WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

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

# Image Steganography: Unveiling Secrets through Hidden Artistry

***Somnath Biswas[1], Sarbani Sarkar[1], Sasmit De[1]***

[1]Department of CSE; JIS College of Engineering, Kalyani, West Bengal

**ABSTRACT –**

Image Steganography is a specialized subset of steganography that focuses on hiding data within digital photographs. This method enables secure data transmission by concealing important information within the aesthetics of images. Through various techniques, the secret message is encoded and integrated into the cover image without perceptible alterations. Considerations such as the cover image's capacity, encoding process, and desired security level are crucial for successful image steganography. Encryption of the payload enhances message security, ensuring its protection even if discovered. Steganalysis techniques aid in detecting images with hidden information by analyzing statistical characteristics, noise patterns, and inconsistencies. Image steganography offers a means to securely hide data within digital photographs, facilitating covert communication and safeguarding privacy. Ongoing advancements in steganography and steganalysis techniques continuously shape data security and privacy in the realm of digital images, driving the evolution of embedding and detection methods.

**Keywords:** image steganography, data hiding, secret message, cover image, encoding, security, steganalysis, encryption, data security, privacy.

## Introduction –

Image steganography, a robust and sophisticated technique, is extensively utilized for concealing sensitive and confidential information within the pixels of an image while keeping its original appearance intact. This innovative approach falls under the broader realm of steganography, an intriguing field dedicated to the art of clandestine data concealment in diverse media formats. Within the domain of image steganography, the primary objective revolves around seamlessly embedding covert or classified data within an image file, rendering it imperceptible to the naked eye and unsuspecting observers. At its core, image steganography encompasses two pivotal components: the cover image and the hidden message. The cover image serves as the unsuspecting carrier for the concealed information, while the hidden message encapsulates the crucial data that necessitates covert protection. The true challenge lies in executing a seamless integration of the hidden message into the cover image, ensuring its surreptitious existence eludes even the most vigilant scrutiny. The realm of image steganography harbors an extensive array of methodologies, with the popular Least Significant Bit (LSB) substitution approach commanding significant attention. In the realm of LSB substitution, the least significant bits of the cover image's pixel values gracefully relinquish their original place to accommodate the bits from the hidden message. These subtle modifications made to the least significant bits remain virtually invisible to casual observation, as they exert minimal influence on the overall visual attributes of the image. Consequently, the artistry of image steganography lies in its ability to seamlessly merge hidden data with the aesthetics of the cover image, rendering the concealed message inconspicuous to unsuspecting eyes. Detecting instances of image steganography poses a formidable challenge, primarily due to the deliberately discreet nature of the alterations imposed upon the cover image. To overcome this obstacle, steganalysis techniques emerge as indispensable tools in identifying potential modifications in images and skillfully distinguishing innocent images from those harboring covert information. These advanced techniques meticulously analyze statistical characteristics, discern noise patterns, and scrutinize inconsistencies embedded within the images to unearth subtle yet telltale signs of potential steganographic alterations.

The effectiveness of image steganography hinges upon numerous factors, including the cover image's capacity to accommodate the hidden message, the intricacy of the employed encoding algorithm, and the desired level of security. Advanced techniques, rooted in the discrete cosine transform (DCT) or the spread spectrum methodology, unlock enhanced embedding capabilities while fortifying resilience against state-of-the-art steganalysis approaches. However, it is vital to acknowledge the inherent limitations within image steganography. The embedding process, albeit imperceptible to the human eye, may introduce marginal distortions to the cover image. Furthermore, the relentless evolution of steganalysis algorithms serves as an ongoing and unyielding test to the effectiveness and robustness of image steganography techniques.

The practical applications of image steganography transcend beyond the mere concealment of data, unveiling its true potential in enabling secure communication channels and safeguarding confidential data transmissions. The hidden message remains an enigma, accessible solely to individuals equipped with the requisite decoding tools or possessing the inherent knowledge to unlock its concealed contents. Augmenting the security of the hidden information, encryption techniques find their place in image steganography, adding an additional layer of impregnability to the covert message. Moreover, image steganography finds fertile ground in various domains where secure communication and impervious data protection stand as paramount concerns. Within the realm of digital forensics, image steganography emerges as a potent tool for covert communication or discreetly shielding evidence from

prying eyes. Additionally, the field of watermarking leverages image steganography to embed invisible information within images, serving purposes such as establishing ownership or validating the integrity and authenticity of the content.

