# Hidden in Plain Sight: The Science of Image Steganography”

Prof. Rupali Bathe

(Research scholar and Assistant Professor Savitribai Phule Pune University's SKNCOE Department of Computer Engineering, Pune.)

Manthan Yelpale, Rohan Ingawale, Shubham Rodge, Tanish Raut

(Department of Computer Engineering, SKNCOE Savitribai Phule Pune University, Pune)

*Abstract*— The project is set in the context of data security and privacy, where increasing concerns about the safety of information transmitted over digital channels have become a pressing issue. In this environment, ensuring confidential communication has become a significant challenge. The primary problem addressed by this project is the risk of unauthorized access to sensitive data during transmission, especially with modern cyber-attacks on the rise. Traditional encryption methods, while useful, are often easily detectable, making the data a target for attacks. The project proposes a solution based on image steganography, a technique that conceals data within digital images in such a way that it remains imperceptible to the human eye and undetectable by common methods of digital analysis. The steganography method used in this project embeds data in the least significant bits (LSB) of pixel values, ensuring the quality of the image is preserved while securely hiding the information. By integrating advanced algorithms for data embedding and retrieval, this technique provides an additional layer of security. Image steganography is an effective tool for secure communication, offering the advantage of hidden data transmission with minimal distortion to the carrier image. This project demonstrates that steganography can complement encryption techniques to enhance security, making it a promising approach for safeguarding sensitive information in the digital age.

***Keywords— digital image steganography; spatial domain embedding; transform domain embedding; cover-image; stego-image; wavelet***

***transform; Steganalysis***

##  **I. INTRODUCTION**

Steganography, derived from the Greek words Steganos (covered) and Graptos (writing), has been practiced for centuries. Historical examples include the use of tattoos and invisible ink. One notable instance from the 5th century BC involved a Roman general who tattooed a message on a slave's scalp, concealing it as the hair regrew.

In the digital era, steganography is the practice of embedding secret data within multimedia carriers (such as images, audio, or video) to create a "stegofile," rendering the hidden information undetectable. This approach aims to evade detection by both the human visual system (HVS) and steganalysis techniques.

Modern steganography often involves shared secret keys between the sender and receiver to enhance security. While cryptography protects data by scrambling it into unreadable forms, steganography conceals the very existence of the data. Combining these techniques can further enhance security, ensuring that even if the steganography is detected, the

uncovered message remains encrypted and unreadable without a decryption key.

This paper critically analyzes recent advancements in digital image steganography, focusing on methods to improve security and embedding efficiency. By exploring contemporary research, we aim to identify areas for innovation and enhancement.

##  **II. IMAGE STEGANOGRAPHY**

The advancement of imaging technologies and the widespread use of high-resolution images have created opportunities to securely transmit information. Digital image steganography leverages the inherent redundancy in images to embed secret data.

Key Factors in Image Steganography:

Capacity: Refers to the amount of data that can be hidden in the cover image, often termed payload.

Robustness: The ability of the stego image to withstand image processing and compression.

Imperceptibility: Ensuring that the embedded data remains undetectable by minimizing alterations to the cover image.

Embedding Process Overview: In an image steganography system, the secret message is embedded into the cover image using an encoding algorithm and a shared key to produce a stego image. The receiver uses the decoding algorithm and the shared key to extract the message.



Fig. 1. Overview of Steganographic system.

## **III. IMAGE STEGANOGRAPHY DOMAINS**

Image steganography techniques provide innovative ways to embed secret information into digital images, categorized into spatial domain, transform domain, and hybrid approaches. Each category offers distinct methodologies, advantages, and trade-offs, enabling diverse applications such as secure communication, watermarking, and data hiding.

