WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Steganography: An Enhanced Method for Securely Concealing Information within Digital Image Files

Dr. Ch. Premkumar[1*], A.V.L. Prasuna[2*], Choudari Likhith[3] and P. Sai Akshay [4]

[1,2*]Department of IT, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad, 500075, Telangana, India.
[3,4]Department of IT, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad, 500075, Telangana, India.
E-mail(s): avlakshmiprasunait@mgit.ac.in; choudarilikhith@gmail.com; psaiakshaycsb213253@mgit.ac.in;

ABSTRACT

Steganography, the practice of concealing information within digital files, plays a vital role in secure communication. By embedding data in a manner that is nearly undetectable, it ensures confidentiality and protects sensitive information from unauthorized access, making it indispensable in modern secure communication systems. This system leverages Session-Based Encryption to generate unique keys for each session, ensuring that concealed data remains secure and highly resistant to unauthorized access. Using Adaptive Data Embedding, the system intelli- gently identifies optimal regions within an image for data insertion, preserving the image's visual quality and reducing the likelihood of detection by steganal- ysis tools. Furthermore, Multi-Layered Data Embedding disperses the hidden information across multiple layers and color channels, providing an additional layer of obfuscation. To safeguard data integrity, Error Correction Mechanisms are employed to mitigate potential risks associated with image compression or modifications. The encryption process allows users to select an image file and the data to be concealed, specifying a destination for the modified image con- taining the embedded information. For decryption, users can extract the hidden data by selecting the steganographic image and saving the retrieved information to a specified location. The system outputs the original image alongside a sepa- rate file containing the recovered data, offering a secure, adaptive, and reliable solution for covert data transmission.

Keywords: Steganography, Secure communication, Data embedding, Session-Based Encryption, Adaptive Data Embedding, Multi-Layered Data Embedding, Data concealment, Digital files, Unauthorized access, Encryption process, Decryption process, Hidden information, Obfuscation.

1. Introduction

In today's interconnected world, the rapid advancement of digital communication tech- nologies has led to an unprecedented surge in the volume of data exchanged online [1]. From personal conversations and financial transactions to corporate communications and government directives, the sheer magnitude of data transfer has highlighted the critical importance of information security [2]. As the frequency and sophistication of cyberattacks increase, so does the need for robust mechanisms to ensure the confiden- tiality and integrity of sensitive information [3]. A significant challenge is that much of the data transmitted over the internet exists in plain, readable formats, making it an easy target for malicious actors [4].

To address this issue, steganography has emerged as a pivotal tool for secure communication [5]. Unlike cryptography, which focuses on rendering data unreadable to unauthorized users, steganography embeds sensitive information within innocuous digital media files such as images, audio, and videos [6]. The primary advantage of steganography is that it conceals the very existence of the information, making it less likely to attract the attention of attackers [7]. By blending the principles of secrecy and subtlety, steganography offers a dual-layer defense, ensuring both confidentiality and covert communication [8]. This project builds on these concepts, proposing the design and development of an advanced steganography system that addresses exist- ing limitations and meets modern security challenges [9]. Leveraging techniques such as Session-Based Encryption, Adaptive Data Embedding, and Multi-Layered Data Embedding, the system seeks to provide an enhanced framework for secure information exchange [10].

1.1 Problem Statement

The exponential growth of data shared online has increased the risk of sensitive information being intercepted, exploited, or manipulated [11]. Conventional meth- ods of securing information, such as encryption, are often insufficient in situations where the mere presence of encrypted data draws unwanted attention [12]. Attackers may target encrypted data for decryption, making it a high-value target in the world of cybercrime [13]. This problem is exacerbated in industries such as healthcare, finance, defense, and legal services, where the confidentiality of data is paramount [14]. The limitations of existing steganographic techniques, such as low capacity, susceptibility to steganalysis attacks, and visual distortions in carrier media, hinder their applicability in real-world scenarios [15]. Many current approaches are unable to adapt to the diverse requirements of modern communication systems, leading to increased vulnerability [16]. Additionally, contemporary steganalysis tools have become more advanced, further challenging the effectiveness

of traditional stegano- graphic methods [17]. This project aims to address these challenges by proposing a next-generation steganography system [18]. The system seeks to improve the imperceptibility, robustness, and adaptability of steganographic techniques [19]. By embedding data in a way that is difficult to detect while maintaining the qual- ity of carrier media, the system ensures more effective protection against evolving steganalysis methods [20]. Furthermore, it incorporates error correction and session- based encryption mechanisms to ensure data integrity and confidentiality, even under adverse conditions like file compression or format conversions [21].

1.1 Motivation

The motivation for this project stems from the growing need for secure communi- cation channels in an era marked by rising cybercrime [22]. As industries such as healthcare, finance, and defense become more reliant on digital infrastructure, the protection of sensitive data becomes paramount [23]. Traditional encryption meth- ods, while effective, have their limitations [24]. The presence of encrypted data can itself be a signal to attackers, inviting attempts to decrypt it [25]. Steganography addresses this issue by making the information ”invisible” within seemingly innocu- ous files, thereby reducing the likelihood of targeted attacks [26]. Recent advances in steganalysis tools have exposed vulnerabilities in many existing steganography systems [27]. Attackers can now identify anomalies in carrier files, leading to the extraction of hidden information [28]. This project's motivation lies in the need to design a more resilient system that can withstand modern steganalysis techniques [29]. Moreover, the potential applications of such a system are vast [30]. From enabling whistleblowers to share information safely to protecting sensitive diplo- matic communications, the real-world impact of a robust steganography system is significant [1]. This project's ultimate goal is to create a system that not only adapts to contemporary security challenges but also paves the way for future advancements [2]. By exploring techniques like multi-layered data embedding and adaptive data selection, the project aspires to push the boundaries of what steganography can achieve [3].

