iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70300

www.ijraset.com

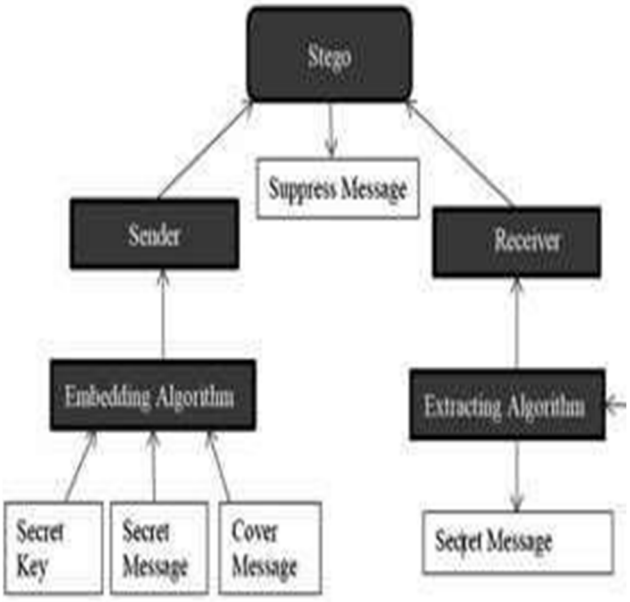
Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Steganography: Data Concealment in Images

Mohammad Hashir Khan[1], Hanshu Agrahari[2], Ayush Sharma[3], Ankit Tiwari[4], Ms. Swati Sheoran[5]
[1, 2, 3, 4]*Dept of CSE, SRMIST, Delhi NCR, U.P., India*
[5]*Assistant, Professor Dept of CSE SRMIST, Delhi NCR U.P., India*

Abstract: ***Steganography is the practice of hiding information behind cover data so that its presence remains undetected. Digital photography steganography harnesses the capability of safeguarding communication, which is crucial in numerous contemporary applications. Steganography possesses numerous beneficial applications. The significant advancement in computational capacity and security expertise has established it as a leader in contemporary security. The primary challenge in proposing steganography lies in balancing capacity, imperceptibility, and security, distinguishing it from other systems like encryption and watermarking. This study presents a thorough evaluation and analysis of novel steganography techniques. Steganography, in contrast, obscures the very existence of communication by embedding.***
Index Terms: ***Image Steganography, Information hiding, Image data hiding***



I. INTRODUCTION

In contemporary society, communication is an essential requirement for any developing sector. All individuals desire the confidentiality and security of their transmitted information. In our daily lives, we utilize several secure channels, such as the internet and telephone, for the transmission and sharing of information; nonetheless, all methods possess inherent vulnerabilities. To disseminate information discreetly, two strategies may be employed. The mechanisms are cryptography and steganography. In cryptography, the communication is altered into an encrypted format using an encryption key that is exclusively known to the sender and receiver. Access to the communication is restricted to individuals possessing the encryption key. Nevertheless, the transmission of encrypted messages may readily provoke an attacker's suspicion, leading to potential interception, assault, or violent decryption of the communication. Steganography approaches have been created to address the limitations of cryptographic methods. Steganography is the discipline of concealing the existence of communication within a message. Consequently, steganography conceals the existence of data, rendering it undetectable. In steganography, the act of concealing information within multimedia content such as images, audio, or video is termed "embedding." To enhance the anonymity of data transmission, both strategies may be integrated.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

Steganography has evolved significantly over the years, finding applications across various domains due to its ability to conceal information within multimedia files. Traditional methods such as the LSB technique, which involves modifying the least significant bits in image pixels, are widely employed for their simplicity and effectiveness [2]. This technique is particularly effective in spatial domains, where hidden data remains relatively undetectable to the human eye and minimal file size changes ensure efficient data concealment. However, LSB's limitations include susceptibility to common image manipulations like compression or filtering, which may expose or alter the embedded data [2].

More advanced methods, including DWT and DCT-based steganography, aim to address these limitations by working in the frequency domain, which offers greater robustness against image modifications [1]. DWT- based steganography leverages frequency transformations to conceal data in specific frequency bands, resulting in higher resistance to data loss and distortion during compression and scaling processes [1]. DCT, another frequency-domain technique, is commonly used in JPEG image compression and enhances steganographic resistance to tampering by embedding data in non-perceptible image components [3]. Studies show that frequency-domain techniques generally provide stronger data security, though they may involve higher computational costs compared to spatial domain techniques [3].