### A. Spatial Domain Embedding

Spatial domain techniques are among the simplest and most commonly used methods for embedding data. These methods work by directly altering the pixel values of an image, making them computationally efficient and capable of embedding large amounts of data. The most widely recognized approach in this domain is the Least Significant Bit (LSB) Replacement, where the LSB of a pixel is substituted with bits of the secret data. This method is easy to implement and maintains minimal distortion in the image, making the changes imperceptible to the human eye. However, because of its straightforward nature, LSB replacement is highly susceptible to attacks such as compression, noise addition, or format conversion, which can disrupt or destroy the hidden information.

To address these vulnerabilities, more advanced techniques like Edge-Based Methods have been developed. These methods embed data in edge regions of an image, as these regions can accommodate modifications more effectively without compromising visual quality. Edges are inherently less uniform and, thus, better at concealing alterations. Another refinement of the basic LSB method is LSB Matching (LSBM), which avoids directly replacing the LSB of a pixel. Instead, it adjusts the pixel values by either incrementing or decrementing them. This subtle modification reduces the statistical detectability of the hidden data and makes it harder for attackers to identify its presence.

Adaptive LSB Methods go a step further by tailoring the embedding process based on the content of the image. These methods analyze the properties of different regions, such as smooth areas, textures, or edges, and strategically embed data where it would cause the least distortion. For example, edge and textured areas are more likely to conceal changes effectively, making adaptive methods ideal for improving both security and imperceptibility.

### B. Transform Domain Embedding

Transform domain techniques operate in the frequency domain of an image rather than directly modifying pixel values. These methods are preferred when robustness against attacks like compression, filtering, or noise is critical. Transform domain techniques embed data into the transformed coefficients of the image, which are less affected by such operations.

One of the most popular transform domain methods is the Discrete Cosine Transform (DCT). DCT is widely used in image compression formats like JPEG, making it an ideal choice for embedding data. By modifying the frequency coefficients rather than the pixel values, DCT ensures that changes are less visible and more resistant to compression-related data loss. For example, secret data can be embedded in the mid-frequency coefficients, striking a balance between imperceptibility and robustness.

Another significant method in this domain is the Discrete Wavelet Transform (DWT), which decomposes an image into different frequency bands, such as low and high frequencies. Data can be embedded in high-frequency bands to preserve the overall structure of the image while maintaining robustness against attacks. A related approach, the Integer Wavelet Transform (IWT), is particularly effective because it maps both the cover image and the secret data into integer coefficients, minimizing rounding errors and improving imperceptibility. IWT methods often exhibit superior performance in terms of robustness and visual quality, making them suitable for high-security applications.

### C. Hybrid Approaches

Hybrid techniques combine the strengths of spatial and transform domain methods to achieve better trade-offs between embedding capacity, security, imperceptibility, and robustness. These methods often involve multi-level embedding strategies or incorporate optimization algorithms to enhance the overall performance of the steganography process.

A common hybrid approach involves combining LSB Replacement with DWT. In this technique, the spatial domain’s high embedding capacity is complemented by the robustness of the transform domain. For instance, the secret data can be pre-processed and embedded into the wavelet coefficients using DWT, while additional data is stored in the spatial domain using LSB. This dual-domain embedding ensures that the hidden information remains secure even if one domain is compromised.

Moreover, hybrid techniques frequently incorporate optimization algorithms like genetic algorithms (GA), particle swarm optimization (PSO), or ant colony optimization (ACO) to refine the embedding process. These algorithms help balance the trade-offs between conflicting goals such as maximizing payload capacity while minimizing perceptual distortions and enhancing robustness. For example, PSO can optimize the selection of embedding regions to ensure that the secret data is distributed in a way that maximizes imperceptibility and minimizes the risk of detection.

