GSJ: Volume 13, Issue 6, June 2025, Online: ISSN 2320-9186

www.globalscientificjournal.com

A Comprehensive Review of Image Steganography Techniques, Challenges, and Future Directions.

Oluwole Ayodeji Ayegbusi

Faculty of Computing

Department of Computer Science

Adekunle Ajasin University, Akungba-Akoko

Nigeria.

oluwole.ayegbusi@aaua.edu.ng

Abstract Image steganography has been widely considered as an important component in the field of information security, since it can effectively support hidden and secret communication by embedding sensitive data inside images. With the growing field of digital communication, the methods and technologies used for steganography are getting updated. In this paper, a comprehensive survey on 30 significant contributions in the field were presented, encompassing spatial and frequency domain algorithms, Machine learning and deep learning based solutions, steganalysis techniques, as well as applications. Current findings, technical challenges and future perspectives from the application of steganography in robust and secure communication were also discussed.

Keywords: data hiding, deep learning, frequency domain, image steganography, steganalysis, secure communication, spatial domain.

1. Introduction

Steganography has advanced significantly due to the growing need for secret and secure communication in a world that is becoming more interconnected. Unlike cryptography, which aims to encrypt and obscure a message's content to prevent unwanted access, steganography aims to conceal the message's existence (Kumar & kim, 2010), making it a vital tool in situations where discretion is crucial. of the different types of steganography, image steganography is one of the most popular methods. This popularity is mostly attributable to digital images' abundance, accessibility, and inherent redundancy, which present numerous opportunities for concealing information without raising red flags. Furthermore, the importance of image-based steganographic techniques has increased due to the quick development of multimedia technologies and the pervasiveness of digital imaging in daily life. In this work, a thorough and critical analysis of image steganography methods, charting their development and emphasizing current developments is presented. The analysis is based on a thorough review of 30 significant contributions that cover both traditional and innovative approaches in order to provide insightful information about the present and potential future paths of research in this ever-evolving field.

1.1 Some key Terminologies

Stego Image:This is the image containing the embedded data.

Steganalysis:This is the process of finding hidden information, or data, within a digital image or other media file,it is the opposite of steganography which aims to concel the message itself.

Digital communication: This encompasses any form of electronic exchange of information, data, or messages using digital technologies. This covers a broad range of techniques, including social media, video conferencing, instant messaging, and images, among many others.

2. Classical Steganography Techniques

2.1 Spatial Domain Techniques

Spatial domain steganography methods involve embedding confidential data directly into the cover image’s pixel values, without any prior transformation. This method is straightforward but can be more

prone to distortion in the stego image. Few example of spatial domain methods include LSB embedding technique, colour based steganography,mapping based method,pixel value differencing technique, collage method steganography,

Suresh and Kamalakannan in 2023 introduced a novel approach that integrates spatial domain steganography with blockchain technology. The method aims to provide double-layered protection for confidential data by embedding it within images and leveraging blockchain for secure verification, eliminating the need to transfer the stego-object. This approach enhances data security and integrity in digital communications.

Ye(2024) presented an article titled Advancements in Spatial Domain Image Steganography: Techniques, Applications, and Future Outlook, The study focused on Least Significant Bit (LSB) substitution, a widely used method in spatial domain steganography. It evaluates various LSB-based techniques, analyzing their security and image quality metrics. The paper emphasizes the trade-offs between embedding capacity, imperceptibility, and robustness, providing a comprehensive comparison of existing methods.

Zhang(2024) provided a comprehensive analysis of spatial domain image steganography techniques, categorizing them into traditional and deep learning-based methods. It discusses the distinctions between information hiding and encryption, and evaluates the performance of various techniques. The study also charts current trends and suggests future research directions to enhance the security and efficacy of steganographic practices.

Riya & Aruna(2024) in their survey paper examined various image interpolation methods used in spatial domain steganography. It discusses traditional interpolation techniques and their role in data hiding, aiming to balance image quality and embedding capacity. The paper provides an in-depth evaluation of current approaches, highlighting their benefits and drawbacks, and offers research recommendations to enhance both embedding capacity and visual quality of images

2.2 Frequency Domain Techniques

Frequency domain methods in steganography involve embedding secret data within an image by modifying its frequency components, rather than directly altering pixel values like in spatial domain methods. This approach uses transforms like Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT) to convert the image from its spatial domain to the frequency domain .