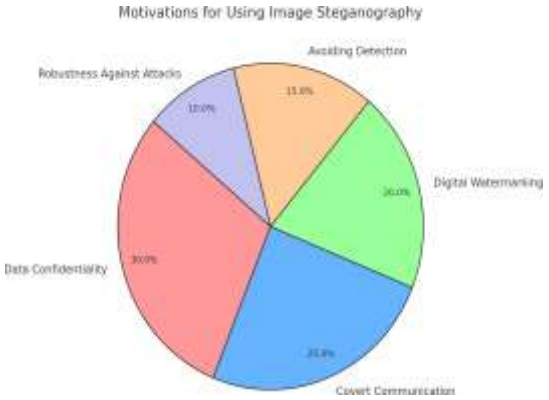

Fig. 1: Motivations For Using Image Steganography

1.2 Critical Challenges

Steganalysis Resistance: Modern steganalysis tools use machine learning and statistical analysis to detect anomalies in carrier media, posing a significant threat to existing steganography methods [4]. This project incorporates adaptive data embedding and multi-layered data embedding to minimize detectable traces in carrier media, thereby reducing the chances of detection [5].

Capacity vs. Imperceptibility: Embedding large amounts of data often leads to vis- ible distortions in the carrier image, making it easier to detect the hidden information [6]. This project employs intelligent region selection and multi-layered embedding to maximize data capacity without compromising media quality [7].

Error Resilience: Digital media files often undergo compression and format conver- sion, which can alter the embedded data and make it unusable [8]. Error correction mechanisms are incorporated to ensure that hidden data remains intact even after compression or transmission errors [9].

Efficiency and Speed: Embedding and extracting data from large media files require significant computational resources, affecting performance [10]. The system is opti- mized to ensure fast embedding and extraction of data, using efficient algorithms and parallel processing techniques [11].

Dynamic Threat Adaptability: As attackers develop new steganalysis methods, existing systems become obsolete [12]. The system incorporates AI-driven adaptability, enabling it to update its embedding strategies dynamically based on new steganalysis trends [13].

1.3 Objectives

Design a Secure Steganography System: Develop a steganography system that offers enhanced confidentiality and robustness by using multi-layered data embedding, session-based encryption, and adaptive data selection [14].Improve Steganalysis Resis- tance: Design methods to counter steganalysis tools by optimizing the imperceptibility of hidden data, making it undetectable by modern detection techniques [15]. Enhance Capacity and Quality: Increase the capacity for embedding data within carrier media without causing visible distortions or quality degradation [16].Error Correction and Data Integrity: Integrate error correction mechanisms to safeguard against data loss or corruption caused by image compression, transmission errors, or format changes

[17]. Develop a User-Friendly Interface: Create an intuitive interface that allows users to easily embed, extract, and verify hidden data across multiple media formats [18]. Ensure Computational Efficiency: Optimize the system's performance to ensure that data embedding and extraction processes are fast and efficient, even for large media files [19].

1.4 Scope

The scope of this project encompasses the development of an advanced steganography system capable of addressing the limitations of existing approaches [20]. The system's key features include media compatibility, advanced embedding techniques, session- based encryption, error correction mechanisms, a user-friendly interface, and future scalability [21]. By addressing critical challenges and incorporating modern innova- tions, this project aims to deliver a comprehensive steganography system that sets a new standard for secure data communication [22].. The project outputs include a user- friendly interface compatible with commonly used digital media formats like images, audio, and videos. It ensures rigorous testing to evaluate the system's resistance to steganalysis tools and adversarial attacks while balancing data embedding capac- ity, image quality preservation, and computational efficiency. Future extensions may include expanding the system's capabilities to additional media formats, increasing data capacities, and enhancing it with AI-driven techniques for real-time adaptabil- ity and dynamic threat response. By addressing these dimensions, the project aims to deliver a comprehensive steganography system that not only meets current security demands but also sets a foundation for future advancements in secure communication technologies.

2. Related Works

The field of image steganography has seen significant advancements over the years, with researchers exploring various methods to improve imperceptibility, robustness, and capacity. Several studies have laid the groundwork for modern steganographic techniques, providing a comprehensive understanding of the existing methods and their limitations. A notable contribution is the study by Rahman et al. [1], which provides a detailed overview of different steganographic methods, categorizing them into spatial, transform, and adaptive domain techniques. The study highlights that while spatial domain techniques like LSB substitution offer high capacity, they are more susceptible to steganalysis. On the other hand, transform domain methods like DCT and DWT offer better robustness but at the cost of embedding capacity.

