International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

A Comprehensive Study of Digital Image Steganography: Techniques, Applications and Security Challenges in Covert Communication

Vinay siwach
M.tech 4th semester, Computer Science & Engineering, BITS Bhiwani
Rahul Kaushik
Assistant professor, Computer Science & Engineering, BITS Bhiwani

Abstract
Digital image steganography has emerged as a crucial technique in the field of secure communication, enabling the concealment of sensitive information within digital images in a manner that is imperceptible to human vision. Unlike cryptography, which focuses on encrypting the content of a message, steganography emphasizes hiding the very existence of the message, thereby providing an additional layer of security. With the rapid growth of digital communication and the widespread use of multimedia content, the demand for covert communication methods has increased significantly. This study presents a comprehensive analysis of digital image steganography, focusing on its core concepts, various embedding techniques, practical applications and associated security challenges. It examines traditional methods such as Least Significant Bit (LSB) substitution, transform domain techniques including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), as well as modern approaches that integrate machine learning and deep learning for improved performance. The study also explores evaluation parameters such as payload capacity, imperceptibility and robustness, which are critical in determining the effectiveness of steganographic systems. Furthermore, it highlights potential threats such as steganalysis, data distortion and attacks that aim to detect or disrupt hidden communication. The findings indicate that while digital image steganography offers a powerful means of secure and covert communication, it also faces significant challenges in maintaining a balance between data hiding capacity, security and resistance to detection. The paper concludes by emphasizing the need for more advanced, adaptive and robust steganographic techniques to address emerging security concerns in the evolving digital landscape.

Keywords
Digital Image Steganography, Covert Communication, Data Hiding, Information Security, LSB Technique, DCT, DWT, Steganalysis, Image Processing, Cybersecurity

Introduction

In the modern era of digital communication, the protection of sensitive information has become a major concern due to the increasing reliance on internet-based platforms for data exchange. As communication technologies continue to evolve, so do the methods used by malicious actors to intercept, manipulate, or misuse information. This has led to the development of various techniques aimed at securing data during transmission. Among these, digital image steganography has gained significant attention as an effective method for covert communication. Steganography, derived from the Greek words meaning “covered writing,”

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

refers to the practice of hiding secret information within a non-secret medium in such a way that the existence of the hidden data remains undetectable.

Unlike traditional cryptographic techniques, which transform readable data into an unreadable format to protect its content, steganography focuses on concealing the presence of the message itself. This makes it particularly useful in scenarios where the detection of communication could raise suspicion or lead to security risks. Digital images serve as an ideal medium for steganography due to their widespread use, large data capacity and the presence of redundant or less perceptible information that can be manipulated without significantly affecting visual quality. As a result, digital image steganography has become an important tool in areas such as military communication, confidential data transmission, copyright protection and secure information exchange. The fundamental principle of digital image steganography involves embedding secret data into an image, known as the cover image, to produce a modified image called the stego image. The goal is to ensure that the stego image appears visually identical to the original image while securely carrying hidden information. Various techniques have been developed to achieve this objective, each with its own advantages and limitations. One of the most commonly used methods is the Least Significant Bit (LSB) technique, where the least important bits of pixel values are altered to store secret data. This method is simple and offers high data capacity, but it may be vulnerable to detection and attacks.

In addition to spatial domain techniques like LSB, transform domain methods have been introduced to enhance robustness and security. Techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) embed data in the frequency components of the image rather than directly modifying pixel values. These approaches provide better resistance against common image processing operations such as compression, filtering and noise addition. More recently, advancements in artificial intelligence and deep learning have led to the development of intelligent steganographic systems that can automatically optimize data embedding while maintaining high levels of imperceptibility and security. Despite its advantages, digital image steganography faces several challenges that limit its effectiveness. One of the primary concerns is the trade-off between payload capacity and image quality. Increasing the amount of hidden data can lead to noticeable distortions in the image, making the steganographic process detectable. Another challenge is robustness, as the hidden information may be lost or corrupted during image processing operations such as resizing, compression, or format conversion. Furthermore, steganalysis techniques, which are designed to detect hidden information, pose a significant threat to steganographic systems by analyzing statistical anomalies and patterns within images. Security is another critical aspect of steganography, as the hidden data must remain protected from unauthorized access. This has led to the integration of cryptographic techniques with steganography to enhance overall security. Additionally, ethical and legal considerations must be taken into account, as steganography can be used for both legitimate and malicious purposes, including illegal communication and data exfiltration. This study aims to provide a comprehensive overview of digital image steganography by examining its concepts, techniques, applications and security challenges. By analyzing existing methods and identifying their strengths and limitations, the

paper seeks to contribute to the development of more secure and efficient steganographic systems. As digital communication continues to expand, the importance of covert communication techniques like steganography will only increase, making it essential to address the challenges and explore innovative solutions in this field.

