CHAPTER 13

HIDDEN IN PLAIN SIGHT: STEGANOGRAPHY'S ROLE IN DIGITAL SECURITY

RAKESH KUMAR, SAVINA BANSAL AND R K BANSAL

Dept. of ECE, GZS Campus, MRSPTU, Bathinda, Punjab, India.

Abstract: Steganography involves concealing secret information within digital media by exploiting redundancies and limitations in human perception. This comprehensive review traces the evolution of steganography from ancient civilizations to present-day advances propelled by AI and deep learning. A taxonomy categorizes steganography based on cover object- text, image, audio, video, and network protocols- used to conceal messages. Core technical data hiding approaches like least significant bit encoding, transform coefficients manipulation, and generative adversarial networks are explored. Practical challenges around security, capacity, robustness and ethical concerns are discussed. Recent strides in robust JPEG steganography, AI-driven text hiding and adversarial techniques point to an intriguing future for this domain. Applications across healthcare, business, governance and academia underscore the vast potential. However, the escalating sophistication of steganalysis, fueled by machine learning, necessitates ongoing innovation in this dynamic field.

Keywords: Steganography, digital security, data hiding, GANs.

1. Introduction

Steganography is the practice of concealing information within digital media, such as images, audio, video, or text, in a way that is not apparent to casual observer [1]. As digital communication continues to proliferate and

sensitive data transmission becomes increasingly vulnerable to interception, steganography offers a clandestine method to safeguard confidential information. The word steganography comes from the Greek words *steganos*, meaning "covered", and *graphein* meaning "to write" [2]. The hidden information itself is called the payload, while the data used to hide the payload is called the cover-text, cover-image, cover-audio or cover-video. The key goal of steganography is covert communication - to hide the very presence of communication. It serves as a contrast to cryptography, which transforms the hides the content of a message but usually reveals the existence of communication. With successful steganography, an adversary would not be able to detect the hidden information at all. Steganography can be useful for a range of applications requiring secure and secret communication. However, it also poses ethical challenges regarding privacy and consent. Overall, steganography is a method that exploits the redundancies in data representation to embed secret messages with diverse modern applications as well as historical precedents.

1.1 Evolution of Steganography

The origins of steganography can be traced back to ancient times when people devised clever methods to conceal information. One of the earliest documented instances of steganography dates to 440 BC, where the Greek historian Herodotus described how a message was tattooed on the shaved head of a slave and then left to regrow hair before being sent. This technique allowed the recipient to read the hidden message only after shaving the slave's head again [2]. Throughout history, various civilizations and cultures employed steganography techniques to transmit secret messages. Ancient Greek texts mention the practice of etching messages on tablets and covering them with wax upon which a legitimate message is written. During the 15th and 16th centuries, early forms of invisible inks were used to hide information inside seemingly innocuous letters and documents [3].

In the 20th century, the onset of world wars and rise in cryptography also led to advances in steganography research and techniques. Microdots became a popular way to hide photographic information in typewritten text. During WWII, null ciphers were used to hide messages by adding superfluous or nonsensical text. With the growth of computation power several digital techniques emerged such as coding secret messages into least significant bits of image and audio files or by carefully modifying image properties [2] [3].

In the contemporary digital era, the Internet and proliferation of digital files provides the perfect cover objects to hide secret communication through steganography. From images posted on public forums to audio files on music sites - a wide variety of file types with a high degree of redundant bits can be exploited to securely embed hidden payloads. This makes modern steganography highly relevant for covert communication. Powerful AI techniques also continue to bolster steganography methods today.

1.2 Classification of Steganography

Steganographic techniques can be broadly categorized based on the type of cover object used for embedding secret messages, as illustrated in Figure 1. The cover object provides the communication medium that masks the hidden data. Choosing covers with high redundancy and randomness enables more effective information hiding [1].

1. Text Steganography

Text steganography refers to the technique of concealing secret information within text files and documents. Subtle manipulations are made to properties of electronic texts to embed messages while preserving semantic coherence and escaping statistical detection. Some key techniques include [4]:

- *Syntax Morphing*: Manipulates syntax of text to hide data e.g., altering punctuation marks, conjugating verbs differently.
- *Semantic Manipulation*: Substitutes words and phrases with synonyms or reorders parts of speech to hide payload.
- *Vertical Shifting*: Encodes data by vertically shifting lines of text by specified number of points.
- *Open Space Manipulation*: Embeds data in open white spaces between words and paragraphs.