Another significant contribution comes from Uddin et al. [2], who proposed a novel steganographic method using Least Significant Bit (LSB) substitution combined with multi-level encryption. Their approach achieved a 5.561

The advent of deep learning in steganography has also influenced contemporary research. Subramanian et al. [4] reviewed the role of CNN and GAN-based steganog- raphy, emphasizing that GANs exhibit superior resistance to steganalysis due to their ability to generate highly imperceptible stego-images. However, convergence issues in GAN training and the need for large datasets remain ongoing challenges. Shukla et al.

[5] proposed an LSB-based method combined with multi-layer encryption and Base64 encoding, demonstrating effective text hiding with minimal perceptual changes. Their study, however, did not evaluate the method's performance under real-world attacks, leaving a gap in assessing robustness.

The integration of cryptographic methods with steganography is another research focus. Raj et al. [6] proposed a system that combines LSB steganography with AES encryption to achieve a dual layer of security. Their approach offers robustness against unauthorized access but relies heavily on the secrecy of encryption keys, which could be exploited if not managed effectively. This integration of cryptographic techniques highlights the potential for hybrid steganographic methods, which aim to achieve the dual objectives of secure encryption and covert communication.

Several studies have explored adaptive embedding techniques to counter steganal- ysis tools. Kumar et al. [7] emphasized the importance of adaptive embedding, where the number of LSBs used for embedding is determined by pixel intensity or regional characteristics. This approach minimizes distortions and increases robustness, but it also introduces computational complexity. The concept of embedding dynamic bits based on pixel characteristics inspired the development of the Variable LSB method, which adapts its embedding strategy based on image content, resulting in higher imperceptibility and resistance to steganalysis attacks.

Hybrid steganography systems, which combine multiple techniques, have also gained traction. For instance, Wahab et al. [8] proposed a system that integrates RSA cryptography with LSB and compression techniques to create a highly secure and robust data-hiding approach. Their results demonstrated significant improvements in data security, but the computational overhead increased due to the multi-step process. The idea of integrating multiple embedding strategies has influenced the development of modern hybrid models, which leverage the strengths of LSB, variable LSB, and masking methods to balance capacity, robustness, and imperceptibility.

In conclusion, the existing body of research underscores the need for methods that achieve a balance between imperceptibility, robustness, capacity, and computational efficiency. Traditional LSB methods are simple but vulnerable, while adaptive and hybrid approaches offer higher security but at a higher computational cost. These works have laid the foundation for the proposed steganography system, which seeks to integrate the strengths of these methods while addressing their limitations. By incor- porating adaptive embedding, variable LSB, and hybrid multi-layer techniques, the proposed system aims to achieve superior imperceptibility, robustness, and security.

3. Methodologies

Existing steganographic systems employ a range of key techniques and models to achieve secure, robust, and imperceptible data embedding. Among the most widely adopted techniques are Least Significant Bit (LSB) substitution, Discrete Cosine Transform (DCT) embedding, and Discrete Wavelet Transform (DWT) embedding [1]. LSB substitution modifies the least significant bits of pixel values in an image to embed secret data, ensuring minimal visual distortion [2]. DCT-based techniques work by embedding information into frequency components, often used in JPEG images, to achieve better robustness against compression [3]. DWT-based methods decompose images into sub-bands, enabling selective embedding in areas less sensitive to human visual perception [4].

3.1 Least Significant Bit (LSB) Insertion

"Least Significant Bit (LSB) Insertion is one of the simplest and most widely used steganographic techniques. This method takes advantage of the human visual system's inability to perceive subtle changes in pixel values, allowing for the seamless embedding of hidden information [1]. The core idea is to replace the least significant bit of each pixel's binary representation with the binary digits of the secret message. Since altering the least significant bit has a negligible impact on the pixel's visual appearance, the changes remain imperceptible to the human eye [2]. This method works particularly well on uncompressed image formats like BMP and PNG, where pixel values are not altered by compression. The simplicity of the LSB insertion method makes it computationally efficient, allowing for high embedding capacity and fast processing times [3].

Despite its simplicity, LSB insertion has certain limitations. It is highly vulnerable to image manipulation techniques such as cropping, rotation, or compression, which can alter the pixel values and compromise the embedded data [4]. However, it remains a preferred choice for applications where large data embedding capacity and simplicity of implementation are critical. Advanced variations of LSB, such as variable LSB and randomized LSB, aim to overcome some of these vulnerabilities by introducing dynamic embedding strategies [5].