Recent research also explores the application of steganography in sectors that require stringent security protocols. For instance, in the medical field, patient data can be embedded within diagnostic images, like X-rays or MRIs, ensuring communication across various fields, offering innovative solutions for covert data embedding and retrieval while addressing the challenges associated with data integrity, efficiency, and detectability.Applications

1) Covert Communication: The utilization of steganography does not facilitate covert communication, hence obstructing the analysis of the sender, message, and recipient. Confidential data, strategies, or other sensitive information may be disclosed unexpectedly to the assailants.

2) Specific content may be incorporated into the image, including the individual's name or the geographical position on the map. Duplicate the steganographic image, extract all embedded features, and display just those characteristics that may be eliminated without compromising the steganography key.

3) Copyright Protection: A mechanism that inhibits the duplication of data, typically in digital form.

III. RELATED WORK

Steganography, the science of hiding information within seemingly innocuous media, has been a crucial topic of research for secure communication, data protection, and digital rights management. Over the years, various methods have been developed to enhance the robustness, security, and imperceptibility of hidden data. This section explores key contributions to the field, focusing on traditional and contemporary techniques.

A. Classical Steganography Techniques

One of the foundational methods in digital steganography is the Least Significant Bit (LSB) embedding technique. It involves replacing the least significant bits of the carrier media (often images) with the secret data. LSB embedding is simple and computationally efficient, but it is highly susceptible to steganalysis due to detectable changes in the media. Yang et al. (2008) proposed an improvement by adapting data hiding to edge areas in images, enhancing security by minimizing visible distortions. While LSB is effective in low-risk environments, modern requirements for security have pushed the development of more complex techniques.

B. Transform Domain Techniques

To address the constraints of spatial domain methods such as LSB, transform domain techniques like the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are frequently employed. These techniques integrate data into the frequency components of the carrier medium, enhancing resistance to prevalent image processing procedures such as compression and noise introduction. Saidi et al. (2017) demonstrated that the combination of DCT with chaotic maps enhances resilience and security. Kumar and Kumar (2018) introduced an improved DWT approach that increases resilience to picture alterations. Audio and Video Steganography Beyond images, steganography in audio and video files has also seen significant progress. Techniques like spread spectrum and phase coding are used for embedding data in audio files. These methods are designed to resist steganalysis by distributing the hidden information across multiple frequencies or altering phase information, making detection more difficult.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Video steganography typically utilizes motion vectors or redundant frames to hide data, taking advantage of the large amount of data present in video streams. Wang et al. (2021) explored payload location optimization in JPEG images, which has direct applications in video steganography.

C. Recent Advances

Recent work in steganography includes the use of deep learning and neural networks to automate the embedding and extraction of hidden data. This approach allows for more sophisticated and flexible steganography systems. Neural networks can be trained to find optimal regions in a carrier file where data can be embedded with minimal detection risk. Islam et al. (2018) demonstrated how neural networks could enhance the robustness of image watermarking techniques, which are closely related to steganography. Another recent trend is the integration of blockchain technology with steganography. As noted by contemporary researchers, blockchain's decentralized and secure nature makes it a promising platform for steganography, particularly in applications requiring immutable and secure Steganalysis and Countermeasures

With the growing sophistication of steganographic techniques, steganalysis—the process of detecting hidden data—has also advanced. Techniques like statistical analysis and machine learning have become popular in detecting inconsistencies in carrier files that suggest the presence of hidden data. Researchers have developed robust steganalysis tools to counteract the increasing complexity of steganographic methods. These tools often analyse anomalies in the statistical distribution of pixel values or audio frequencies, making it easier to detect hidden information.

Steganography's effectiveness depends on striking a balance between security and detectability. Recent research by Luo et al. (2017) focused on reversible data hiding methods that allow the original carrier to be restored after the embedded data is extracted, minimizing alterations to the carrier file

Furthermore, Shafi et al. (2018) proposed an adaptive hybrid fuzzy- wavelet approach that optimizes the bit reduction and pixel adjustment to enhance the quality of steganography in various media formats.

