions for embedding secret data, followed by LSB embedding. [11] presented a minimal compression algorithm that uses the Burrows-Wheeler Transform (BWT) to reduce the confidential message size before LSB embedding. In contrast, [12] introduced a novel method using a U-Net neural network for pixel area segmentation to conceal secret messages. A novel visual analysis technique for revealing concealed data through pixel alterations was introduced by [13]. A method called Least Significant Bit plane steganography (LPS) based on Linked Lists was developed for improving the security of steganographic methods and is different from the traditional methods in the LSB approaches [6]. An Exclusive-NOR gate was used with LSB cryptography where color channels in an image were used as the encryption key by [14] [15]. The proposed approach yielded better payload capacity security, and quality compared to the previous techniques [16]. For assessing, measures taken for estimating the performance of the provided methods were PSNR, mean-square error, and structural index similarity. Performance measures used in transform coding are PSNR values. Superiority of this presented technique has been shown, utilizing the investigation of various measures of efficiency such as peak signal-to-noise ratio and mean squared error [17]. Steganalysis is a statistical method dealing with methods used to identify the hidden steganographic content based on the analysis of statistical properties of the cover media, such as pixel value, frequency distributions, correlations, and higher-order statistical features in the pixel domain [18]. A short overview of existing cryptography and steganography techniques together with recent developments in each category of the different modalities, especially in the representation of data through images and audio data, appeared in [19]. The present work emphasizes that the use of various techniques under cryptography and steganography provides better security. Deflate coding is one of the very popular lossless compression techniques which combines the LZSS compression technique along with Huffman coding [20] [21]. This method has widely been used in lossless data compression. In [23], Huffman coding was introduced by a new method that compresses a string of numbers by the special relation between the internal nodes and efficiently stored the number of the internal nodes in each layer. To overcome the errors of high results and lower accuracy in conventional power fault record data compression. For overcoming the problem of high errors as well as low accuracy through conventional power fault record data compression, research has implemented a novel multi-level lossless compression technique called LZ77 in managing large fault record data [24]. Nevertheless, there is room for advancement in compression methodologies to decrease the size of hidden messages and to further exploit the benefits of steganography. Although the LSB implementation in images is considered reliable, it is crucial to enhance the message component. To maintain message confidentiality, it is essential to employ optimal text encryption and compression techniques to minimize alterations. This study investigated data compression and the role of the LSB algorithm in image steganography by introducing the deflation algorithm, which combines LZ77 and Huffman coding. The LSB algorithm then encodes private communication in a condensed format utilizing an XNOR gate to select color channels for information concealment.

II. RELATED WORK

"Applied Cryptography" by Bruce Schneier is a comprehensive guide to cryptography and its applications, including steganography. This book provides an in-depth analysis of various steganographic techniques and their effectiveness. Neil F. Johnson, Zoran Duric, and Sushil Jajodia's "Steganography: Techniques and Applications" offers a detailed examination of steganography and its uses, such as watermarking, fingerprinting, and covert channels. It also explores different steganographic methods and their implementations. Jessica Fridrich, Miroslav Goljan, and Dorin Hogea's book on "Steganography in Digital Media: Principles, Algorithms, and Applications" provides a thorough overview of steganography in digital media, covering image, audio, and video steganography. This book discusses various steganographic algorithms and their real-world application. A new image steganography technique was presented in [25] [26], Among these, the most preferred technique is the Least Significant Bit (LSB). In this technique, the researchers encrypted their data first and then used the Stern-Brocot Sequence in order to randomly select those pixels on which they would embed the secret message. The decrypted message was multiplied LSBs of the RGB colour image and embedded into the randomly chosen pixels in the encrypted form. Thus obvious variations appeared in the quality of the cover images based upon the size of the inserted secret messages. However, the quality of the stego image was the same as before applying the proposed technique, and a secret message could be extracted from the stego image. Data to be encrypted prior to hiding and Stern-Brocot Sequence have been used by researchers to pick random pixels in the image. The product of LSBs of RGB colour image embeds the encrypted message onto the randomly selected pixels. This approach resulted in alterations to the cover image quality when secret messages of various sizes were inserted. However,the quality of the stego image remained consistent after applying the proposed technique., and the hidden message was successfully retrieved from the stego image.