Fundamentals of Digital Image Steganography

Digital image steganography is a technique of information hiding in which secret data is embedded within a digital image in such a way that its presence remains invisible to human perception. The fundamental concept of steganography is not just to protect the content of the message, but to conceal the very existence of communication, making it different from cryptography. In this process, three main components are involved: the cover image, which is the original image used to hide data, the secret message, which is the information to be concealed and the stego image, which is the final output after embedding the secret data into the cover image. The embedding process modifies certain parts of the image in a controlled manner so that changes are imperceptible, while the extraction process retrieves the hidden data using specific algorithms or keys. At its core, digital image steganography relies on the properties of digital images, particularly the redundancy and sensitivity of pixel values. A digital image is composed of pixels and each pixel contains intensity or color information represented in binary form. Since slight changes in the least significant bits of pixel values do not noticeably affect image quality, these bits are often used to embed secret data. This principle forms the basis of many steganographic techniques. The effectiveness of steganography depends on achieving a balance among three key factors: imperceptibility, which ensures that the stego image looks visually identical to the original; payload capacity, which determines how much data can be hidden; and robustness, which reflects the ability of hidden data to resist image processing operations such as compression, resizing, or noise addition. Furthermore, digital image steganography can be implemented in different domains, primarily the spatial domain and the transform domain. In spatial domain techniques, data is directly embedded into pixel values, making them simple and efficient but sometimes less secure. In contrast, transform domain techniques embed data in the frequency components of the image, offering greater resistance to attacks and image manipulations. The security of steganographic systems can also be enhanced by using encryption keys or combining steganography with cryptographic methods. Overall, the fundamentals of digital image steganography revolve around the careful manipulation of image data to securely and covertly transmit information, ensuring that communication remains hidden and protected in a digital environment.

Definition and Working Principle

Digital image steganography is defined as the technique of concealing secret information within a digital image in such a way that the existence of the hidden data remains undetectable to human observers and difficult to identify through standard analysis. Unlike encryption, which scrambles the content of a message to make it unreadable, steganography embeds the message inside another medium, ensuring that the communication appears completely normal and does not raise suspicion. In this process, a digital image acts as a carrier or cover medium

because of its large data capacity and inherent redundancy, which allows small modifications to be made without noticeably affecting visual quality. The result of this embedding process is known as a stego image, which looks almost identical to the original image but contains hidden information. The working principle of digital image steganography involves two main stages: embedding and extraction. During the embedding phase, the secret message is first prepared and in many cases, it may also be encrypted to add an additional layer of security. This message is then inserted into the cover image using specific algorithms that modify certain components of the image data, such as pixel values or frequency coefficients. The most common approach is to alter the least significant bits of pixel values, as these changes are not easily detectable by the human eye. In more advanced methods, data is embedded in the transform domain, where image information is represented in terms of frequency components, providing better resistance to compression and image processing operations. In the extraction phase, the hidden data is retrieved from the stego image using a corresponding extraction algorithm, often requiring a secret key or knowledge of the embedding method. This ensures that only authorized users can access the concealed information. The overall effectiveness of the working principle depends on maintaining a balance between invisibility, data capacity and resistance to detection or distortion. By carefully manipulating image properties, digital image steganography enables secure and covert communication, making it a valuable tool in various fields such as data security, military communication and digital rights protection.

Types of Steganography

Steganography can be classified into different types based on the medium used to hide the secret information. Each type utilizes the characteristics of a specific digital medium to embed data in a covert manner while maintaining normal appearance or functionality. The main types of steganography include image, audio, video and text steganography, each offering unique advantages and facing specific challenges in terms of capacity, robustness and security.