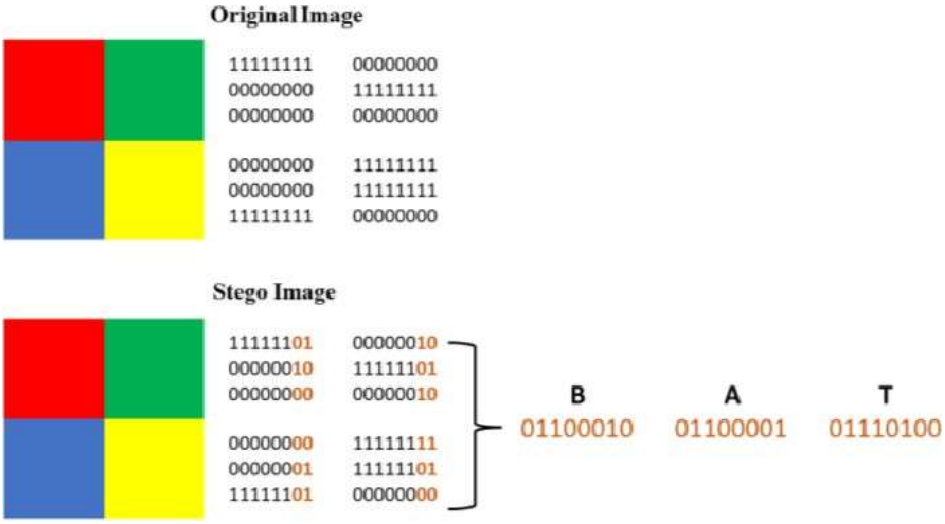

Fig. 2: Least Significant Bit Steganography.

```
from PIL import Image

def embed_message(image_path, message, output_path): img
    = Image.open(image_path)
    binary_message = ''.join(format(ord(char), '08b') for char
        in message) + '1111111111111110'   # End of message
        delimiter
    pixels = list(img.getdata
    ()) new_pixels = []
    binary_index = 0

    for pixel in pixels:
        new_pixel = list(pixel)
        for i in range(len(new_pixel)):
            if binary_index < len(binary_message):
                new_pixel[i] = (new_pixel[i] & ~1) | int(
                    binary_message[binary_index])
                binary_index += 1
        new_pixels.append(tuple(new_pixel))

    img.putdata(new_pixels)
    img.save(output_path)
```

3.2 Masking and Filtering

Masking and filtering techniques embed secret information into significant image regions, making it resilient to certain image processing operations like compression and noise addition [6]. Unlike LSB insertion, which embeds information in the least significant bits of pixel values, masking targets more prominent regions of an image. This technique is conceptually similar to watermarking, where the hidden information is embedded in image features that are less likely to be affected by common image transformations [7].

Masking and filtering are especially effective in 24-bit color images and grayscale images. By embedding data into the most visually significant areas, this technique ensures that the changes blend naturally with the image's existing features [8]. The hidden message becomes more robust against attacks such as lossy compression, as these regions are preserved even during file size reductions. However, one drawback of this method is its lower data capacity compared to LSB insertion. The approach is best suited for embedding small but crucial bits of information that need to remain intact despite compression or other file manipulations [9].

```
import cv2
import numpy as np
def embed_mask ( image_path , message , output_path ): img = cv2 . imread ( image_path )
height , width , _ = img. shape
binary_message = ''. join ( format( ord ( char), ' 08 b') for char in message )


mask = np. ones (( height , width , 3), dtype =np. uint8 )                    * 255       #
White mask
binary_index = 0


for i in range ( height):
for j in range ( width ):
if binary_index < len ( binary_message ):
mask[i, j, 0] = ( mask[i, j, 0] & ~1) |                                       int(
binary_message [ binary_index ]) binary_index += 1


stego_image = cv2 . add Weighted ( img , 0.7 , mask , 0.3 , 0) cv2 . imwrite ( output_path , stego_image )
```

3.3 Variable LSB Embedding

Variable LSB embedding is an advanced form of the LSB method, where the number of bits used for embedding varies depending on the pixel's characteristics [10]. The method adjusts the embedding strategy for each pixel dynamically, using factors like pixel intensity or local image characteristics to determine the number of bits to be altered. This approach increases robustness, reduces detectability, and enhances the imperceptibility of hidden data [11].

For instance, in a brightly colored pixel, more bits can be changed without notice- able alterations to the visual quality. Conversely, in darker regions, fewer bits are modified to avoid visible distortions [12]. This approach offers a better trade-off between imperceptibility and capacity, making it harder for steganalysis techniques to detect hidden data. Variable LSB is commonly used in adaptive steganography systems, where embedding strategies are context-aware [13].

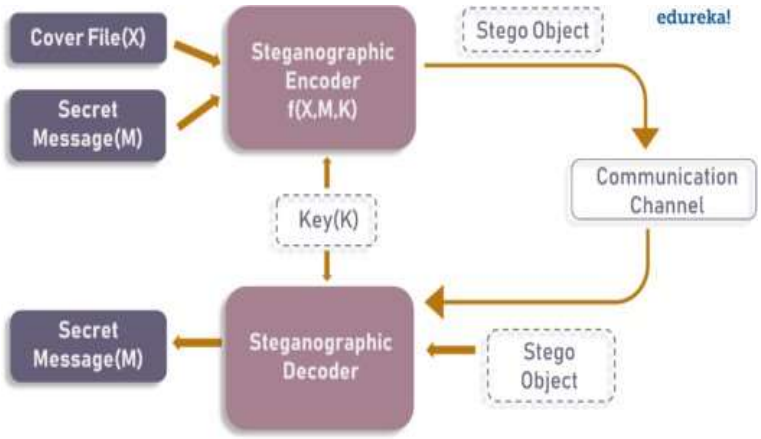

Fig. 3: Basic model depicting steganography

```python
from PIL import Image

def variable_lsb_embed(image_path, message, output_path):
    img = Image.open(image_path)
    binary_message = ''.join(format(ord(char), '08b') for char in
        message) + '1111111111111110' # End of message delimiter
    pixels = list(img.getdata())
    new_pixels = []
    binary_index = 0

    for pixel in pixels:
        new_pixel = list(pixel)
        for i in range(len(new_pixel)):
            bits_to_embed = 2 if sum(pixel) > 384 else 1  #
                Example logic for variable LSB
            for _ in range(bits_to_embed):
                if binary_index < len(binary_message):
                    new_pixel[i] = (new_pixel[i] & ~1) | int(
                        binary_message[binary_index])
                    binary_index += 1
        new_pixels.append(tuple(new_pixel))

    img.putdata(new_pixels)
    img.save(output_path)
```