Pramanik(2023) presented a hybrid steganography technique that combines spatial and frequency domain methods. It utilizes the Integer Wavelet Transform (IWT) to identify high-frequency sub-bands

suitable for embedding. A genetic algorithm selects optimal coefficients to maximize the Peak Signal-to-Noise Ratio (PSNR) of the stego image. The approach demonstrates enhanced security against steganalysis attacks such as PDH analysis and RS analysis, outperforming previous methods like SPAM and SRM.

Kapoor and Shivani, 2024 introduced a novel algorithm that embeds binary data into grayscale images by dividing the host image into 8×88 times 88×8 DCT blocks. Four embedding locations are selected in each block to embed 4 bits of the secret message, enhancing embedding capacity. The method computes differences between DCT coefficients of adjacent blocks to embed the secret bits. Robustness is evaluated against various steganalysis techniques, including median filtering, Gaussian noise, and histogram analysis, showing improved resilience.

Vivek and Anusuya 2024 presented a work titled Robustness Realisation in image steganography using frequency domain-based transforms for e-voting. Their research Addressed the security needs of e-voting systems, the study proposed two steganography models employing Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) fused with Linear Congruential Generators (LCG) for pseudo-random embedding. The models embed voter data into cover images, ensuring confidentiality and integrity. Performance is evaluated using PSNR and RMSE under various noise environments, with the DWT-based technique showing superior robustness under limited payloads.

Chen et.al(2023) proposed a novel method called Low-frequency Image Deep Steganography (LIDS) that manipulates the frequency distribution during the embedding process. By focusing on low-frequency components, the method enhanced robustness against attacks that distort high-frequency components. The approach involves extracting a feature map from the secret image and adding it to the cover image, avoiding high-frequency artifacts. Experimental results showed that LIDS outperforms state-of-the-art methods in terms of robustness while maintaining high fidelity.

Wu et.al(2024) in their study introduced a steganography scheme that utilizes wavelet transformation for side-information estimation, aiming to enhance robustness against image compression and noise. The method focused on embedding data into wavelet coefficients, ensuring that the hidden information remains imperceptible and resilient to various attacks. The scheme demonstrated improved performance in maintaining image quality and data integrity under different conditions.

3. Machine Learning and Deep Learning Approaches

Machine learning (ML) and deep learning (DL) offer powerful approaches to enhance steganography, the practice of hiding information within other media. DL, specifically, has shown promise in creating steganographic systems that are more robust against detection. ML techniques like Support Vector Machines (SVM) or K-Nearest Neighbors (KNN) can be used to identify optimal embedding locations, while DL models like Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) are used for more complex data hiding and extraction tasks

3.1 CNN and Autoencoder-Based Techniques

Bui et, al(2023) in a research titled 'RoSteALS: Robust Steganography using Autoencoder Latent introduced a steganography method that leverages pretrained autoencoders to embed secret messagesThis approach eliminates the need for the embedding process to learn the distribution of cover images, resulting in a lightweight secret encoder (~300k parameters) that is easy to train. The method achieves perfect secret recovery and maintains high image quality across multiple benchmarks. Additionally, RoSteALS can be adapted for cover-less steganography applications, where the cover image is generated from noise or conditioned on text prompts via a denoising diffusion process.

Ofoegbu et al.(2023) proposed an image steganography method combining convolutional autoencoders with the ResNet architecture. The system includes a preprocessing model for feature extraction and an operational model for embedding and extraction, both based on ResNet. Evaluated using the CIFAR dataset, the method demonstrates high imperceptibility (PSNR > 30 dB, SSIM > 0.98) and substantial hiding capacity, enabling the concealment of color images within others.

Ahmad et al.(2024)This paper presents a hybrid approach combining Convolutional Neural Networks (CNNs) and Discrete Cosine Transform (DCT) for image steganography, particularly in cloud-based environments. The CNN extracts robust features from the cover image, while DCT facilitates embedding in the frequency domain, enhancing imperceptibility and data-hiding capacity. The method achieves a balance between security and visual quality, with a competitive execution time of 2.3 seconds, making it suitable for real-world applications.