Additionally, hybrid approaches sometimes use cryptographic techniques to further secure the embedded data. By encrypting the secret information before embedding it, these methods add an additional layer of protection, ensuring that even if the steganographic method is detected, the actual content remains inaccessible without the decryption key.

|  |  |  |  |
| --- | --- | --- | --- |
| **Technique** | **Capacity** | **Imperceptibilty** | **Robustness** |
| Spatial Domain | High | Moderate | Low |
| Transform Domain | Moderate | High | High |
| Hybrid Approaches | High | High | High |

## **IV. PERFORMANCE SPECIFICATION OF IMAGE**

### **STEGANOGRAPHY FACTORS**

The The effectiveness of image steganography techniques is assessed using three primary metrics: robustness, imperceptibility, and capacity. Achieving a balance among these factors is essential, as they often exhibit trade-offs. The relationship between these metrics is frequently visualized using the steganography triangle, which highlights the inherent compromises in designing steganographic methods.

Fig. 3, represents a balance triangle each of its ribs specifies a factor associated with a steganographic method. So that for instance in order to improve capacity, you sacrifice security. It makes scenes that the more embedding in an image the more probability that an observer will notice the degradation and suspect something is out of place. It is obvious that improving one factor will affect the other factors so that any steganography method must take care of the three factors at all times trying to keep the triangle as balanced as possible you have to change the other two elements.

Robustness refers to the ability of a technique to resist attacks, distortions, and image manipulations such as compression, filtering, noise addition, or resizing. Robust methods ensure that the embedded data remains intact and retrievable even after such operations. Techniques in the transform domain, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), are particularly effective in enhancing robustness. However, the added complexity of these methods may reduce the embedding capacity or increase computational requirements.

Imperceptibility measures how well the modifications introduced by embedding data remain invisible to the human eye. This ensures that the stego-image appears indistinguishable from the original cover image. Methods such as adaptive Least Significant Bit (LSB) and edge-based techniques enhance imperceptibility by embedding data in regions of the image where visual changes are less noticeable. However, achieving high imperceptibility often requires limiting the payload capacity to avoid perceptible distortions.

Capacity refers to the amount of data that can be embedded within a cover image without degrading its quality. Spatial domain methods, particularly LSB replacement, are known for their high embedding capacity, making them suitable for transmitting large payloads. However, increasing capacity often compromises imperceptibility, as embedding larger amounts of data raises the risk of detectable visual artifacts. Additionally, higher capacity can reduce robustness, making the embedded data more susceptible to attacks.



Fig. 3. The Steganography Triangle.

**V. RELATED WORK**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Author** | **Year** | **Description** |
| Systematic literature review and analysis for Arabic text steganography method practical | Nuur Alifah Roslana, Nur Izura Udzirb, Ramlan Mahmodc, Adnan Gutub | 2022 | The paper explores the potential of Arabic Text Steganography (ATS) by identifying four key characteristics of Arabic script: diacritics, Kashida, dots, and letter shapes, which offer new methods for hiding data. Kashida and Unicode techniques emerged as the most effective due to their high-level invisibility, while diacritics are less commonly used outside religious texts.  |
| Image Steganography: A Review of the Recent Advances | Nandhini Subramanian,Omar Elharrouss, Somayaal-maadeed, Andahmed Bouridane | 2016 | The paper reviews advancements in image steganography, highlighting a shift from traditional methods like LSB substitution, PVD, and DCT, which are limited in capacity and security, to deep learning approaches using CNNs and GANs. GAN-based methods, in particular, show superior performance in hiding capacity and security, with high PSNR values indicating minimal image distortion. |
| Video Steganography: Secure Data Hiding Technique | Gat Pooja Rajkumar, Dr V. S. Malemath | 2017 | The paper presents a dual-level security method using video steganography to securely transmit sensitive information. It employs two main techniques: encryption using the DES algorithm and data hiding via the Least Significant Bit (LSB) technique. DES encryption is chosen for its simplicity and speed, involving 16 rounds of encryption with subkey substitutions for enhanced security. |
| Information Hiding in Images Using Steganography Techniques | Anoop Kumar | 2020 | Image Steganography is a technique used to securely hide information within an image, making the communication appear ordinary and preventing unauthorized access. It differs from traditional encryption methods by focusing not just on securing data, but on concealing the fact that communication is taking place.  |
| Hide and Seek: An Introduction to Steganography | Niels Provos and Peter Honeyman | 2003 | This Paper discusses the detection of hidden messages within digital images using steganographic techniques. It explains that some methods, like JSteg, which sequentially modify the least-significant bits of Discrete Cosine Transform (DCT) coefficients. |