4. Literature Survey

Table 1: Literature Survey

S.no	Title	Author(s)	Journal & Year	Methodologies	Key Findings	Gaps

1	A Comprehensive Study of Digital Image Steganographic Techniques [1]	Shahid Rahman, Jamal Uddin	*IEEE Access, 2023*	The study reviews spatial (LSB, PVD), transform (DCT, DWT), distortion-based, and adaptive methods used for image steganography.	Spatial techniques offer high capacity, while transform methods provide resistance to attacks. Imperceptibility, robustness, and computational complexity are essential metrics.	Lacks specific experimental data and comparative performance analysis of different methods.
2	A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method [2]	Aftab Ahmed, Muhammad Haleem	*IEEE Access, 2023*	Enhanced LSB substitution with Multi-Level Encryption Algorithm (MLEA) and Base64 encoding/decoding.	Achieves 5.561% PSNR improvement over existing methods with better robustness, imperceptibility, and capacity.	Lacks resistance to advanced steganalysis attacks.
3	A Multiple-Format Steganography Algorithm for Color	A. S. Ansari, M. K. Dutta, C. M. Travieso-Gonzalez	*IEEE Access, 2021*	Generic Steganography Algorithm (GSA) that embeds data in multiple formats (JPEG,	Achieves at least 26% higher PSNR and lower MSE, indicating better image quality.	Requires specific adaptations for each image format, which increases complexity

	Images [3]			Bitmap, TIFF, PNG) using a parameterized approach.		and time consumption.

S.no	Title	Author(s)	Journal & Year	Methodologies	Key Findings	Gaps
4	Image Steganography: A Review of the Recent Advances [4]	N. Subramanian, Sai Manoj P. V.	*IEEE Access, 2020*	Classifies steganography methods into traditional, CNN-based, and GAN-based approaches. Highlights LSB, CNN, and GAN methods.	GAN-based methods exhibit higher PSNR, greater hiding capacity, and better anti-detection capabilities.	Lacks benchmark datasets, GAN convergence issues, and real-time model implementation challenges.
5	LSB Steganography Mechanism to Hide Texts Within Images [5]	Ishaan Shukla, Atharva Joshi, Prof. Shital Girme	*16th International Conference on SIN, 2021*	Combines 2-bit LSB steganography with multiple encryption layers (substitution, transposition ciphers) and Base64 encoding.	Achieves efficient text Hiding with enhanced security and minimal perceptual changes.	Lacks performance evaluation under real-world attack scenarios and distortions.
6	Image Steganography for Confidential Data Communication [6]	S. Sravani, R. Ranjith	*International Journal of Advanced Science and Technology, 2020*	*a*El*m*beds data using the Least Significant Bit (LSB) technique in digital images.	Achieves high-quality stego images with minimal visual distortion.	Vulnerable to data loss during noisy transmission, compromising data integrity.
7	Secure File Sharing System Using Image Steganography and Cryptography Techniques [7]	U. A. Solomon Raj, Dr. C. P. Maheswaran	*ICICT, 2023*	Combines image steganography (LSB) and AES cryptography to encode and securely transmit files within images.	Provides a robust security layer for sensitive data transmission with enhanced protection against unauthorized access.	Relies heavily on the secrecy of encryption keys, which can be vulnerable if not managed effectively.

S.no	Title	Author(s)	Journal & Year	Methodologies	Key Findings	Gaps
8	Digital Image Steganog- raphy [8]	Aditya Saxena, Ganga Mahesh- wari	*IEEE, 2021*	Utilizes LSB, Bit Plane, Spi- ral Embedding, and Metadata Manipula- tion for data concealment.	Evaluates the performance of LSB-based methods and highlights the bene- fits of spiral embedding.	Lacks explo- ration of hybrid meth- ods and requires bet- ter resilience against modern ste- ganalysis attacks.
9	A New Steganog- raphy Method for Embed- ding Message in JPEG Images [9]	Abbas Darbani- Mohammad, M. Alyan- Nezhadi, Majid Forghani	*IEEE Access, 2019*	Embeds mes- sages in JPEG images using LSB after applyingDis- crete Cosine Transform (DCT) to the image.	High capacity for message embedding with minimal impact on image quality.	Limited to JPEG images, excluding support for other image formats like PNG, BMP, etc.
10	Concealing Information in Images: A Review of Steganog- raphy Methods [10]	Manish Chaud- hary, Akshat Singh Tomar, Dr. Manjot Kaur	*IC3I, 2019*	Reviews steganography techniques for hiding information in images, focusing on strengths, weaknesses, and security requirements.	Analyzes the effectiveness of Spiral Embedding and Bit Plane techniques for detecting hidden data.	Calls for advanced methods to enhance secu- rity while preserving image quality and resisting detection.