## Literature Survey –

S. Nagaraj and K. K. Gowda's "A Survey on Image Steganography and Steganalysis Techniques" (2015) [1] provides an overview of image steganography methods, including LSB replacement, spatial domain techniques, and frequency domain methods, while also discussing steganalysis techniques.

In their review paper titled "Steganography Techniques: A Review Paper" (2016), S. S. Manjunath and N. Chandrakala [2] thoroughly examine spatial and transform domain approaches in image steganography, analyzing their benefits, drawbacks, and relative performance.

D. Bhattacharyya et al.'s "A Review on Image Steganography Techniques" (2017) [3] presents an in-depth investigation of image steganography methods, focusing on various strategies and comparing them. The paper covers both traditional approaches like LSB substitution and advanced technologies like wavelet- and neural network-based steganography.

P. Gupta and A. Singh's article "Image Steganography: A Survey of Techniques and Evaluation of Practicality" (2017) [4] offers an overview of image steganography techniques, emphasizing their practicality in real-world applications. It discusses both spatial and transforms domain approaches, their usage, and applications.

M. N. P. Anju and A. S. Karun's "A Comparative Study of Image Steganography Techniques" (2018) [5] compares LSB replacement, pixel value differencing, and transform domain techniques with other image steganography methods, evaluating them based on embedding capability, imperceptibility, and robustness against attacks.

V. Asnani et al.'s "A Review on Image Steganography Methods and Performance Metrics" (2016) [6] presents an overview of image steganography techniques, discussing their classification and performance evaluation metrics.

In their paper "Image Steganography: A Review" (2016), [7] A. Kaur and R. K. Rani review various steganography techniques, including spatial and transform domain methods, as well as the challenges and future directions in the field.

R. Kumar and N. Kumar's "A Survey on Image Steganography and Its Techniques" (2017) [8] provides a comprehensive survey of image steganography techniques, covering traditional methods and modern approaches like transform domain and artificial intelligence-based techniques.

R. Singh and P. Kaur's article "A Comprehensive Review on Image Steganography Techniques" (2019) [9] explores different image steganography techniques, their characteristics, advantages, and limitations, focusing on spatial domain and transform domain methods.

A. Sinha et al.'s "A Comprehensive Survey on Image Steganography" (2020) [10] presents a detailed survey of image steganography techniques, including spatial, frequency, and transform domain methods, along with their advantages, limitations, and applications.

In the paper titled "A Review on Image Steganography Techniques and Comparison" (2020) [11], V. Kumar and A. Kaur review different image steganography methods, comparing their features, advantages, and limitations.

S. Pandey and S. Upadhyay's "A Survey on Image Steganography Techniques and Its Applications" (2021) [12] provide an extensive survey of image steganography techniques, their applications, and challenges, along with a discussion on the future scope of the field.

G. R. Aishwarya and K. R. Aishwarya's "A Study on Image Steganography Techniques" (2021) [13] explore various image steganography techniques, including LSB substitution, transform domain techniques, and their applications in different domains.

S. V. Patil and A. R. Raut's article "Review on Image Steganography Techniques and Challenges" (2021) [14] presents an overview of image steganography techniques, challenges, and advancements in the field, with a focus on both spatial and transform domain methods.

R. Yadav et al.'s "Image Steganography: A Review on Techniques, Challenges, and Applications" (2021) [15] discusses different image steganography techniques, challenges, and emerging applications, highlighting the advancements and potential areas of future research.

## Methodology –

Figure 1 demonstrates the architectural workflow of this work.

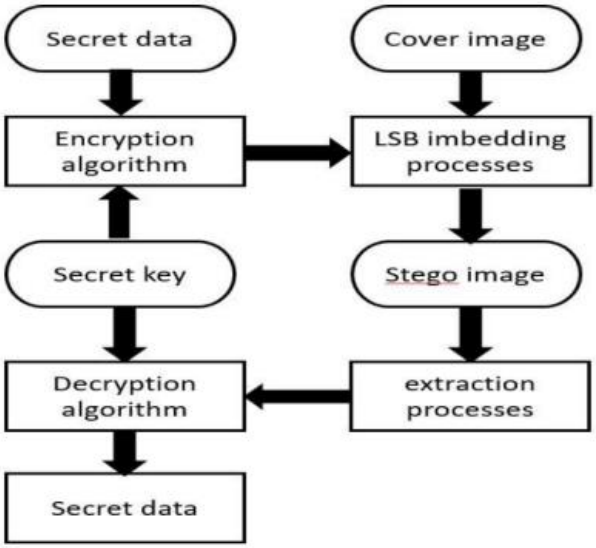


Figure 1:- Architectural Flow

The 2 realms of workflow are mainly GUI method and CUI method.