Image steganography encompasses techniques for concealing secret messages within digital images, rendering them imperceptible and indecipherable to unauthorized individuals. This method involves hiding confidential information in image files and preventing access or interpretation by third parties. Various digital formats, including PNG, JPG, and BMP, can be used for this purpose [27]. A similar pixel-based approach was employed in [28], where the pixel intensity value provide histogram analysis and additional quality metrics to showcase the resilience of the algorithm against statistical attacks. Spatial Domain based steganalysis using Deep Learning was proposed by [26] for finding out whether text is embedded in LSB stegoimage or not. In their approach, a custom CNN model was used and an

effectives of more than 90% with variation against the key is shown. In [29], the method was developed to embed information in spatial domain by mapping from spatial domain to compressed form. The LSB method improves it with respect to statistical performance. To improve security, the stego image underwent transformation and quantization. This approach demonstrated greater effectiveness than the alternative proposed methods. It effectively integrates an efficient LSB technique with the security advantages offered by the transform domain.[30] presented an idea that focuses on modern deep image steganography, primarily emphasizing container image quality and capacity, while neglecting other important steganographic aspects. First, many techniques in this area are restricted to concealing data in an image format, excluding other types such as text and code, which limits their practical applications. Second, the current study prioritizes visual imperceptibility over statistical security, making it vulnerable to steganalysis. This strategy fails to address the need for effective steganography. [31] Introduces a new method of image-based steganography based on a function known as DCT coefficients, pseudorandom sequence generator, computer networks, and information security. The three very basic requirements for any covert data-hiding mechanism, as claimed by [32], are: security, capacity, and resilience. It is very difficult to acquire these three factors simultaneously because of their inverse relationship. Instead, the strategies for enhancing security and capacity of information hiding are of great concern to researchers. Their steganography technique uses high-resolution digital media as a cover signal that can hold considerable payloads, thus differentiating it from other traditional techniques of information hiding. Researchers have used oversized payloads such as images as cover imagesIn the direction of contrast enhancement, a new method for watermarking was proposed in [33] where reversible data hiding was suggested. The original image is modified in the spatial domain by way of an embedded watermark logo. In this method, through the possible recovery via contrast enhancement of the watermarked image, it can hide a large amount of secret data, recoverable in turn. The recovery of the watermark image to its original form follows the same process as that used in the enhancement technique.. The experimental outcomes show the efficacy of the algorithm in protecting the intellectual property of digital media. The increased use of smart devices and open networks has resulted in the improved creation and usage of multimedia content, including audio, video, and images. The proposed approach aims to enhance data security and safeguard the intellectual property of digital carriers and multimedia content. In [34] The study improves the efficiency of current techniques was improved by adjusting the prediction error to increase the likelihood of the value in the second prediction error aligning with its closest value. This strategy not only expands the capacity for embedded data, but also reduces the chances of changes during bit shifting. The results show an enhanced peak signal-to-noise ratio (PSNR) compared with existing methods for various carrier videos. This increases the payload capacity while ensuring that the extracted video remains consistent with the original carrier video. In contemporary society, protecting information is a critical concern that must be addressed to safeguard the data transmitted between the sender and receiver without external interference. Data hiding is a mechanism to avoid interception by unauthorized people of secret information. A trust-worthy data-hiding technique needs to be developed in order to make the secret information inaccessible to any intruder to decode. The research proposed aims at maintaining the secrecy of confidential data hidden in a video that acts as a cover object. In [35], the Number Theory Research Unit (NTRU), provides immunity against fast computing attacks and ensures secure encryption and decryption. In this research approach, this method is highly appropriate to wireless networks and provides data confidentiality and authentication of the system. Reversible data hiding within the homomorphic encrypted domain is described in this approach. This method directly segments an image into a set of references and neighboring pixels. Procedure of encryption by NTRU to each set: Subsequent to encryption, data hiding process is also carried out on the encrypted image. The subsequent segmentation is done by utilizing the very same method to the encrypted image. Histogram for every set was obtained by computing absolute differences of the adjacent pixels. Histogram of absolute differences may be shifted to embed further information in the stego images. Then, at the receiver side, she may either employ a data concealment key to extract additional information directly from the stego domain and recover the encrypted image, or she may employ both her private key and a data concealment key to recover the additional information from the plain text-domain. This new method has been proposed for more security as well as the ability to hide data compared with the rest of the novel techniques available.