- **Image Steganography** is the most widely used form of steganography due to the large amount of redundant data present in digital images. In this method, secret information is embedded within the pixels of an image by modifying their values in a way that does not significantly alter visual quality. Techniques such as Least Significant Bit (LSB), pixel value differencing and transform domain methods are commonly used. The high data capacity and widespread use of images on digital platforms make this approach highly effective for covert communication. However, it may be vulnerable to detection through statistical analysis or image processing operations if not properly implemented.
- **Audio Steganography** involves hiding information within audio signals such as music or speech files. This technique exploits the limitations of the human auditory system, which cannot detect slight variations in sound. Data can be embedded by modifying audio samples, frequencies, or phases without affecting sound quality. Methods like LSB substitution, echo hiding and phase coding are commonly used. Audio steganography offers good robustness against certain types of attacks, but it can be sensitive to compression and noise, which may distort or destroy the hidden information.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

- **Video Steganography** combines both image and audio steganography by embedding data within video files, which consist of sequences of images (frames) along with audio tracks. This method provides a very high payload capacity because of the large size of video data. Secret information can be hidden in individual frames, motion vectors, or audio components of the video. Due to the complexity and size of video files, detection becomes more difficult, making it a powerful technique for secure communication. However, it also requires significant computational resources and may be affected by video compression and editing processes.
- **Text Steganography** is one of the simplest yet most challenging forms of steganography, as text files have very limited redundancy compared to images or audio. In this method, information is hidden within textual content by manipulating characters, formatting, spacing, or linguistic structures. Techniques include using invisible characters, altering word spacing, employing synonyms, or using specific patterns in text arrangement. Although text steganography offers low capacity, it can be highly secure if implemented carefully, as the changes are often subtle and difficult to detect. However, it is more susceptible to data loss during formatting changes or retyping. Overall, each type of steganography utilizes the unique properties of its respective medium to achieve covert communication. The choice of technique depends on factors such as data capacity, level of security required, robustness against attacks and the nature of the communication channel.

Characteristics of Effective Steganography

Effective steganography is defined by a set of essential characteristics that determine how securely and efficiently secret information can be hidden within a digital medium without being detected or corrupted. The most important characteristic is **imperceptibility**, which ensures that the stego object, such as an image, audio, or video file, appears visually or audibly identical to the original cover medium. This is crucial because any noticeable distortion can raise suspicion and compromise the covert nature of communication. Another key characteristic is **payload capacity**, which refers to the amount of secret data that can be embedded within the cover medium. A good steganographic system should be able to hide a reasonable amount of information without significantly affecting the quality of the carrier file. However, there is often a trade-off between payload capacity and imperceptibility, as increasing the amount of hidden data can lead to detectable changes. **Robustness** is another critical factor, which indicates the ability of the hidden data to remain intact even after the stego object undergoes common processing operations such as compression, resizing, filtering, or noise addition. A robust system ensures that the secret information can still be accurately extracted even if the file is modified during transmission or storage. Additionally, **security** plays a vital role in effective steganography. It ensures that unauthorized users cannot detect or extract the hidden information. This is often achieved by using secret keys, encryption techniques, or complex embedding algorithms. The system should be resistant to steganalysis, which involves detecting the presence of hidden data through statistical or computational methods. Another important characteristic is **undetectability**, which goes beyond imperceptibility by ensuring that even advanced analytical techniques cannot easily identify the presence of hidden

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

information. Furthermore, reliability and accuracy are essential to guarantee that the embedded data can be correctly extracted without loss or distortion. Lastly, **computational efficiency** is also considered important, as the embedding and extraction processes should not require excessive time or resources. Overall, effective steganography is achieved by balancing these characteristics, ensuring that the hidden communication remains secure, invisible and resilient in various real-world conditions.

Digital Image Representation

Digital image representation refers to the way images are stored, processed and interpreted in a computer system using numerical data. Every digital image is composed of a grid of tiny elements called pixels, where each pixel holds specific intensity or color information. The representation of these pixels determines how the image appears and how it can be manipulated for applications such as steganography. In digital image steganography, understanding image representation is essential because secret data is embedded by modifying pixel values or frequency components without noticeably affecting visual quality. The efficiency, security and robustness of steganographic techniques largely depend on the type of image format used, the structure of pixels and the method of image compression.