The utilization of a graphical user interface (GUI) has the potential to simplify and enhance the accessibility of image steganography. This entails the development of a GUI-based technique that facilitates the process of concealing information within an image. The following steps outline an overview of the procedures involved in creating such a technique:

1. Design the GUI layout: Carefully select and design the layout of the graphical user interface, considering elements such as buttons, text boxes, image display spaces, and other components. The aim is to create a user-friendly interface that enables seamless interaction.

2. Image Selection: Incorporate a button or option that allows users to choose a cover image from their local storage. Implement the necessary functionality to load and display the selected image within the GUI.

3. Hidden message input: Create a designated input field where users can enter the text or information they wish to conceal within the image. This can be in the form of a text box or the ability to upload a file containing the concealed message.

4. Encryption Options: Provide users with the option to select an encryption algorithm, if desired, and prompt them to enter the necessary password or keys for encrypting the secret message. This ensures the security of the hidden data during the embedding process.

5. Embedding process: Implement a steganography technique, such as LSB replacement or other suitable methods, to embed the concealed message into the selected cover image. If encryption was applied, incorporate it before embedding the hidden message.

6. Display and decryption: After retrieving the hidden message from the image, display it within the GUI for the user to view. If encryption was used, allow users to input the password or decryption keys to unlock and access the extracted message.

7. Error handling and validation: Implement robust error handling and validation procedures to address potential issues such as erroneous inputs, mistyped decryption keys, or unsupported image formats. This ensures the smooth functioning of the GUI-based technique.

8. Enhancements and features: Consider incorporating additional features and enhancements for advanced users. This could include image preview capabilities, image alteration options, image quality evaluation tools, or even steganalysis capabilities for detecting hidden information.

9. Instructions and user guidance: To assist users throughout the image selection, message input, embedding, extraction, and other necessary steps, provide clear instructions or tooltips within the GUI. This helps users navigate the steganography process effectively.

By developing a GUI-based technique for image steganography, individuals with varying levels of technical expertise can intuitively use the application, easily configure settings, and visualize the steganography process with ease.

The CUI (Command-Line User Interface) method of image steganography utilizes openCV, a popular open-source library for image processing and computer vision applications. It enables the concealment of data within images through a text-based interface. Users provide the concealed message, cover image, and optional encryption parameters as input. The program saves the stego image, employs techniques like LSB substitution to embed the concealed message, and can encrypt it if specified by the user. To decode and reveal the hidden message, users must supply the stego image as input to the program. The CUI approach supports command-line arguments and incorporates error handling and validation mechanisms to ensure proper execution and data integrity. Users can refer to the accompanying documentation to gain a better understanding of the available commands and functionalities. OpenCV plays a crucial role in this approach, providing a comprehensive set of functions and algorithms for image manipulation, analysis, and processing. Its capabilities include accessing and modifying pixel values, image transformation, applying filters, and performing various image processing tasks.

These features are particularly relevant in the context of image steganography, where OpenCV enables the alteration of the least significant portions of the cover image to embed the concealed data, resulting in the creation of a stego image that can be securely saved. The CUI method, facilitated by OpenCV, offers an efficient and effective means of concealing and retrieving data within images.