Subramanian et al.(2021) End-to-End Image Steganography Using Deep Convolutional Autoencoders, This study introduces a lightweight deep convolutional autoencoder architecture designed for embedding a secret image within a cover image. The model emphasizes end-to-end training, allowing the network to learn optimal embedding and extraction strategies directly from data. The approach

achieves high imperceptibility and robustness, making it suitable for practical steganographic applications.

3.2 Steganography using GAN-Based Techniques.

Fan et al(2025) AGASI: A Generative Adversarial Network-Based Approach to Strengthening Adversarial Image Steganography This study introduces AGASI, a GAN-based method designed to enhance the robustness of image steganography against steganalysis. The approach employs an encoder as the generator and a discriminator within the GAN framework to produce stego-images that are resistant to detection. Additionally, a decoder is utilized to accurately extract the secret image from the stego-image. Experimental results demonstrate that AGASI not only maintains high-quality secret images but also significantly reduces the accuracy of neural network classifiers in detecting stego-content, thereby improving the security of the steganographic system .

Li et al.(2024) Image Steganography and Style Transformation Based on Generative Adversarial Network . This paper presents a novel approach that integrates image steganography with style transformation using GANs. The proposed method embeds secret messages during the generation of art-style images, making the stego-images indistinguishable from typical style-transferred images. By employing an encoder–decoder model and adversarial training, the technique ensures high imperceptibility and robustness against steganalysis. The approach achieves an embedding capacity of up to 3 bits per pixel for color images, providing a secure means of covert communication on social networks.

Ramandi et al(2024) VidaGAN: Adaptive GAN for Image Steganography VidaGAN introduces an adaptive GAN framework for image steganography that addresses challenges such as low network accuracy and imbalances between capacity and transparency. The architecture comprises an encoder, decoder, and critic, incorporating innovations to enhance visual quality and embedding capacity. VidaGAN achieves a hiding capacity of 3.9 bits per pixel on the DIV2K dataset and demonstrates resilience against steganalysis tools like StegExpose, indicating its effectiveness in secure data hiding applications. .

4. Steganalysis and Detection

Steganalysis when applied on images aim to detect hidden data within it, this is the opposite of steganography, that has to do with concealing information.

4.1 Steganalysis and Detection

Li & Dong(2024) in their research work titled Image Steganalysis Algorithm Based on Deep Learning and Attention Mechanism for Computer Communication, present an image steganalysis algorithm that integrates deep learning with attention mechanisms to enhance detection accuracy. By incorporating attention modules into convolutional neural networks, the model focuses on relevant regions of the image, improving the identification of hidden information. Experimental results demonstrate a recognition accuracy of 92.58% on a dataset of 20,000 images, indicating the model's effectiveness in practical scenarios.

Chikkara et al.(2023) introduced a blind image steganalysis method utilizing a modified Bird Swarm Algorithm (BSA) for feature selection. The approach enhances the detection of stego-images by optimizing feature subsets, leading to improved classification accuracy when combined with Support Vector Machines (SVM). The method demonstrates effectiveness in identifying hidden information without prior knowledge of the embedding algorithm .

Huo et al.(2024) proposed CHASE, a steganography network that combines chaotic mapping with GANs to achieve high-capacity and secure image steganography. The method enables the embedding of color images into grayscale images by reducing differences between the container and cover images through image permutation techniques. The integration of chaotic mapping and GAN optimization enhances both the security and image quality of the steganographic process. Experimental evaluations indicate that CHASE offers superior resistance to steganalysis and maintains high fidelity in the extracted secret images, outperforming existing state-of-the-art methods

Zhu et al.(2023) presented a novel, energy-efficient steganalysis framework based on green learning principles. It comprises three modules: pixel-based anomaly prediction, embedding location detection, and decision fusion for image-level classification. GS achieved comparable detection performance to state-of-the-art deep learning models while significantly reducing computational complexity and model size, making it suitable for deployment on mobile and edge devices.

Farooq & Selwal(2023) Prsesented a comprehensive review that examines the evolution of image steganalysis techniques, emphasizing the transition from traditional methods to deep learning approaches. It discussed various deep learning architectures, such as Convolutional Neural Networks

(CNNs), and their effectiveness in detecting steganographic content. The paper also identifies open research challenges, including the need for large annotated datasets and the development of robust models against adaptive steganography .