- **Image Formats (JPEG, PNG, BMP)**

Image formats define how image data is stored and encoded in digital form and they play a crucial role in steganography. Different formats have different characteristics in terms of compression, quality and data storage. JPEG is a widely used lossy compression format that reduces file size by discarding less important image information. It is suitable for storing photographs but can affect hidden data due to compression loss. PNG is a lossless compression format that preserves image quality and does not discard data, making it more reliable for steganographic purposes where data integrity is important. BMP is an uncompressed format that stores raw pixel data without any compression, resulting in large file sizes but providing maximum data capacity for embedding secret information. Each format offers different trade-offs between storage efficiency, image quality and robustness, which must be carefully considered when applying steganographic techniques.

- **Pixel Structure and Color Models (RGB, Grayscale)**

The pixel structure of a digital image refers to how individual pixels are organized and how their values represent color or intensity. In most digital images, pixels are arranged in a two-dimensional matrix and each pixel contains numerical values that define its appearance. The RGB color model is one of the most common representations, where each pixel is composed of three components: red, green and blue. Each of these components is typically represented by 8 bits, allowing a wide range of color combinations. This structure provides multiple channels where secret data can be embedded. On the other hand, grayscale images use a single intensity value per pixel, representing shades of gray from black to white. Although grayscale images have lower data capacity compared to RGB images, they can still be used for steganography with simpler implementation. Understanding pixel structure and color models is essential for selecting appropriate embedding techniques and ensuring that modifications remain imperceptible.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

- **Image Compression Techniques**

Image compression techniques are used to reduce the size of digital image files by eliminating redundant or less significant information, thereby improving storage efficiency and transmission speed. Compression can be broadly classified into lossy and lossless methods. Lossy compression, as used in JPEG format, removes some image details that are considered less important to human perception, which can significantly reduce file size but may also affect the integrity of hidden data. Lossless compression, as used in PNG format, preserves all original data, ensuring that no information is lost during compression. In the context of steganography, compression plays a critical role because it can either preserve or destroy the embedded secret data. Advanced steganographic techniques often embed data in frequency domains to improve resistance against compression. Therefore, understanding compression techniques is essential for designing robust steganographic systems that can withstand common image processing operations while maintaining both image quality and data security.

Steganographic Techniques

Steganographic techniques refer to the various methods and algorithms used to embed secret information within a digital medium, such as images, in a way that conceals the existence of the hidden data while maintaining the original appearance of the carrier file. These techniques are designed to achieve covert communication by modifying certain components of the cover medium in a controlled and imperceptible manner. In digital image steganography, the primary goal is to hide information within pixel values or image structures without causing noticeable distortion, ensuring that the stego image appears visually identical to the original image. The effectiveness of steganographic techniques depends on their ability to balance imperceptibility, payload capacity, robustness and security. Steganographic techniques are broadly categorized into two main domains: spatial domain and transform domain methods. In spatial domain techniques, secret data is directly embedded into the pixel values of the image. The most common example is the Least Significant Bit method, where the least important bits of pixel values are altered to store hidden information. These methods are simple, fast and offer high data capacity, but they are more vulnerable to detection and image processing operations. In contrast, transform domain techniques embed data in the frequency components of the image after applying mathematical transformations such as Discrete Cosine Transform or Discrete Wavelet Transform. Modern steganographic techniques also incorporate machine learning and deep learning to optimize embedding strategies and enhance resistance against steganalysis. These intelligent systems can adapt to different types of images and automatically determine the best locations for embedding data. Overall, steganographic techniques form the core of covert communication systems, enabling secure and hidden data transmission while continuously evolving to address emerging security challenges in the digital environment.