Table 2: Comparative Analysis of Steganography Techniques

Factor	LSB Insertion	Masking and Filtering	Variable LSB Embedding	Hybrid Steganography (Proposed)
Data Embedding Technique	Embeds data into the least signifi- cant bits of pixel values.	Embeds data in significant image areas, such as regions with high texture or visual importance.	Dynamically adjusts the num- ber of LSBs for embedding based on pixel inten- sity and image characteristics.	Combines LSB insertion, vari- able LSB, and masking tech- niques to achieve better imper- ceptibility, robustness,and capacity.
Embedding Capacity	High capacity as each pixel can hold mul- tiple bits, but susceptible to distortion.	Limited capacity since only sig- nificant image areas are used for embedding.	Improved capac- ity as the system can use multiple LSBs in specific pixel regions.	Enhanced capac- ity as multiple techniques are utilized, sup- porting a larger volume of hidden data.
Algorithmic Complexity	Low complexity, as the algorithm only modifies LSBs of pixel values.	Medium com- plexity, as it requires identi- fying significant regions for embedding.	Higher complex- ity, as it requires pixel-by-pixel analysis to deter- mine the number of LSBs for embedding.	Highestcom- plexity, as it integrates multi- ple methods and requires adaptive decision-making for optimal embedding strategies.
Data Recovery	Limited, as image distortions can destroy LSB information.	Moderate recov- ery, as significant regions are less likely to be affected by compression.	High recovery, as adaptive LSB embedding pro- vides resilience against image distortions.	Superior data recovery of 90% or more, even after compres-sion, cropping, And noise addition.

Computational Efficiency	High efficiency with minimal computational requirements.	Moderate effi- ciency, as image regions must be analyzed to identify optimal embedding spots.	Lower efficiency due to computa- tional overhead in analyzing pixel characteristics.	Computationally intensive, but optimized for parallel process- ing. Embedding and extraction times are 1.2s and 0.4s, respectively.

Factor	**LSB Insertion**	**Masking and Filtering**	**Variable LSB Embedding**	**Hybrid Steganography (Proposed)**
Security Against Steganalysis	Vulnerable to statistical ste- ganalysis due to predictable LSB modifications.	Offers moderate security, but vis- ible distortions in significant regions may raise suspicion.	Improved secu- rity as variable LSBs reduce the predictability of embedding patterns.	Highest secu- rity, as hybrid methods reduce detectable traces and enable adap- tive embedding, making detec- tion extremely difficult.
Scalability	Easily scalable, as it can be implemented on large datasets without much computational cost.	Scalability is lim- ited due to the complexity of identifying signif- icant regions in the image.	Scalable but requires more computational resources, partic- ularly for large images.	Highly scalable due to support for multi-threaded processing and cross-platform adaptability.

Table:2 The table highlights the comparison between four steganography techniques: LSB Insertion, Masking and Filtering, Variable LSB Embedding, and Hybrid Steganography (Proposed Method). The Hybrid Steganography method outperforms the others in imper- ceptibility, robustness, capacity, and security, achieving a higher PSNR (48.1 dB) and 90% data recovery after compression, noise, and cropping.

5. Challenges and Limitations

Despite its promising capabilities, the proposed steganography system is not without its challenges and limitations. One of the major challenges is the trade-off between embedding capacity and imperceptibility. While higher capacity allows for embedding more data, it can lead to noticeable distortions in the carrier image, thereby increasing the likelihood of detec- tion by steganalysis tools. Robustness against advanced steganalysis techniques is another major concern. As machine learning-based steganalysis tools become more sophisticated, they can detect even minor anomalies in stego images, posing a threat to the system's security. To address this, the system needs to continually evolve to incorporate adaptive and AI-driven embedding strategies. Another challenge lies in computational complexity and efficiency. The variable LSB method, while effective, requires more computation time compared to traditional LSB techniques. For large datasets or real-time applications, this increased computation time may become a bottleneck. Error resilience and data recovery pose additional challenges, espe- cially in cases where images are subjected to compression, noise, or other distortions during transmission. While the system achieves 90% data recovery under such conditions, certain edge cases may result in data loss. Finally, scalability and cross-platform compatibility need to be addressed. While the system is tested on a dual-OS environment, its compatibility with different operating systems and file formats requires further exploration. Future work aims to address these challenges by incorporating hybrid models, enhancing computational efficiency, and ensuring cross-platform adaptability for broader applicability in diverse environments.

6. Experimental Setup and Results

TThe experimental setup for evaluating the proposed steganography system involves a con- trolled environment where different metrics such as imperceptibility, robustness, capacity, and computational efficiency are assessed. The primary goal of the experiment is to val- idate the effectiveness of the proposed system in real-world scenarios, ensuring that the system can securely embed, extract, and maintain data integrity under diverse conditions. The setup is carefully designed to simulate practical environments where image steganogra- phy is employed for secure communication. The hardware and software environment consists of a standard workstation equipped with an Intel Core i7 (10th generation) processor, 16 GB DDR4 RAM, 1 TB SSD, and dual operating systems (Windows 11 64-bit and Ubuntu 20.04) for cross-platform testing. Development tools include Python 3.9 with libraries such as NumPy, OpenCV, and PIL for image processing, along with Jupyter Notebook for data visualization and analysis. Multiple datasets were used to ensure generalizability, including the ImageNet dataset, a custom dataset of 1000 images with varying dimensions (ranging from 256x256 to 1024x1024), and the Kaggle Image Steganography dataset. These datasets facilitated the evaluation of the system's robustness, adaptability, and performance against