Aljarf et al.(2024) investigated the practicality of blind image steganalysis using feature-based classification methods. By extracting features such as Gray-Level Co-occurrence Matrix (GLCM) properties and employing Radial Basis Function (RBF) classifiers, the study evaluates the effectiveness of detecting stego-images without prior knowledge of the embedding algorithm. The findings suggest that feature-based classifiers can achieve reasonable detection accuracy, highlighting their potential in real-world applications.

5. Applications of Image Steganography

5.1 Secure Communication

Military and intelligence operations use steganography to transmit secret messages that are concealed within innocuous-looking images, reducing the risk of interception. **Diplomatic communication** between governments or agencies may use stego-images to securely share sensitive documents or data.

Rezaei and Javadpour(2024) proposed an innovative image steganography approach utilizing a fusion of bio-inspired algorithms, including Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Simulated Annealing (SA). The method aims to enhance data security and image quality by optimizing the embedding process, thereby disrupting pixel correlations that could reveal hidden information. The study conducts extensive experiments on both grayscale and color images, demonstrating improved Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) values, which indicate better image quality and robustness against attacks.

5.2 Copyright Protection and Authentication

Used to **embed watermarks or copyright information** directly into media (images, audio, video) for authentication and ownership verification. Prevents **unauthorized duplication or distribution** of digital content by making ownership details retrievable but hidden

Zaina et,al(2024) in a research work titled ‘A Hybrid Steganography and Watermark Algorithm for Copyright Protection’ by Using Multiple Embedding Approaches presents a hybrid algorithm that combines steganography and watermarking techniques to enhance copyright protection. The method

employs multiple embedding strategies, including Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), One-Time Pad (OTP), and Playfair cipher, to embed watermark information into digital images.

5.3 Forensic and Legal Evidence

Investigators can **embed metadata or case details** within forensic images to maintain chain-of-custody without altering the visible image.

Newman et.al.(2019) This study introduces *StegoAppDB*, a comprehensive image database designed to support forensic investigations involving steganography. Recognizing the increasing use of steganographic applications on mobile devices, the researchers compiled a dataset comprising over 810,000 images, including both original (cover) and stego images generated using various mobile steganography app

Internet of Things (IoT) and Smart Systems

Hassaballah et al.(2021) in their work titled A Novel Image Steganography Method for Industrial Internet of Things Security , introduced an innovative approach to enhance security in Industrial IoT (IIoT) environments by employing image steganography. The proposed method utilizes the Harris Hawks Optimization (HHO) algorithm in conjunction with the Integer Wavelet Transform (IWT) to embed secret data within digital images. The HHO algorithm optimizes the selection of pixel locations for data embedding, ensuring minimal distortion and high imperceptibility.

6. Challenges and Limitations

Key challenges include:

- Trade-offs between capacity, imperceptibility, and robustness.
- Vulnerability to compression and image processing.
- Adaptive steganalysis and machine learning-based detection.

Laxmi & Rajkumar (2023) provided a comprehensive examining both traditional and modern image steganography techniques, highlighting several persistent challenge

7. Future and Emerging Trends

Emerging trends include:

7.1 Explainable Steganography

Explainable steganography aims to make the process of hiding information in plain sight to be transparent and understandableImplementing explainable AI (XAI) techniques to understand where and how information is hidden, aiding in transparency and trust.

Kuchumova et al.(2024) in their work titled 'STEG-XAI: Explainable Steganalysis in Images Using Neural Networks 'introduced STEG-XAI, a novel methodology that combines convolutional neural networks (specifically, the EfficientNet architecture) with explainability techniques like LIME and Grad-CAM. The approach not only detects steganographic content in images but also provides visual explanations of the model's decisions, highlighting the specific modifications introduced by steganography algorithms such as UERD. The model achieved a weighted AUC of 0.944, demonstrating high discrimination between original and tampered images

7.2 Steganography for Multimedia and 3D Data

- Expanding from static images to **video, 3D models, AR/VR content**, and **metaverse assets**, adapting to emerging digital formats..

Zhang et al.(2025) in their paper titled "SecureGS: Boosting the Security and Fidelity of 3D Gaussian Splatting Steganography" introduced *SecureGS*, a framework designed to enhance the security and fidelity of 3D Gaussian Splatting (3DGS) steganography. 3DGS has emerged as a premier method for 3D representation due to its real-time rendering capabilities and high-quality outputs. Traditional Neural Radiance Fields (NeRF) steganography methods are inadequate for 3DGS due to these explicit characteristics. Existing solutions often compromise rendering fidelity, increase computational demands, and have security vulnerabilities, particularly concerning the geometric structure of visualized point cloud.