D. Challenges and Future Directions

Despite the significant progress in steganography, challenges remain. Maintaining a high data capacity without compromising the imperceptibility of the hidden data is a primary concern. Techniques that alter fewer bits in the carrier media are less detectable but often limit the amount of data that can be embedded. Furthermore, standardization and regulation of steganographic methods are necessary to ensure their responsible use, particularly in preventing misuse in cyberattacks. The future of steganography may involve greater integration with emerging technologies like quantum computing, which has the potential to either break existing steganographic methods or offer new ways to hide data. Additionally, the development of steganography in cloud computing and IoT environments is expected to address the growing need for secure communication in distributed systems.

IV. STEGANOGRAPHY TECHNIQUES

The following are the classifications of steganography technologies:

A. Frequency Domain Technology

This technique employs numerous algorithms and tweaks to conceal messages, with the embedding method being proposed. This strategy is considered somewhat laborious by numerous algorithms and is categorized as follows:

1) *Discrete Cosine Transform Technology:* It is utilized to transform the signal to its basic frequency employing the features of the Discrete Cosine Transform (DCT).
2) *Discrete Wavelet Transform Methodology:* When the wavelet is identified in a discrete manner, it constitutes a discrete wavelet transform (DWT). frequency component of the pixel intensity.

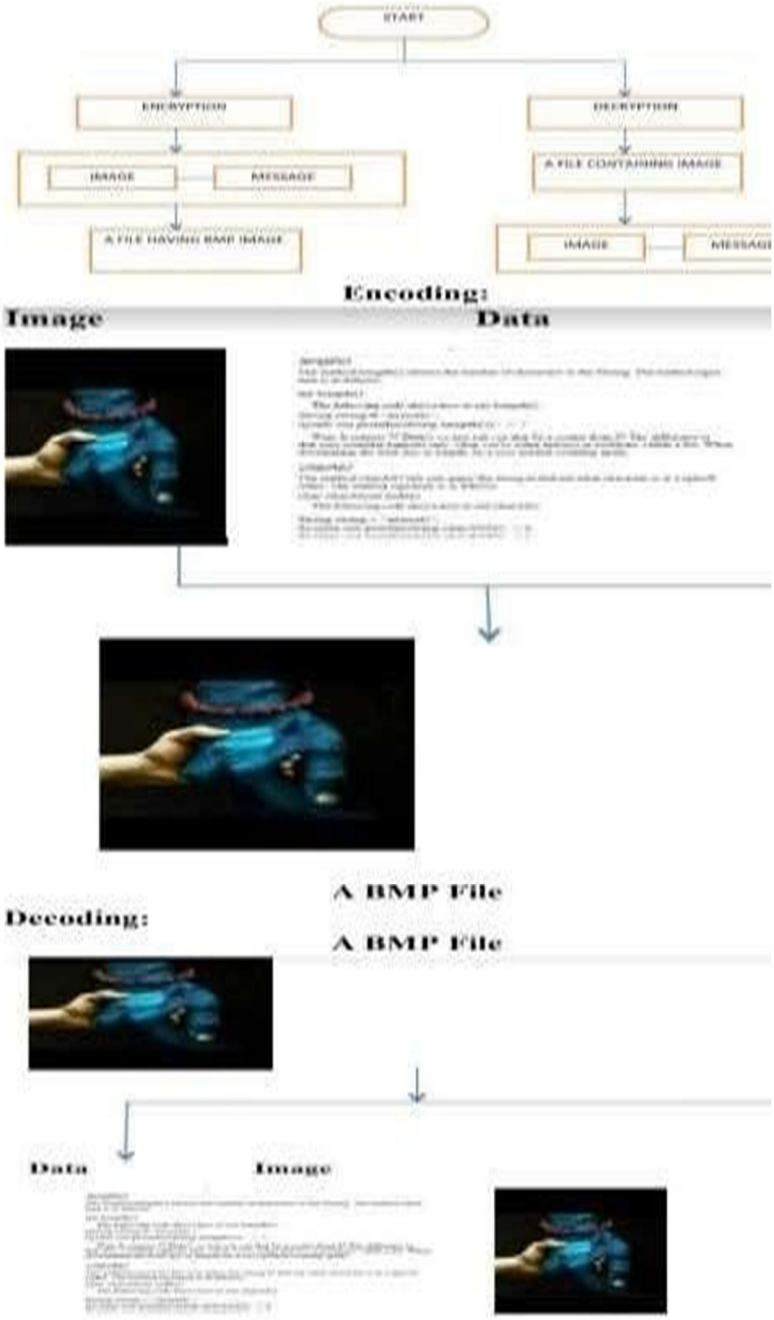
B. Method in the Spatial Domain

This method involves directly altering a few bits of the image pixels to conceal the data. This procedure is categorized as:

1) *Difference in Pixel Values:* During this procedure, numerous quantization tables are generated, the payload is established, and the countability of the steganography is preserved.
2) *Edge-centric data embedding technique:* This approach utilizes every pixel edge in the image. Initially, we compute the mask picture and identify the edge pixels using the edge detection technique. Data is concealed among the least significant bits of the edge pixels, and the recipient obtains the steganographic bits. For instance, in the binary number 110100101001, the least significant bit (LSB) is 1, located on the right. The concealed message resides in the least significant bit of the image.