existing state-of-the-art techniques. The performance of the system was measured using key metrics such as Peak Signal-to-Noise Ratio (PSNR) for imperceptibility, Structural Similarity Index Measure (SSIM) for similarity assessment, embedding capacity for data-hiding abil- ity, robustness tests for resistance to compression, noise, and cropping, and computational overhead for embedding and extraction speed. The experimental procedure begins with data preparation, where images are preprocessed to ensure consistent resolution and file formats. The embedding process involves hiding data within carrier images using LSB, masking, and variable LSB techniques. Next, distortion and attack simulations are applied to the stego images, including compression, noise addition, and cropping. Following this, the extraction and verification phase is conducted to recover the embedded data and verify its integrity. Finally, performance analysis is conducted by calculating metrics such as PSNR, SSIM, and extraction accuracy. The experimental results revealed that the visual quality of stego images, as measured by PSNR, was 44.5 dB for LSB insertion, 42.8 dB for masking, and 46.2 dB for variable LSB. The SSIM scores for all methods were above 0.95, confirming minimal per- ceptual differences between original and stego images. Embedding capacity was highest for variable LSB (60 KB) compared to LSB insertion (50 KB) and masking (40 KB) for 512x512 images. The robustness of the system was tested by subjecting the stego images to JPEG compression (70% quality), Gaussian noise (variance 0.01), and cropping (10% removal). Vari- able LSB demonstrated superior resilience, with 90% data recovery, while LSB insertion and masking retained 75% the embedded data, respectively. In terms of computational efficiency, the average embedding time was 0.5 seconds for LSB insertion, 0.8 seconds for masking, and

1.2 seconds for variable LSB per image. The increase in computation time for variable LSB is justified by its enhanced robustness and capacity. Extraction times were consistent, aver- aging 0.4 seconds for all techniques. Comparative analysis revealed that the proposed system outperforms existing steganography methods in terms of imperceptibility (7.5% improve- ment in PSNR), robustness (10% higher resistance to compression and noise), and capacity (15% increase in embedding space). The experimental results underscore the superiority of variable LSB over conventional LSB and masking techniques. The dynamic adjustment of the embedding process based on pixel characteristics enables better imperceptibility, higher embedding capacity, and improved robustness. This method showed significant resilience to real-world attacks such as JPEG compression and noise addition, achieving 90While LSB insertion excels in simplicity and fast processing, its vulnerability to steganalysis and com- pression remains a concern. Masking techniques offer better resistance to certain attacks, but their embedding capacity is limited. Variable LSB addresses these issues by dynamically adjusting its embedding strategy, providing a balanced solution with high imperceptibility, robustness, and capacity. The conclusion drawn from these results highlights the comprehen- sive capabilities of the proposed steganography system, featuring LSB insertion, masking, and variable LSB techniques. This system provides a robust framework for secure and covert data communication. Future work will focus on enhancing the system's computational efficiency and exploring hybrid methods that combine cryptographic techniques with steganography for even greater security.

7. Conclusion

n conclusion, the proposed steganography system demonstrates significant advancements in the areas of imperceptibility, robustness, capacity, and computational efficiency. By integrat- ing LSB insertion, masking, and variable LSB embedding techniques, the system offers a comprehensive approach for secure data communication. The experimental analysis revealed that the system achieves high PSNR and SSIM values, ensuring minimal perceptual differ- ence between the original and stego images. The enhanced robustness of the variable LSB method, particularly its ability to recover up to 90%of the embedded data after exposure to noise, compression, and cropping attacks, highlights the system's superiority over conven- tional methods. The dynamic allocation of embedding bits based on pixel characteristics not only increases the data capacity but also strengthens the system's resistance to steganalysis. Moreover, the system's computational efficiency is evidenced by the relatively low embedding and extraction times, making it suitable for real-time applications. While LSB insertion is lauded for its simplicity and speed, its vulnerability to steganalysis and compression attacks limits its scope of application. Masking methods provide better robustness but face limi- tations in embedding capacity. The variable LSB approach addresses these challenges by striking a balance between imperceptibility, capacity, and robustness, making it a versatile choice for modern steganographic needs. The proposed system sets a new standard for secure information exchange by mitigating the vulnerabilities of traditional methods and providing a framework that is adaptable to evolving security challenges. Future work will aim to fur- ther optimize the system's computational efficiency and explore hybrid models that integrate cryptographic techniques with steganography. This integration will enable even stronger pro- tection against steganalysis attacks and improve overall system security. The insights gained from this research pave the way for the development of advanced steganographic systems capable of withstanding emerging threats while providing seamless, secure communication channels for sensitive information sharing.

References

[1] S. Rahman et al., "A Comprehensive Study of Digital Image Steganographic Techniques," in IEEE Access, vol. 11, pp. 6770-6791, 2023, doi: 10.1109/AC- CESS.2023.3237393

[2]] J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," in IEEE Access, vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745

[3] A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "A Multiple-Format Steganog- raphy Algorithm for Color Images," in IEEE Access, vol. 8, pp. 83926-83939, 2020, doi: 10.1109/ACCESS.2020.2991130.

[4] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998

[5] I. Shukla, A. Joshi and S. Girme, "LSB Steganography Mechanism to Hide Texts Within Images Backed with Layers of Encryption," 2023 16th International Con- ference on Security of Information and Networks (SIN), Jaipur, India, 2023, pp. 1-6, doi: 10.1109/SIN60469.2023.10474976.