III. PERFORMANCE METRICS

This study investigated four key aspects: undetectability, data hiding capacity, durability, and protection. Researchers have developed various methods for evaluating the effectiveness of steganographic techniques. Multiple strategies can be used to determine whether an image's quality remains intact after concealing a message. The concept of "payload capacity" denotes the amount of concealed information that can be embedded within a cover image. A higher payload capacity improves steganography efficiency by requiring fewer cover images to transmit messages. It is worth noting that larger payload sizes generally have a more significant effect on undetectability. In [37], evaluating the ability to avoid detection was a critical security consideration, involving image analysis to identify the presence of hidden data. Following text embedding, undetectability is used to assess the level of distortion applied to the cover image. Excessive alteration can reduce the image quality, potentially making it discernible to the human eye. "Robustness" refers to an image's ability to maintain hidden text despite various image-modifying processes, such as sharpening, blurring, noise addition, cropping, and enhancement. In[38] At its core, robustness denotes the capacity of an algorithm to safeguard concealed information within the cover medium, even when significant alterations are made to the cover. It also encompasses the volume of data that can be embedded without jeopardizing or obliterating the

existing information. In [36], Elevated PSNR values played a crucial role in reducing the risk of confidential data exposure, which is particularly critical when embedding sensitive content into images. The computational complexity evaluates the number of operations required for concealing and retrieving the steganographic message as well as the execution duration. Thus, it is beneficial to select techniques that require a shorter processing time.

1.1 **Peak Signal-to-Noise Ratio** :.

The Peak Signal-to-Noise Ratio (PSNR) quantifies the maximum signal to noise ratio resulting from distortion and is typically measured in decibels. A PSNR value above 40 dB is considered strong, but a range of 30-40 dB is deemed acceptable. The image quality improves as the PSNR value increases. It's crucial to note that the PSNR value is calculated exclusively from the Mean Squared Error (MSE) value [27][39]

1.2 **Mean Squqre Error :** MSE, defined in [27], is the average of squared differences between pairs of corresponding pixels in the original and stego images. Hence, it reflects how much modification has been done on the cover image by the process of embedding data. A lower result of MSE indicates better accuracy with a minimal amount of distortion. In theory, if the original and stego images are the same, then the value of MSE is 0.

IV. PROPOSED METHODOLOGY

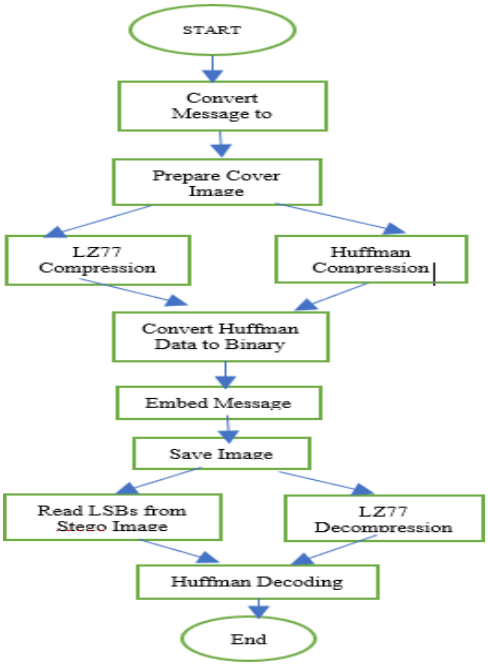


Fig. 1. Propose Architecture Flowchart

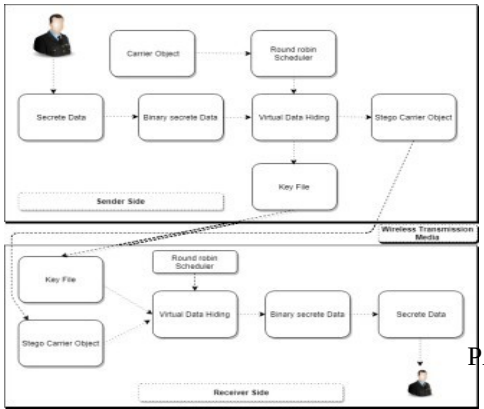


Fig. 2. Propose Architecture Diagram

A. Working of LSB Steganography

As presented in the flowchart of Figure 1 and the proposed architecture diagram of Figure 2, one of the methods to hide information using least significant bits applied for pixel values inside an image, that is LSB Steganography.