## Results and Discussions –

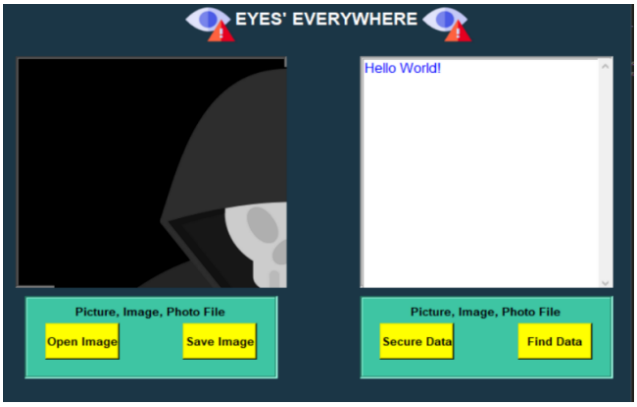


Figure 2- GUI Method

Figure 3 – Image before data hiding for GUI method

Figure 4 – Image after data hiding for GUI method

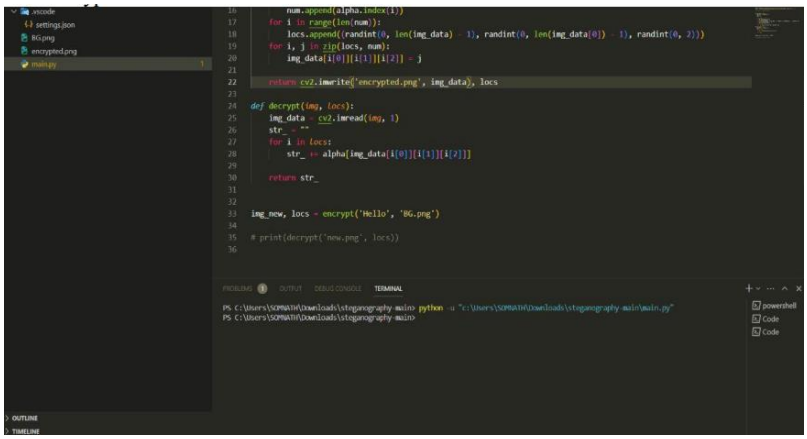


Figure 5 – CUI Method of Data Encryption


Figure 6 – Image before hiding in CUI Method of Data Encryption


Figure 7 – Image after hiding in CUI Method of Data Encryption

The GUI method for image steganography encountered an issue with the image input frame, leading to the adoption of the CUI (Command-Line User Interface) method. However, apart from the framing aspect, all other functionalities in the GUI method functioned properly. In the CUI method, OpenCV is utilized to decrypt the encrypted data directly in the terminal, making the process of data encryption and decryption more straightforward compared to the GUI method. Image steganography serves as a reliable means of securely concealing data within digital photographs, enabling covert communication and private data transmission. It operates by embedding the data into the frequency components or pixel values of the image. While image steganography offers several advantages, such as data protection and covert communication, it is crucial to acknowledge the potential challenges associated with detection and security vulnerabilities that need to be carefully addressed.

## Conclusion –

In conclusion, image steganography serves as a powerful tool for concealing data within photographs, ensuring the preservation of their visual appeal. Through techniques such as LSB substitution and advanced encryption, data can be hidden in the least significant bits of pixel values, safeguarding it during transmission and storage. This technique finds applications in various domains, including data protection, covert communication, and digital watermarking, offering a range of possibilities for secure information exchange. However, it is crucial to consider the limitations and potential vulnerabilities associated with steganography methods, as they may be susceptible to detection or unintended alterations. By understanding the intricacies of image steganography and addressing its challenges, we can harness its potential for discreet data concealment while upholding the integrity and confidentiality of the image content. The continuous advancement and exploration of steganography techniques will contribute to the evolution of secure communication and data privacy in an increasingly digital world.

**References –**

1. S. Nagaraj and K. K. Gowda. "A Survey on Image Steganography and Steganalysis Techniques" (2015).

2. S. S. Manjunath and N. Chandrakala. "Steganography Techniques: A Review Paper" (2016).

3. D. Bhattacharyya et al. "A Review on Image Steganography Techniques" (2017).

4. P. Gupta and A. Singh. "Image Steganography: A Survey of Techniques and Evaluation of Practicality" (2017).

5. M. N. P. Anju and A. S. Karun. "A Comparative Study of Image Steganography Techniques" (2018).

6. V. Asnani et al. "A Review on Image Steganography Methods and Performance Metrics" (2016).

7. A. Kaur and R. K. Rani. "Image Steganography: A Review" (2016).

8. R. Kumar and N. Kumar. "A Survey on Image Steganography and Its Techniques" (2017).

9. R. Singh and P. Kaur. "A Comprehensive Review on Image Steganography Techniques" (2019).

10. A. Sinha et al. "A Comprehensive Survey on Image Steganography" (2020).

11. V. Kumar and A. Kaur. "A Review on Image Steganography Techniques and Comparison" (2020).

12. S. Pandey and S. Upadhyay. "A Survey on Image Steganography Techniques and Its Applications" (2021).

13. G. R. Aishwarya and K. R. Aishwarya. "A Study on Image Steganography Techniques" (2021).

14. S. V. Patil and A. R. Raut. "Review on Image Steganography Techniques and Challenges" (2021).

15. R. Yadav et al. "Image Steganography: A Review on Techniques, Challenges, and Applications" (2021).