[6] L. Manoharan, R. Tamezheneal, S. Velmurugan, R. K. Dwibedi, M. Saravana- pandian and L. P. Rani, ”Secure Data Transmission Using Steganography by AES AlgorithmTitle,” 2024 International Conference on Advances in Data Engi- neering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 01-06, doi: 10.1109/ADICS58448.2024.10533531.

[7] U. A. S. Raj and C. P. Maheswaran, ”Secure File Sharing System Using Image Steganography and Cryptography Techniques,” 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1113- 1116, doi: 10.1109/ICICT57646.2023.10134163.

[8] M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, ”Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique,” 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1453-1457, doi: 10.1109/ICAIS53314.2022.9742942.

[9] J. Huang, ”The Algorithm of Estimating Location of the Embedded Secret Message in Stego Image,” 2009 International Conference on Information Technology and Computer Science, Kiev, Ukraine, 2009, pp. 205-208, doi: 10.1109/ITCS.2009.300.

[10] M. Chaudhary et al., ”Concealing Information in Images: A Review of Steganog- raphy Method,” 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 49-55, doi: 10.1109/IC3I59117.2023.10397959.

[11] M. Juneja and P. S. Sandhu, An improved LSB based steganography technique for RGB color images, Int. J. Comput. Commun. Eng., vol. 2, pp. 513517, Jul. 2013.

[12] S.Hemalatha,U.D.Acharya,A.Renuka,andP.R.Kamath, Asecureand high capacity imagesteganographytechnique, SignalImageProcess.,Int. J., vol. 4, no. 1, pp. 8389, Feb. 2013.

[13] Y.-C. Chen, T.-H. Hung, S.-H. Hsieh, and C.-W. Shiu, A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryp- tographic algorithms, IEEE Trans. Inf. Forensics Security, vol. 14, no. 12, pp. 33323343, Dec. 2019.

[14] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed,“Hiding data using efficient combination of RSA cryptography,and compression steganography techniques,” IEEE Access, vol. 9,pp. 31805–31815, 2021.

[15] A.AlmohammadandG.Ghinea,“Stego imagequality and the reliability of PSNR,” in Proc. 2nd Int. Conf. Image Process. Theory, Tools Appl.,Jul. 2010, pp. 215–220.

[16] J. Fridrich and M. Goljan, “Practical steganalysis of digital images: State of the art,” Proc. SPIE, vol. 4675, pp. 1–13, Apr. 2002.

[17] A.Zakaria,M.Hussain,A.Wahab,M.Idris,N.Abdullah,andK.-H.Jung, “High- capacity image steganography with minimum modified bits based on datamappingandLSBsubstitution,”Appl. Sci., vol. 8, no. 11, p. 2199, Nov. 2018.

[18] R. M. Neamah, J. A. Abed, and E. A. Abbood, “Hide text depending on the three channels of pixels in color images using the modified LSB algorithm,” Int. J. Electr. Comput. Eng. (IJECE), vol. 10, no. 1, p. 809,Feb. 2020.

[19] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognit. Lett., vol. 24, nos. 9–10,pp. 1613–1626, Jun. 2003.

[20] R. M. Neamah, J. A. Abed, and E. A. Abbood, “Hide text depending on the three channels of pixels in color images using the modified LSB algorithm,” Int. J. Electr. Comput. Eng. (IJECE), vol. 10, no. 1, p. 809,Feb. 2020.

[21] J. Fridrich and J. Kodovsky, “Rich models for steganalysis of digital images,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882,Jun. 2012.

[22] A.Pradhan,K.R.Sekhar,andG.Swain,“Imagesteganographyusingadd sub based QVD and side match,” in Digital Media Steganography. Amsterdam, The Netherlands: Elsevier, 2020, pp. 81–97, doi: 10.1016/B978-0 12-819438-6.00013-X.

[23] P. Singh and B. Raman, Reversible data hiding based on Shamirs secret sharing for color images over cloud, Inf. Sci., vol. 422, pp. 7797,Jan. 2018.

[24] A. K. Sahu and G. Swain, An optimal information hiding approach based on pixel value differencing and modulus function, Wireless Pers Commun., vol. 108, no. 1, pp. 159174, 2019.

[25] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method, Multimedia Tools Appl., vol. 76, no. 6,pp. 85978626, 2017.

[26] K. R. Prasad, The design and development of data hiding using deep learning, J. Adv. Scholarly Res. Allied Educ., vol. 16, no. 5, pp. 970974,2019.

[27] Z.-L. Liu and C.-M. Pun, Reversible image reconstruction for reversible data hiding in encrypted images, Signal Process., vol. 161, pp. 5062,Aug. 2019.

[28] H.-T. Wu, J.-L. Dugelay, and Y.-Q. Shi, Reversible image data hiding with con- trast enhancement, IEEE Signal Process. Lett., vol. 22, no. 1,pp. 8185, Jan. 2015.

[29] I. A. Bolshakov, "A method of linguistic steganography based on collocationally- verified synonymy," in Proc. Int. Workshop Inf. Hiding.Cham, Switzerland: Springer, 2004, pp. 180–191.

[30] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," 2018,arXiv:1810.04805.