**VI. CRITICAL ANALYSIS**

A comparative analysis of the main techniques reveals the strengths and limitations of spatial, transform, and hybrid domains. Spatial methods excel in capacity and simplicity but are vulnerable to attacks. Transform domain techniques offer robustness but with limited payloads. Hybrid approaches show promise but require further research to achieve optimal results.

## **VII. CONCLUSION**

Image steganography plays a crucial role in data security, enabling sensitive information to be transmitted covertly while reducing the likelihood of detection. Its key strengths, including invisibility, adaptability, and user-friendliness, make it an attractive solution for various purposes such as secure communication and digital watermarking. However, the field faces challenges like limitations in embedding capacity, potential degradation of image quality, and vulnerability to detection. These challenges highlight the importance of ongoing research and innovation.

As technology progresses, both the techniques for embedding data and the methods for detecting hidden information are becoming more sophisticated. Future advancements in image steganography should focus on developing algorithms that enhance data capacity while maintaining high image quality. The integration of machine learning approaches can enable the creation of adaptive and robust techniques capable of resisting detection. Moreover, exploring multi-carrier steganography could introduce novel ways to distribute hidden data across different media formats, thereby improving security. Ensuring resilience against common image processing operations, such as compression and resizing, remains a critical goal for preserving the integrity of embedded data.

Additionally, the development of intuitive and accessible tools can expand the use of steganography to non-expert users. Establishing well-defined legal and ethical guidelines will also help address concerns around potential misuse. By addressing these areas, the field of image steganography can continue to advance, providing innovative solutions for secure and reliable communication in an increasingly digital world.

**REFERENCES**  [1]. Information Hiding in Images Using Steganography Techniques-Anoop-Kumar. [2]Johnson,-Neil-F."Steganography."Nov.1995.Web [3] Niels Provos, and Peter Honeyman. “Hide and Seek: An Introduction-to-Steganography.” [4] IEEE Security & Privacy Magazine, May-June 2013. Web. [5] Shikha, and Vidhu Kiran Dutt. "International Journal of Advanced Research in Computer Science and Software Engineering." [6] Nick Nabavian. “Image steganography” Nov. 28, 2007. [7] "Systematic literature review and analysis for Arabic text steganography method practical".Nuur-Alifah-Roslana,Nur Izura-Udzirb,Ramlan-Mahmodc,Adnan-Gutub.2022 [8]"Image-Steganography:A-Review-of-the-Recent Advances".Nandhini-Subramanian,Omar-Elharrouss,Somaya almaadeed,Andahmed-Bouridane.2016 [9] "Video Steganography: Secure Data Hiding Technique".Gat Pooja-Rajkumar,Dr.V.S.Malemath.2017 [10] Nur Farhana Hordri, Siti Sophiayati Yuhaniz, and Siti Mariyam Shamsuddin. Deep learning and its applications: a review. In Conference on Postgraduate Annual Research on Informatics-Seminar,2016. [11] Amritpal Singh and Harpal Singh. An improved lsb based image steganography technique for rgb images. In 2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT), pages 1–4. IEEE, 2015. [12] Munthir Bahir Tuieb, Mahmood Zaki Abdullah, and Nazhat Saeed AbdulRazaq. An efficiency, secured and reversible video steganography approach based on least significant bit [13]Vojtech Holub and Jessica Fridrich. Designing steganographic distortion using directional filters. 12 2012. [14] Ming-ming Liu, Coverless information hiding based on generative adversarial networks.