7.3 Integration with Blockchain

Using blockchain for secure transmission and verification of stego-content, ensuring tamper-proof audit trails and decentralized control.

Integrating block chain technology can provide added layer of security, Singh(2023) applied LSB along with hash function in producing the stego image in his paer titled"Block chain Image based Steganography.**"**

7.4 Steganography in IoT and Edge Devices

- Lightweight, energy-efficient algorithms designed for **resource-constrained environments** like sensors, wearables, and edge AI systems.

Cao et al.(2024) introduced an innovative framework that integrates blockchain technology with generative behavior steganography to enhance secure communication in IoT edge computing environments. The proposed system employs a fog computing architecture, utilizing the InterPlanetary File System (IPFS) for decentralized data storage. To safeguard data retrieval processes, stream cipher encryption is applied to file hash values A distinctive feature of this framework is the use of AlphaZero's Gomoku algorithm for steganographic transmission. This approach allows for the covert dissemination of stream cipher keys across the blockchain network without relying on traditional carriers, thereby achieving a dual-layer encryption mechanism. Experimental results indicate that this model significantly improves the capacity for confidential information transmission, scaling from kilobytes to megabytes, while maintaining high levels of security and discretion.

7.5 Quantum and Blockchain Integration

- **Quantum steganography** is an emerging field exploring how quantum states can be used for unbreakable covert communication.
- **Blockchain** is used to validate and timestamp stego transactions, providing auditability and protection against tampering.

Dutta et al.(2025) introduces innovative quantum steganographic protocols that leverage catalytic and entanglement-assisted quantum error-correcting codes (QECCs). The authors propose three distinct schemes:

1. **Catalytic Quantum Codes**: Utilize minimal pre-shared resources to embed secret messages within quantum codes, enhancing efficiency.
2. **Entanglement-Assisted QECCs**: Incorporate prior entanglement into QECCs, allowing for the embedding of steganographic information while maintaining code performance.
3. **Phase Bit Embedding**: Employ the phase bit of a pre-shared entangled bit (ebit) combined with QECCs to conceal information.

These protocols aim to minimize the resources required for secure quantum steganography, making them suitable for integration with blockchain systems that prioritize efficiency and security.

7.6 Coverless Steganography

- Instead of modifying existing images, new methods generate the stego image directly (e.g., using GANs) with the hidden message encoded from scratch.
- This eliminates tell-tale statistical artifacts common in traditional methods.

Yang et al.(2024) in their article titled"DiffStega: Towards Universal Training-Free Coverless Image Steganography with Diffusion Models "introduced a training-free approach to coverless image steganography by leveraging diffusion models. It employs a password-dependent reference image alongside text prompts, ensuring that only authorized parties can retrieve hidden information. The method also incorporates a "Noise Flip" technique to enhance security against unauthorized decryption.

Liu et al. (2024) in their study titled 'A Dynamic YOLO-Based Sequence-Matching Model for Efficient Coverless Image Steganography' presented a coverless steganography scheme that utilizes the YOLO object detection model to select optimal objects within images. A mapping dictionary is established between these objects and scrambling factors, enabling efficient data hiding. The approach demonstrates robustness against geometric attacks and requires a relatively small image library for effective steganography.

8.0 Conclusion

From simple spatial domain methods to complex deep learning-based strategies like CNNs, autoencoders, and GANs, the topic of image steganography has undergone substantial development. These developments have significantly increased the ability to conceal data, make it imperceptible, and make it resistant to steganalysis. With a focus on security and interpretability, recent studies have also investigated cutting-edge fields like explainable steganography, forensic applications, and IoT integration. Notwithstanding these advancements, there are still issues, such as computational complexity, payload-capacity trade-offs, and susceptibility to sophisticated detection technologies. Future research must concentrate on creating adaptive, intelligent, and transparent steganographic systems that can guarantee safe, undetectable, and morally sound data hiding across a variety of application domains as digital communication becomes more widespread and surveillance becomes more sophisticated.