This method is based on the fact that the changing the least significant bit of any pixel color does not greatly affect the image appearance, so it is an acceptable way for secret message communication.

1. CONVERT THE MESSAGE INTO BINARY:
   - The hidden message (data) is coded in binary format.
2. PREP THE COVERIMAGE:
   - The cover image is just a common image to which user wants to conceal the secret message. All pixels of any image consist of three channels: Red, Green, and Blue (RGB) in which value of each such channel can be between 0 and 255.
3. EMBED THE MESSAGE:
   - Replace the least significant digit of each color of a pixel in the image with a bit of the binary message. This is by replacing the least significant bit of each channel with a bit of the binary message.
4. SAVE THE IMAGE:
   - The manipulated image was kept for saving in new file. This new image was a secret message in pixels.
5. EXTRACT THE MESSAGE:
   - Hidden message is extracted by reading the least significant bits from each color channel of the image pixels and is then reconstructed in binary form and decoded back to its original form.

B. Example with Numerical Values

IV. ENCODING EXAMPLE

Suppose you want to hide the message "Hi" in a 2x2 pixel image. Here's how you can do it:

1. CONVERT MESSAGE TO BINARY:
   - Message: "Hi"
   - ASCII values: H = 72, i = 105
   - Binary representation: 72 = 01001000, 105 = 01101001
   - Combined binary message: 01001000 01101001
2. PREPARE THE COVER IMAGE:
   - Assume a 2x2 image with the following pixel values:

Pixel (0,0): (R=100, G=150, B=200) Pixel (0,1): (R=120, G=160, B=220) Pixel (1,0): (R=130, G=170, B=230) Pixel (1,1): (R=140, G=180, B=240)

3. EMBED THE MESSAGE:
   - Binary message to hide: 01001000 01101001

- Update the least significant bit of each color channel:

For pixel (0,0):

- Original: R=100 (01100100), G=150 (10010110), B=200 (11001000)

- Modify LSBs to 01001000:
  - R: Change 01100100 to 01100100 (LSB remains 0)
  - G: Change 10010110 to 10010111 (LSB changes to 1)
  - B: Change 11001000 to 11001001 (LSB changes to 1) For pixel (0,1):

- Original: R=120 (01111000), G=160 (10100000), B=220 (11011100)

- Modify LSBs to 01101001:

- R: Change 01111000 to 01111001 (LSB changes to 1)
- G: Change 10100000 to 10100001(LSB changes to 1)
- B: Change 11011100 to 11011101 (LSB changes to 1)

The final modified image would have the following pixel values:

Pixel (0,0): (R=100, G=151, B=201) Pixel (0,1): (R=121, G=161, B=221)

Pixel (1,0): (R=130, G=170, B=230) // Remaining pixels untouched

Pixel (1,1): (R=140, G=180, B=240) // Remaining pixels untouched

V. EXTRACTION EXAMPLE

To extract the hidden message:

1. READ THE LSBS FROM THE IMAGE:
   - For pixel (0,0):
     - R=100 (01100100), LSB = 0
     - G=151 (10010111), LSB = 1
     - B=201 (11001001), LSB = 1
   - For pixel (0,1):
     - R=121 (01111001), LSB = 1
     - G=161 (10100001), LSB = 1
     - B=221 (11011101), LSB = 1
2. RECONSTRUCT THE BINARY MESSAGE:
   - Extracted LSBs: 01001000 01101001
3. CONVERT BINARY BACK TO TEXT:
   - Binary 01001000 = ASCII 72 = 'H'
   - Binary 01101001 = ASCII 105 = 'i'
   - Hidden message: "Hi"

C. Proposed Algorithm

This section describes the step-by-step approach used to implement the proposed methodology for enhancing Least Significant Bit (LSB) steganography by integrating LZ77 compression and Huffman coding techniques.