Embedding and Extraction Process

The embedding and extraction process is the core mechanism of digital image steganography, as it explains how secret information is hidden inside an image and later recovered by the intended receiver. In the embedding process, a normal digital image, called the cover image, is selected as the carrier medium for the secret message. The secret data may be plain text, an

image, a document, or any other confidential information. Before embedding, the secret message is often converted into binary form and may also be encrypted to provide an additional layer of protection. After this, a steganographic algorithm inserts the data into selected parts of the cover image, such as pixel values in spatial domain methods or frequency coefficients in transform domain methods. For example, in the Least Significant Bit technique, the least important bits of image pixels are modified because small changes in these bits usually do not create visible distortion. After successful embedding, the resulting image is known as the stego image, which appears almost identical to the original image but contains hidden information. The extraction process is the reverse operation, where the hidden message is retrieved from the stego image. The receiver uses a corresponding extraction algorithm and in many systems, a secret key is required to locate and recover the embedded data correctly. If the same embedding logic and key are not available, it becomes difficult for unauthorized users to extract the concealed information. The quality of this process depends on important factors such as imperceptibility, payload capacity, robustness and security. A good embedding process should hide maximum possible data without affecting image quality, while a reliable extraction process should recover the secret message accurately even after minor image processing operations. Therefore, embedding and extraction together determine the overall effectiveness of a steganographic system and play a vital role in secure covert communication.

Applications of Digital Image Steganography

Digital image steganography has a wide range of applications in modern information systems, primarily due to its ability to provide covert and secure communication by hiding sensitive data within digital images. One of its most significant applications is in military and defense communication, where confidential information must be transmitted securely without revealing the existence of the message. By embedding data within images, military agencies can exchange critical intelligence without attracting attention. Similarly, steganography is widely used in secure data transmission, especially in environments where privacy and confidentiality are essential, such as banking, corporate communication and government operations. It ensures that sensitive information remains hidden even if the transmission channel is compromised. Another important application is in copyright protection and digital watermarking, where ownership information is embedded into digital images to prevent unauthorized use and piracy. This helps content creators and organizations protect their intellectual property. In the field of medical data security, steganography is used to embed patient information within medical images such as X-rays and MRI scans, ensuring both data integrity and confidentiality during storage and transmission. Additionally, it is used in online communication security, where individuals can exchange private messages over public platforms without revealing their presence to third parties. Steganography also plays a role in cybersecurity and authentication systems, where hidden data can be used for identity verification or secure access control. However, while these applications demonstrate the positive use of steganography, it is important to note that the same technology can also be misused for illegal activities, such as covert communication by cybercriminals. Therefore, while digital image steganography

provides powerful advantages in secure communication, it must be used responsibly and in conjunction with proper legal and ethical guidelines.

Security Challenges in Steganography

Security challenges in steganography refer to the risks and limitations that affect the safety, reliability and secrecy of hidden communication. Although steganography is designed to conceal the existence of secret data, it is not completely free from threats. One of the major challenges is steganalysis, which is the process of detecting hidden information inside an image, audio, video, or text file. Advanced steganalysis tools can identify unusual statistical patterns, pixel changes, or frequency variations in a stego image and may reveal that secret data is present. Another important challenge is the trade-off between payload capacity, imperceptibility and robustness**.** If a large amount of data is hidden in an image, the visual quality may be affected, making the changes easier to detect. On the other hand, if the system focuses only on invisibility, the amount of data that can be embedded becomes limited. Another serious challenge is the vulnerability of hidden data to image processing operations such as compression, resizing, cropping, filtering, noise addition and format conversion. These operations may damage or completely destroy the embedded information, especially in simple spatial-domain methods like LSB. Security is also affected when the embedding algorithm is weak or predictable, because attackers may identify the hiding pattern and extract or alter the secret message. Therefore, the use of secret keys, encryption and adaptive embedding strategies becomes necessary to strengthen protection. In addition, ethical and legal concerns are also linked with steganography because the same technique used for privacy and secure communication can also be misused for criminal communication, data leakage, or hiding malicious content. Thus, the main security challenge in steganography is to design systems that are highly invisible, resistant to attacks, difficult to detect and safe for legitimate use in digital communication.

Conclusion

In conclusion, the study titled *"A Comprehensive Study of Digital Image Steganography: Techniques, Applications and Security Challenges in Covert Communication"* provides a detailed and systematic understanding of how steganography has become a vital tool in modern secure communication systems. With the rapid growth of digital communication and multimedia technologies, the need for protecting sensitive information has increased significantly. Unlike traditional cryptographic methods, steganography offers an additional layer of security by concealing the very existence of communication, making it highly effective for covert data transmission.