9.0 Acknowledgment.

I will like to thank my friends and colleagues for the support shown in the course of writing this paper.

REFERENCES

Abuali, M. S., Rashidi, C. B. M., Salih, M. H., Raof, R. A. A., & Hussein, S. S. (2019). Digital image steganography in spatial domain a comprehensive review. *Journal of Theoretical and Applied Information Technology*, *97*(19), 5081–5102.

Ahmad, S., Ogala, J. O., Ikpotokin, F., Arif, M., Ahmad, J., & Mehfuz, S. (2024). Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud. *SN Computer Science*, *5*(4). https://doi.org/10.1007/s42979-024-02756-x

Aljarf et al.(2024) This research investigates the practicality of blind image steganalysis using feature-based classification methods. By extracting features such as Gray-Level Co-occurrence Matrix (GLCM) properties and employing Radial Basis Function (RBF) classifiers,

Bui, T., Agarwal, S., Yu, N., & Collomosse, J. (2023a). RoSteALS: Robust Steganography using Autoencoder Latent Space. *ArXiv:*, *1*. http://arxiv.org/abs/2304.03400

Cao, Yuanlong & Li, Junjie & Chao, Kailin & Xiao, Jianmao & Lei, Gang. (2024). Blockchain Meets Generative Behavior Steganography: A Novel Covert Communication Framework for Secure IoT Edge Computing. Chinese Journal of Electronics. 33. 886-898. 10.23919/cje.2023.00.382.

Dutta, S., Dash, N. R., Banerjee, S., & Srikanth, R. (2025). *Quantum steganography using catalytic and entanglement-assisted quantum codes*. http://arxiv.org/abs/2505.15869

Fan, H., Jin, C., & Li, M. (2025). AGASI: A Generative Adversarial Network-Based Approach to Strengthening Adversarial Image Steganography. *Entropy*, *27*(3). https://doi.org/10.3390/e27030282

Farooq, N., Selwal, A. Image steganalysis using deep learning: a systematic review and open research challenges. *J Ambient Intell Human Comput* 14, 7761–7793 (2023). https://doi.org/10.1007/s12652-023-04591-z

Hamid, Nagham & Yahya, Abid & Ahmad, R.Badlishah & Al-qershi, Osamah. (2012). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security. 6. 168-187.

Hassaballah M., Hameed M, Awad A, & Muhammad K. (2021). A Novel Image Steganography Method for Industrial Internet of Things Security. IEEE Transactions on Industrial Informatics. 17. 7743-7751. 10.1109/TII.2021.3053595.

Huo, L., Chen, R., Wei, J., & Huang, L. (2024). A High-Capacity and High-Security Image Steganography Network Based on Chaotic Mapping and Generative Adversarial Networks. *Applied Sciences (Switzerland)*, *14*(3). https://doi.org/10.3390/app14031225

Kapoor, S., Shivani, S. Robust and high capacity image steganography technique using spiral-walk inter-block DCT coefficient differencing. *Multimed Tools Appl* 83, 86405–86424 (2024). https://doi.org/10.1007/s11042-024-19520-1

Kuchumova, E., Martínez-Monterrubio, S.M. & Recio-Garcia, J.A. STEG-XAI: explainable steganalysis in images using neural networks. *Multimed Tools Appl* 83, 50601–50618 (2024). https://doi.org/10.1007/s11042-023-17483-3

Kumar Singh, A., & Singh, A. K. (2023). *Blockchain Based Image Steganography*. http://ijesc.org/

Laxmi. (2024). Advancements and Challenges in Image Steganographer: A Comprehensive Review. *International Journal of Communication Networks and Information Security*, *2023*(4), 462–484. https://https://ijcnis.org/

Lan, Y., Shang, F., Yang, J., Kang, X., & Li, E. (2023). *Robust Image Steganography: Hiding Messages in Frequency Coefficients*. www.aaai.org

Li, H., & Dong, S. (2024). Image steganalysis algorithm based on deep learning and attention mechanism for computer communication. *Journal of Electronic Imaging*, *33*(01). https://doi.org/10.1117/1.jei.33.1.013015

Li, L., Zhang, X., Chen, K., Feng, G., Wu, D., & Zhang, W. (2024). Image Steganography and Style Transformation Based on Generative Adversarial Network. *Mathematics*, *12*(4). https://doi.org/10.3390/math12040615