C. Bitmap Steganography Technique

The Bitmap type is one of the simplest forms of images, as it employs no technology to reduce file size. A bitmap image is composed of pixels, utilizing three colors (green, red, and blue, abbreviated as GRB) for pixel production. Each color component of a pixel contains one byte of information, which determines the color's representation. The colors observed in these images result from the amalgamation of these three hues. One byte is comparable to eight bits, with the first bit designated as the Most Significant Bit (MSB) and the last bit as the Least Significant Bit (LSB). In this context, the LSB is utilized for encoding security information within a BMP image. If the eighth layer, which is the final layer of information, requires modification, we simply need to alter the last bits of each pixel. Since there are three bits per pixel, the memory required for writing our data is equivalent to 3 multiplied by height and breadth. The data name and data file name must be accurately designated, which can be accomplished by allocating the initial bit of RAM. (01110101 01010101 11101100) (11010010 10010101 00010100) (10110010 10011100 01101011) Three pixels are utilized to store one byte of



V. METHODOLOGY

This study introduces a more straightforward adaptive technique that efficiently identifies the ideal configuration for inverted Least Significant Bit (LSB) replacement in steganography. The main goal is to improve the embedding process by assessing error ratios linked to different patterns prior to embedding messages into a container image. Steganography, the technique of hiding messages within non-secret data, fundamentally encompasses two essential processes: embedding and extracting message.

A. Embedding Procedure

The embedding procedure, as depicted in the accompanying diagrams, adheres to a methodical approach:

B. Reading Pixel Values

The first stage entails extracting the pixel values of a container image and ascertaining its dimensions. designated as mm for width and nn for height. For instance, a sample image matrix may comprise pixel values: [228, 233, 162, 140, 231, 33, 25, 45] The total pixel count is determined by multiplying mm by nn. The image is subsequently transformed into a one-dimensional array and stored in a variable named CC. For example, with m=4 and n=2, the array C transforms into: C = [228, 231, 233, 33, 162, 25, 140, 45]C = [228, 231, 233, 33, 162, 25, 140, 45]

1) Message Preparation: The digital message designated for embedding is reviewed to confirmdimensions are compatible with the container image. The message is transformed into its ASCII representation and then into binary format. For instance, the character 'A' corresponds to the ASCII value 65, which is represented in binary as 01000001.
2) Message Encryption: A key for encryption is inputted, and the message is encoded using the RC4 technique, resulting in ciphertext. For instance, if the key is 'password', the encrypted message for M=65M=65 may produce a binary representation of 1100101011001010.
3) Pattern Selection: The subsequent phase entails choosing a three-bit combination from the pixel values, specifically the 6th, 7th, and 8^{th} bits.
4) Error Counting: Sixteen variables are designated to quantify eight patterns, each denoting the quantity of pixels that alter their values throughout the embedding process. The eight remaining variables account for those that stay constant. The quantity of bits that alter (designated as pp) and those that remain constant (designated as p′p′) are computed using particular formulae.
5) Calculation of Error: The cumulative error for the eight patterns is aggregated and saved in the variable ee. The minimal total error is calculated, directing the choice of the ideal embedding pattern.
6) Pattern Embedding: Steps 3 to 8 are reiterated for the remaining three-bit combinations, yielding a total of 21 combinations. The combination that produces the minimal error is chosen for embedding, and the associated pattern data is recorded as an extraction key kk.
7) Finalizing the Image: The binary values of the altered pixels are reverted to decimal form, restructuring the array to correspond with the original image dimensions m×n. The resultant image retains the original pixel values while incorporating the concealed message.[3]

C. Extraction Procedure

Upon completion of the embedding process, the recipient can retrieve the concealed message by following these steps:

1) Reading the Image: The receiver interprets the image and acquires its dimensions.
2) Pixel Reshaping: The image is transformed into an array and assigned to the variable SS.
3) Extraction Key Utilization: The extraction key kk is read to identify the bit combination and inverted bit pattern used during embedding.
4) Message Extraction: The least significant bits of the image are accessed according to the extraction key, facilitating the retrieval of the embedded message bits.
5) Binary to ASCII Conversion: The extracted bits are grouped and converted back into an ASCII number, revealing the encrypted message.
6) Message Decryption: The message is decrypted using the RC4 technique with the identical key, yielding the original ASCII value, which is subsequently transformed back to its character representation, so finalizing the extraction process. This method demonstrates a robust and efficient approach to steganography, enhancing both the security and reliability of message embedding and extraction while minimizing detectable alterations to the carrier image.[3]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VI. DISCUSSION

The adaptive LSB approach presented in this study enhances both security and detectability reduction. Traditional LSB methods faced challenges in high-security contexts due to detectable pattern changes; however, the adaptive pattern selection approach here addresses this by dynamically choosing the least disruptive bit combinations. By optimizing based on error ratios, the method reduces the visibility of alterations, making detection by steganalysis tools significantly more challenging.

The use of encryption algorithm adds an additional layer of security to the embedded message, mitigating risks even if data extraction is partially successful. This dual approach, combining adaptive LSB embedding with encryption, balances the need for high data capacity with minimal detectability. Despite its robustness, future iterations could benefit from integrating artificial intelligence to dynamically adapt patterns based on media type and complexity.

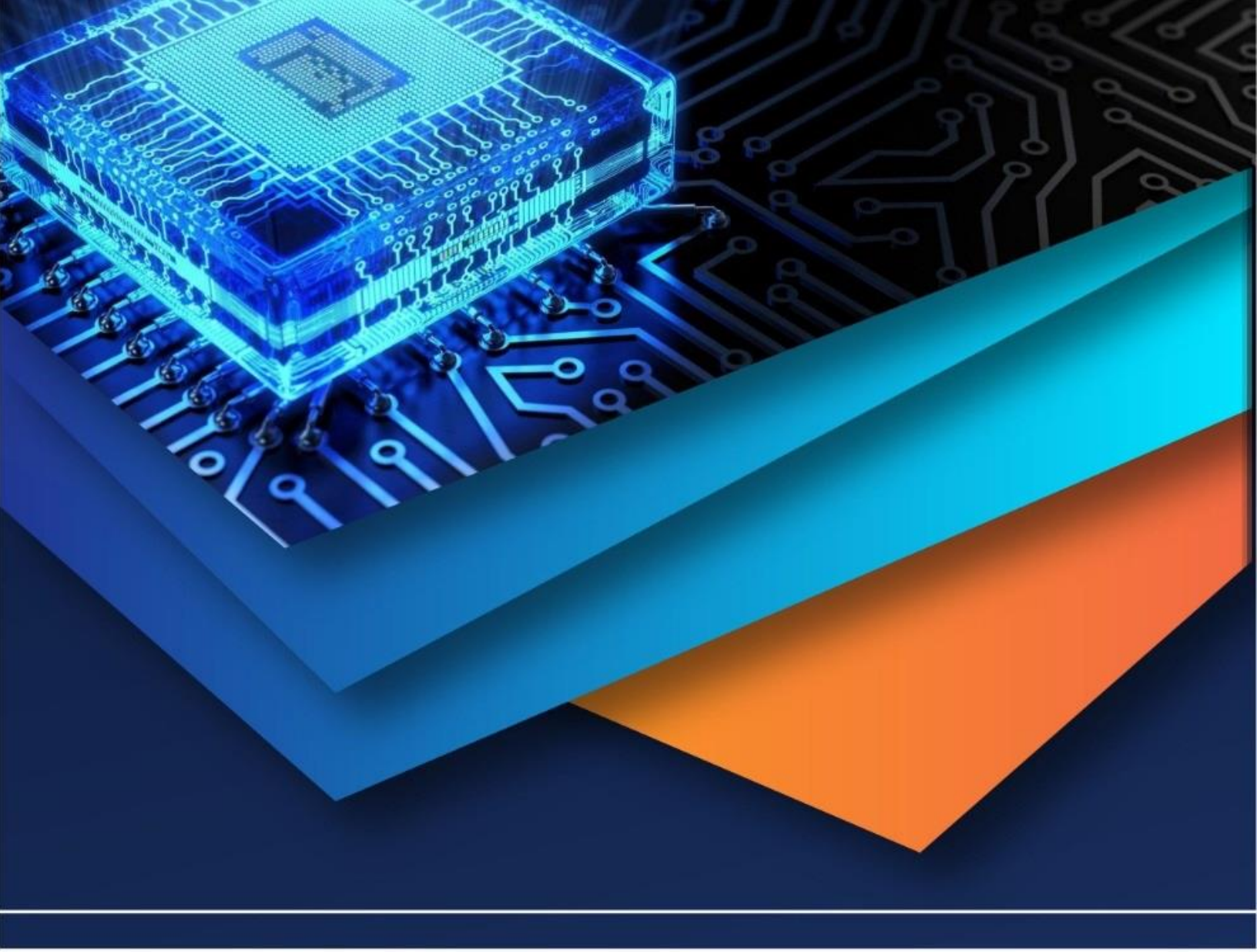
Furthermore, incorporating blockchain or cloud environments may improve traceability and secure distribution in networked applications. While the current approach is highly effective, addressing its dependency on image resolution and size could broaden applicability across diverse media.