The study highlights that digital image steganography is particularly advantageous due to the large data capacity and widespread use of images in digital environments. Various techniques such as spatial domain methods like Least Significant Bit and transform domain approaches like Discrete Cosine Transform and Discrete Wavelet Transform have been analyzed in detail. Each technique offers unique benefits in terms of simplicity, robustness and security. The integration of machine learning and deep learning has further enhanced the capability of steganographic systems by improving data embedding strategies and resistance to detection.

Additionally, key processes such as embedding and extraction, along with supporting components like image representation, preprocessing and feature handling, play a crucial role in determining the overall effectiveness of steganographic systems. The study also emphasizes important evaluation parameters such as imperceptibility, payload capacity, robustness and security, which must be carefully balanced to achieve optimal performance. While steganography offers numerous applications in areas such as military communication, secure data transmission, copyright protection and medical data security, it also faces several significant challenges. Issues such as steganalysis attacks, vulnerability to image processing operations, trade-offs between capacity and quality and the risk of misuse present serious concerns. Furthermore, ethical and legal implications must be considered, as the same technology can be used for both legitimate and malicious purposes. Therefore, the study concludes that although digital image steganography is a powerful and promising technique for covert communication, continuous research and innovation are required to address its limitations. Future advancements should focus on developing more robust, adaptive and intelligent systems that can withstand evolving threats while maintaining high levels of security and imperceptibility. The integration of advanced technologies such as artificial intelligence, along with proper regulatory frameworks and ethical practices, will play a key role in ensuring the safe and effective use of steganography in the digital age.

References:

1. Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, 16(4), 474–481.
2. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3–4), 313–336.
3. Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography. *IEEE International Conference on Image Processing*, 1019–1022.
4. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). Digital image steganography: Survey and analysis. *Signal Processing*, 90(3), 727–752.
5. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). *Digital watermarking*. Morgan Kaufmann.
6. Fridrich, J. (2009). *Steganography in digital media*. Cambridge University Press.
7. Gutub, A., & Al-Ghamdi, M. (2014). Image based steganography techniques. *International Journal of Computer Applications*, 102(3), 12–18.
8. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography. *Computer*, 31(2), 26–34.
9. Katzenbeisser, S., & Petitcolas, F. (2000). *Information hiding techniques*. Artech House.
10. Ker, A. D. (2007). Steganalysis of LSB matching. *IEEE Transactions on Information Forensics*, 2(4), 441–452.
11. Kharrazi, M., Sencar, H. T., & Memon, N. (2004). Image steganography techniques. *IEEE Signal Processing Magazine*, 21(2), 48–60.

12. Lyu, S., & Farid, H. (2004). Steganalysis using higher-order statistics. *IEEE Transactions on Information Forensics*, 1(1), 111–119.
13. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). Overview of image steganography. *Information Hiding Workshop*, 1–11.
14. Petitcolas, F. A. (1999). Information hiding techniques. *Proceedings of the IEEE*, 87(7), 1062–1078.
15. Provos, N., & Honeyman, P. (2003). Detecting steganographic content. *IEEE Security & Privacy*, 1(3), 24–31.
16. Roy, S., & Changder, S. (2016). Evaluation of image steganography. *Multimedia Tools and Applications*, 75(12), 6993–7020.
17. Sharma, R., & Gupta, A. (2013). LSB based steganography techniques. *International Journal of Engineering Research*, 2(5), 1–6.
18. Singh, S., & Singh, R. (2015). A review of image steganography. *International Journal of Computer Science*, 12(2), 1–7.
19. Swain, G. (2018). Digital image steganography using LSB. *Procedia Computer Science*, 132, 178–185.
20. Wang, H., & Wang, S. (2004). Cyber warfare: Steganography vs steganalysis. *Communications of the ACM*, 47(10), 76–82.
21. Westfeld, A. (2001). F5 steganographic algorithm. *Information Hiding Workshop*, 289–302.
22. Wu, D., & Tsai, W. H. (2003). A steganographic method for images. *Pattern Recognition Letters*, 24(9–10), 1613–1626.
23. Xuan, G., Shi, Y. Q., & Ni, Z. (2002). Lossless data hiding. *IEEE Transactions on Circuits and Systems*, 49(6), 737–742.
24. Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding. *IEEE Transactions on Information Forensics*, 3(3), 384–395.
25. Zhang, X., & Wang, S. (2006). Efficient steganographic embedding. *IEEE Signal Processing Letters*, 13(5), 273–276.