The methodology is aimed at improving data hiding capacity, reducing the distortion in the cover image, and ensuring robust and efficient data retrieval.

1. Data Compression Using LZ77 Algorithm

The first step in the process is compressing the secret data to be hidden in the cover image. LZ77 (Lempel-Ziv 1977) is employed for this task because of its ability to exploit patterns and repetitions in the data, thus reducing its size. This compression step is crucial to ensure that a larger amount of data can be embedded within the image with minimal impact on its visual quality.

LZ77 Compression Steps:

1. A sliding window is used to scan the input data for repetitive patterns.
2. If a sequence of symbols is found that has appeared before, it is replaced with a reference to the previous occurrence, represented as a pair (offset, length).
3. If no match is found, the current symbol is output directly.
4. The output consists of compressed symbols in the form of pointers and literals (direct symbols), leading to a smaller data size.

Example: Input string: ABABABA LZ77 compressed output: (0,0,'A'),(0,0,'B'),(2,2)

2. Huffman Coding for Further Compression

After the LZ77 compression, Huffman coding is applied to the compressed output for further reduction in size. Huffman coding gives symbols binary codes of varying lengths based on their frequencies, giving shorter codes to more frequent symbols.

Huffman Coding Steps:

1. The frequency of each symbol in the LZ77-compressed output is calculated.
2. A binary tree is constructed using these frequencies, where symbols with lower frequency are placed deeper in the tree.
3. Variable-length codes are generated from the tree, where more frequent symbols are assigned shorter codes.
4. The secret data is re-encoded using the generated Huffman codes.

Example: LZ77 output: (0,0,'A'),(0,0,'B'),(2,2) Huffman codes: A=0, B=1 Encoded data: 00 01 10

Combining LZ77 with Huffman compression in this dual-compression process significantly decreases the size of the data being embedded, allowing for more information to be concealed within the image.

3. Embedding Compressed Data Using Steganography

After compressing the data, the LSB technique is utilized to hide the data within the original image. LSB steganography includes changing the least significant bit of every pixel's color part in order to conceal the compressed data.

Steps for LSB Embedding:

1. The compressed data is converted into a binary stream.
2. The cover image is selected, and the least significant bits of the pixel values are identified.
3. Each bit of the binary stream is embedded into the LSB of the pixel's red, green, or blue channel.
4. Care is taken to modify the pixel values minimally to avoid noticeable distortion in the cover image.
5. After embedding, the modified image (stego-image) is generated, which contains the hidden compressed data.

Example: Cover image pixel (before): (10110110 11100101 10100010) Data to embed: 110 Stego-image pixel (after): (10110111 11100101 10100011)

4. Extracting Hidden Data from the Stego Image

To retrieve the hidden data, the stego-image is processed to extract the embedded bits from the LSBs of the pixel values.

Steps for Data Extraction:

1. The stego-image is scanned, and the least significant bits of the pixels are extracted.
2. The binary stream representing the compressed secret data is reconstructed.
3. The binary stream is decoded using Huffman decoding, followed by LZ77 decompression to recover the original data.
4. The extracted data is verified for accuracy, ensuring no loss occurred during embedding or extraction.

5. Ensuring Data Integrity and Image Quality

To evaluate the effectiveness of the methodology, two key factors are considered:

1. **Peak Signal-to-Noise Ratio (PSNR):**

The PSNR metric is utilized to evaluate the quality of the stego-image in comparison to the original cover image. A high PSNR value suggests that there is little distortion from hiding the secret data.

$$PSNR = 10.$$

MAX represents the highest pixel value achievable, while MSE calculates the average squared difference between the original and stego-images.

2. **Compression Ratio:**

The compression ratio was determined to evaluate the effectiveness of the combined LZ77 and Huffman compression techniques. A higher compression ratio suggests that the image can accommodate more concealed data.

$$\text{Compression Ratio} =$$

6. Robustness Against Image Manipulations

The resilience of the concealed information was tested by subjecting the stego-image to typical image processing techniques, including JPEG compression, size alteration, and the introduction of noise. Subsequently, the embedded data are retrieved and their integrity is checked. The efficacy of the method is determined by assessing how well the information resisted these alterations without degradation.