VII. CONCLUSION

This research's innovation lies in employing the adaptive pattern to execute the inverted LSB. Prior to embedding the message, the message and container image bits are quantified, and the error ratio for each bit combination is computed. Eight patterns (000 to 111) are employed to invert the least significant bit (LSB) for each combination, comprising 2 bits plus the LSB of the container image pixels. Inverted LSB is executed. To get a reduced error ratio for each pattern. The cumulative sum of all lesser error ratios for each pattern is calculated for every bit combination. The bit combination yielding the minimal error ratio is selected for message embedding. Due to its reliance on the error ratio measurement, the optimal bit combination may vary for different pairs of container images and message sizes. Testing on standardized and less varied medical images demonstrates that the suggested technique effectively enhances imperceptibility, as indicated by PSNR and SSIM metrics. This method can be enhanced in future research by incorporating factors to identify trends and optimize utilizing artificial intelligence techniques.

REFERENCES

[1] Ansari, A.Q.; Khan, M.E.; Pant, M. Data Security by Steganography: A Review, 2019.
[2] Sharma, S.; Parashar, P. Steganography in Images Using LSB Technique, 2020.
[3] Thampi, S.M.; Mukhopadhyay, S.; Moschoyiannis, S. A Survey on Image Steganography, 2015.
[4] Changder, S.; Chakraborty, M.; Sarkar, R. Steganography Techniques and Their Applications in Security, 2001.
[5] Fridrich, J.; Goljan, M.; Du, R. Detecting LSB Steganography in Color and Gray Scale Images, 2001.
[6] Rustad, S.; Setiadi, D.R.I.M.; Syukur, A.; Andono, P.N. Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility.
[7] Chandramouli, R.; Kharrazi, M.; Memon, N. Image Steganography and Steganalysis: Concepts and Practice, 2004.
[8] Cheddad, A.; Condell, J.; Curran, K.; McKevitt, P. Digital Image Steganography: Survey and Analysis of Current Methods, 2010.
[9] Kharrazi, M.; Sencar, H.T.; Memon, N. Image Steganography: Concepts and Practice, 2006.
[10] Qian Shen, Tao Jiang, Yongjun Zhu, Yin Wu. An Improved Image Steganography Scheme Based on Partial Preservation Embedding Algorithm for Wireless Visual Sensor Networks, 2021.
[11] Abbas Cheddad Joan Condell Kevin Curran Paul Mc Kevitt . Digital Image Steganography: Survey and Analysis of Current Methods, 2010.
[12] Sarita Gulia, Saurabh Mukherjee & Tanupriya Choudhury. An Extensive Literature Survey on Medical Image Steganography, 2016.
[13] Donghui Hu, Yu Zhang, Cong Yu, Jian Wang, Yaofei Wang. Image Steganography Based on Style Transfer, 2022.
[14] Kirti D. Nagpal, Prof. D. S. Dabhade. A Survey on Image Steganography & Its Techniques in Spatial & Frequency Domain, 2015.
[15] P. Haridas, G. S. Prajapati, "A Combined Approach of Steganography and Cryptography Techniques for Information Security: A Survey" (International Journal of Engineering Research & Technology ISSN: 2278-0181 vol 4 Issue 12, December 2015)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)