Newman, J., Lin, L., Chen, W., Reinders, S., Wang, Y., Wu, M., & Guan, Y. (2019). *StegoAppDB: a Steganography Apps Forensics Image Database*. http://arxiv.org/abs/1904.09360

Ofoegbu, C., Ofoegbu, C. I., Nwokorie, E. C., & Amadi, O. S. A. (2023). An Improved Image Steganography System Using Convolutional Neural Networks. In *International Journal of Research Publication and Reviews* (Vol. 4, Issue 11). www.ijrpr.com

Pramanik, S. An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm. *Multimed Tools Appl* 82, 34287–34319 (2023). https://doi.org/10.1007/s11042-023-14505-y

Punia, R., Malik, A. (2023). Image Interpolation-Based Steganographic Techniques Under Spatial Domain: A Survey. In: Tanwar, S., Wierzchon, S.T., Singh, P.K., Ganzha, M., Epiphaniou, G. (eds) Proceedings of Fourth International Conference on Computing, Communications, and Cyber-Security. CCCS 2022. Lecture Notes in Networks and Systems, vol 664. Springer, Singapore. https://doi.org/10.1007/978-981-99-1479-1_50

Ramandi, V. Y., Fateh, M., & Rezvani, M. (2024). VidaGAN: Adaptive GAN for image steganography. *IET Image Processing*. https://doi.org/10.1049/ipr2.13177

Rezaei, S., & Javadpour, A. (2024). Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-18776-x

Sabri Abuali, M., Aliana Raof, R. A., Rashidi, C., Salih, M. H., A Raof, R. A., & Saad Hussein, S. (2019). DIGITAL IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN A COMPREHENSIVE REVIEW. *Article in Journal of Theoretical and Applied Information Technology*, *15*, 19. www.jatit.org

Subramanian, Elharrouss, Alma'adeed, & Bouridane. (2021). (PDF) End-to-End Image Steganography Using Deep Convolutional Autoencoders. *IEEE Access*, 1–1.

Suresh, K. S., & Kamalakannan, D. T. (n.d.). International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Digital Image Steganography in the Spatial Domain Using Block-Chain Technology to Provide Double-Layered Protection to Confidential Data Without Transferring the Stego-Object. In *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE* (Vol. 2023, Issue 2s). www.ijisae.org

Vivek M , Anusuya K. (2024)Robustness realisation in image steganography using frequency domain-based transforms for e-voting
Electronic Government, an International Journal .20:2, 223-239

Wu, T., Hu, X., Liu, C., Wang, Y., & Zhu, Y. (2024). An efficient steganography scheme based on wavelet transformation for side-information estimation. *Journal of King Saud University - Computer and Information Sciences*, *36*(6). https://doi.org/10.1016/j.jksuci.2024.102109

Yang, Y., Liu, Z., Jia, J., Gao, Z., Li, Y., Sun, W., Liu, X., Zhai, G., Jiao, S., & University, T. (2024). *DiffStega: Towards Universal Training-Free Coverless Image Steganography with Diffusion Models*. https://github.com/evtricks/DiffStega.

Ye. (2024). Advancements in Spatial Domain Image Steganography_ Techniques, Applications, and Future Outlook _ Applied and Computational Engineering. *Applied and Computational Engineering*, *94*, 6–19.

Zainal, N., Hoshi, A. R., Ismail, M., Rahem, A. A. R. T., & Wadi, S. M. (2024). A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches. *Bulletin of Electrical Engineering and Informatics*, *13*(3), 1877–1896. https://doi.org/10.11591/eei.v13i3.6337

Zhang, C. (2024). Research on Key Technologies of Spatial Domain Image Steganography and Analysis of Typical Applications. In *Transactions on Computer Science and Intelligent Systems Research* (Vol. 6).

Zhang, X. ,Meng, J. Xu, Z.,Yang, S. ,Wu, Y. ,Wang, R. & Zhang, J. (2025). SecureGS: Boosting the Security and Fidelity of 3D Gaussian Splatting Steganography. 10.48550/arXiv.2503.06118.

Zhu, Y., Wang, X., Chen, H.-S., Salloum, R., & Kuo, C.-C. J. (2023). *Green Steganalyzer: A Green Learning Approach to Image Steganalysis*.