7. Computational Efficiency

The effectiveness of the data compression, embedding, and extraction processes is considered in terms of time complexity and computational resource usage. The LZ77 and Huffman algorithms were developed in such a way that they are computationally feasible for the whole process even when there are large images and datasets involved. The proposed approach strengthens the traditionally used LSB-based image steganography through the inclusion of the LZ77 and Huffman compression techniques. This integration will allow increased data embedding with less distortion of the image and improved resilience. Both algorithms maximize the amount of concealable data while preserving visual quality of the cover image. Moreover, the proposed methodology ensures that the hidden data can be extracted efficiently and securely, making it appropriate for real-world applications involving in confidential data transmission.

8. RESULTS AND DISCUSSIONS

TABLE 1

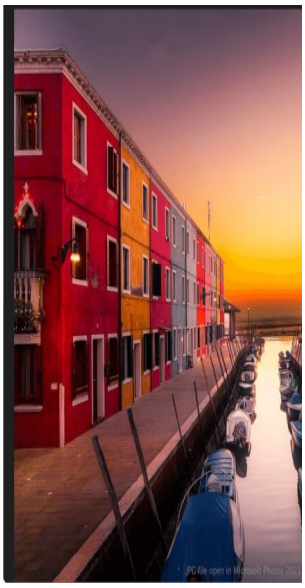
Metric	Cover Image (Image 1)	Stego Image (Image1)	Traditional Method (Image 1)	Proposed Method (Image1)	Cover Image (Image 2)	Stego Image (Image2)	Traditional Method (Image 2)	Proposed Method (Image2)
MSE	217.49	249.01	92.32	70.99	203.12	238.12	87.58	78.66
PSNR (dB)	24.76	24.17	28.48	29.62	25.05	24.36	28.71	29.17

Performance Measure Analysis of Traditional versus Proposed Method

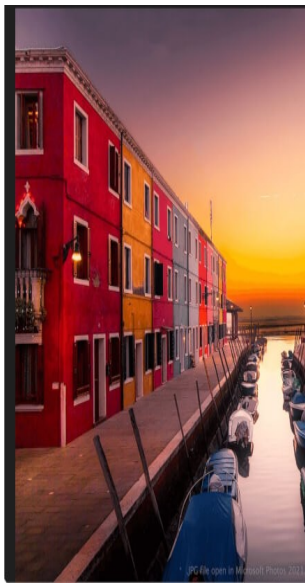
Original Image **Steg-Image**

Original Size : 162KB

Steg Image Size: 121KB



Original Size : 90.9KB



Steg image Size: 63.3KB

REFERENCES

[1] J. Cheng, X. Yan, L. Liu, Y. Sun, F. Xing, Comprehensive reversible secret image sharing with palette cover images, Journal of Information Security and Applications. 68 (2022) 103233. https://doi.org/10.1016/j.jisa.2022.103233.

[2] H. Mohammed Zaki, Color Pattern Steganography in Images, Technium Romanian Journal of Applied Sciences and Technology. 9 (2023) 60–65. https://doi.org/10.47577/technium.v9i.8337.

[3] Y. Lan, X. Kang, E. Li, F. Shang, J. Yang, Robust Image Steganography: Hiding Messages in Frequency Coefficients, Proceedings of the AAAI Conference on Artificial Intelligence. AAAI Conference on Artificial Intelligence.3(2023 14955–14963. https://doi.org/10.1609/aaai.v37i12.26746.

[4] M. Habiban, N.A. Mohsin, N.A. Mohsin, F.R. Hamade, Hybrid Edge Detection Methods in Image Steganography for High Embedding Capacity, Cybernetics and Information Technologies. 24 (2024) 157–170.https://doi.org/10.2478/cait-2024-0009

[5] A. Saepulrohman, L. Heliawati, A. Ismangil, Message Encryption in Digital Images using the Zhang LSB Image Method, Komputasi: Jurnal Ilmiah Ilmu Komputer Dan Matematika. 21 (2024) 21–30. https://doi.org/10.33751/komputasi.v21i1.9314

[6] V. Dwivedi, Improved LSB Based Image Steganography Using Linked Pixel Technique: A Linked-List Inspired Approach, International Journal of Scientific Research in Engineering and Management. 08 (2024) 1–5. https://doi.org/10.55041/ijsrem34005

[7] P.C. Mandal, I. Mukherjee, Integer Wavelet Transform based Secured Image Steganography using LSB and Coefficient Value Differencing, (2021). https://doi.org/10.1109/icsccc51823.2021.9478095.

[8] M. Virginia, J.A. Ginting, Game Edukasi Match Puzzle Mengunnakan Algoritma Fisher-Yates Shuffle Berbasis Android, JurnalAlgoritma,LogikaDanKomputasi. (2023).https://doi.org/10.303/j-alu.v6i1.3530

[9] P. Puteaux, W. Puech, A Recursive Reversible Data Hiding in Encrypted Images Method With a Very High Payload,IEEE Transactions on Multimedia. 23 (2021) 636–650. https://doi.org/10.1109/tmm.2020.2985537

[10] M.A. Aslam, M. Rashid, Y. Rasheed, F. Azam, S.S. Alotaibi, M.W. Anwar, M. Abbas, Image Steganography using Least Significant Bit (LSB). A Systematic Literature Review (2022} https://doi.org/10.1109/iccit52419.2022.9711628.

[11] S.N. Mahendra, F. Budiman, Message Hiding Using the Least Significant Bit Method with Shifting Hill Cipher Security, Journal of Applied Intelligent System. 8 (2023) 376–388. https://doi.org/10.33633/jais.v8i3.9321

[12] D. India, N. Malarvizhi, R. Bhavani, R. Priya, Deep Neural Network-based Reversible Image Steganography Technique using Circle-U-Net, Fusion: Practice and Applications. 13 (2023) 114–126. https://doi.org/10.54216/fpa.130210.

[13] Y.Y. Demircan, S. Ozekes, A novel LSB Steganography Technique using Image Segmentation, Journal of Universal Computer Science. 30 (2024) 308–332. https://doi.org/10.3897/jucs.105702

[14] L.B. Handoko, C. Umam, Data Security Using Color Image Based on Beaufort Cipher, Column Transposition and Least Significant Bit (LSB), Journal of Applied Intelligent System. 8 (2023) 140–151. https://doi.org/10.33633/jais.v8i2.7863

[15] R.I.H. Nasution, A. Fauzi, H. Khair, Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image, Journal of Artificial Intelligence and Engineering Applications (JAIEA). 2 (2023) 89–98. https://doi.org/10.59934/jaiea.v2i3.201

[16] B. Ramapriya, Y. Kalpana, A Competent Medical Image Steganography using Improved Optimization Algorithm with Huffman Encoding Techniques, (2023). https://doi.org/10.1109/iccmc56507.2023.10083698.

[17] K. Suriyan, N. Ramaingam, J. Sakkarai, B. Asokan, S. Rajagopal, M. Alagarsamy, Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method, Bulletin of Electrical Engineering and Informatics. 11 (2022) 286–292. https://doi.org/10.11591/eei.v11i1.3332.

[18] N.J.D.L. Croix, N.J.D.L. Croix, T. Ahmad, F. Han, Comprehensive survey on image steganalysis using deep learning, Array. 22 (2024) 100353. https://doi.org/10.1016/j.array.2024.100353

[19] M. Bansal, R. Ratan, Comprising Survey of Steganography & Cryptography: Evaluations, Techniques and Trends in Future Research, (2022). https://doi.org/10.1109/icsc56524.2022.

[20] D. Takafuji, K. Nakano, A. Kasagi, Y. Ito, GPU implementations of deflate encoding and decoding, Concurrency and Computation : Practice & Experience. 35 (2022). https://doi.org/10.1002/cpe.7454

[21] D. Takafuji, Y. Ito, A. Kasagi, K. Nakano, Acceleration of Deflate Encoding and Decoding with GPU implementations, (2021). https://doi.org/10.1109/candarw53999.2021.00036.

[22] S. Thind, A.K. Shukla, A Review on Analysis and Development of Quantum Image Steganography Technique for Data Hiding, in: springer nature singapore, 2022: pp. 663–671. https://doi.org/10.1007/978-981- 19-4193-1_65

[23] Q. Cheng, N. Yu, W. Yan, S.-J. Lin, Compressing the Tree of Canonical Huffman Coding, (2022).

https://doi.org/10.1109/dcc52660.2022.00061.

[24] J. Di, C. Wang, P. Yang, L. Yan, Layered Lossless Compression Method of Massive Fault Recording Data, International Journal of Circuits, Systems and Signal Processing. 16 (2022) 17–25. https://doi.org/10.46300/9106.2022.16.3

[25] Md Abdullah Al Mamun, S. M. Maksudul Alam, Md. Shohrab Hossain, M. Samiruzzaman, **A** Novel Image Steganography using Multiple LSB substitution and Pixel Randomization using Stern-Brocot Sequence, *Future of Information and Communication Conference (FICC)*, 756-773, 2020. https://link.springer.com/chapter/10.1007/978-3-030-39445-5_55

[26] ALabaichi A, Al-Dabbas M. A. A. A. K, & Salih A, Image Steganography Using the Least Significant Bit and Secret Map Techniques, International Journal of Electrical & Computer Engineering. 10(1) (2020) 2088-8708 http://doi.org/10.11591/ijece.v10i1.pp935-946

[27] Dilovan Asaad Zebari, Diyar Qader Zeebaree, Jwan Najeeb Saeed, Nechirvan Asaad Zebari, Adel AL-Zebari (2020).” Image steganography based on swarm intelligence algorithms: A survey “people, 7(8), 9. http://testmagzine.biz/index.php/testmagzine/article/view/11281

[28] J. Singh and M. Singla, "A Novel Method of high-Capacity Steganography Technique in Double Precision Images," 2021 International Conference on Computational Performance Evaluation (ComPE), 2021, pp. 780-784 (2021) https://doi.org/10.1109/ComPE53109.2021.9751905

[29] S. Mondal, R. Debnath and B. K. Mondal, "An improved color image steganography technique in spatial domain," 2016 9th International Conference on Electrical and Computer Engineering (ICECE), 2016, pp. 582-585, doi: 10.1109/ICECE.2016.7853987

[30] Mehdi Boroumand, Mo Chen, and Jessica Fridrich. Deep residual network for steganalysis of digital images. IEEE TIFS, 14(5):1181–1193, 2018 https://doi.org/10.1109/TIFS.2018.2871749

[31] Weike You, Hong Zhang, and Xianfeng Zhao. A Siamese CNN for image steganalysis. IEEE TIFS, 16:291–306, 2020

[32] Arup Kumar Bhaumik, Minkyu Choi,Rosslin J.Robles and Maricel O.Balitanas. "Data Hiding in video" International journal of Database Theory and Application vol.2, No. June 2,2009.pp 9-14

[33] Jaime Sarabia-Lopez; Diana Nuñez-Ramirez; David Mata-Mendoza; Eduardo Fragoso-Navarro; Manuel Cedillo-Hernandez, ’Visible Imperceptible Image Watermarking based on Reversible Data Hiding with Contrast Enhancement’, 2020 International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE)

[34] Alek Nur Fatman; Tohari Ahmad, ’Two Level Prediction Error and Three Direction Shifting for Hiding Data in Digital Video’, 2021 International Seminar on Intelligent Technology and Its Applications (ISITIA)

[35] Neng Zhou; Minqing Zhang; Han Wang; Yan Ke; Fuqiang Di, ’Separable Reversible Data Hiding Scheme in Homomorphic Encrypted Domain Based on NTRU’, April 28, 2020 IEEE Access (Volume: 8)

[36] Zeebaree, D. Q., Abdulazeez, A. M., Hassan, O. M. S., Zebari, D. A., & Saeed, J. N. (2020). Hiding image using contourlet transform. vol, 83, 16979-16990

[37] Zebari, D., Haron, H., & Zeebaree, S. (2017). Security issues in DNA based on data Hiding: A review. International Journal of Applied Engineering Research, 12(24), 0973-4562

[38] Arunkumar, S., Subramaniya swamy, V., & Logesh, R. (2019). Hybrid Robust Image Steganography approach for the secure transmission of biomedical images in the Cloud. EAI Endorsed Transactions on Pervasive Health and Technology, 5(18), e1-e1.

[39] Maji, G., & Mandal, S. (2019). Secure and robust image steganography using a reference image as key. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN, 2278-3075.