2. Image Steganography

Image steganography is by far the most researched technique in steganography that leverages digital images as cover objects. Payload is embedded through manipulation of image content and properties. Both spatial and frequency domain techniques are employed for hiding information while preserving visual quality. Some approaches include:

- *Spatial Domain Techniques*: Manipulates pixel intensity values directly to encode bits.
- *Transform Domain Techniques*: Alters image properties in frequency domain after mathematical transforms.
- *Masking & Filtering*: Uses data hiding in selective significant regions of interest in image.
- Integrates with machine learning models like GANs to automate hiding in generated natural images.

3. Audio Steganography

Audio steganography [5] [6] refers to hiding secret information within digital sound files and streaming audio. It exploits limits of human auditory perception and audio properties like masking, echo and phase to embed messages while preserving file quality. Some key techniques include:

- *Temporal Encoding*: Alters time domain amplitude/frequency to encode payload.
- *Frequency Domain Encoding*: Manipulates spectrographic transform representations.
- *Ambient Mimicry Insertion*: Imitates and inserts payload within ambient sounds.

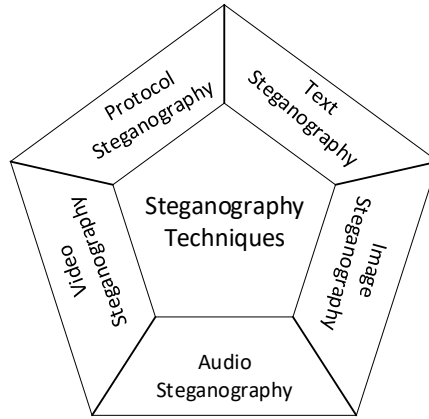

Figure 1 Classification of steganography techniques

4. Video Steganography

Video steganography [7] leverages the high inter-frame redundancy in digital videos and limitations in human visual perception to embed hidden payloads through subtle pixel value variations. It encodes messages both in spatial as well as frequency domain representations across video frames and formats. Major approaches include:

- *Frame Sequence Encoding*: Leverages high inter-frame redundancy in videos by embedding payload through pixel variations between frames.
- *ROI Substitution*: Replaces selected regions of interest across frames with payload embedded image/video patches.
- *Transform Domain Techniques*: Embeds data by altering transformed coefficients of visual contents in frequency domain.
- *Format Impersonation*: Generates stego video that mimics normal video syntax and behaviors with hidden payload.

5. Protocol Steganography

Network protocol steganography [8] [9] refers to techniques for hiding information within network protocols and behaviors. It alters non-functional optional protocol fields or creates covert channels using subtle timing, sequencing and error anomalies. Below are some core techniques:

- *Manipulating Packet Headers*: Altering optional header fields reserved for future.
- *Leveraging Covert Channels*: Hiding data in header timings, packet sequencing.
- *Generating Stego Traffic*: Creating innocent cover protocol behaviors or transactions with embedded payload.

2. Overview of Steganography Process

The steganography process essentially involves hiding a secret message (payload) within a cover object like a digital image, audio, video, text file or network packet. The output product is called a stego object which contains the hidden information. A generalized version of typical steganography system is shown in Figure 2, major steps are:

1. *Payload preparation*: The secret message to be hidden is first preprocessed and encrypted using cryptography. Optional compression is applied to reduce payload size. Error correction codes may be added to compensate for potential cover object distortions. This prepared payload is embedded in the next stages.
2. *Selection of cover object*: An appropriate carrier for hiding is chosen - such as an image file, audio track, video file, text document or network streams depending upon channel constraints. Required properties include high data redundancy and low susceptibility to distortion.
3. *Embedding process*: This key stage hides the encrypted payload within the cover object by exploiting redundancies in its data representation or subtle signal alterations that are imperceptible to human perception. Common techniques modify least significant bits, discrete cosine transform coefficients or spread spectrum modulation for images/audio. For text, syntactic/semantic modifications or random character insertions may hide data.
4. *Stego object transmission*: The payload embedded object (stego object) is transmitted over the chosen communication channel to the receiving party where message extraction can occur.
5. *Extraction process*: Using shared secret keys, the payload is extracted from the stego object by reversing the embedding process. Decryption delivers the original hidden message payload to the receiver.

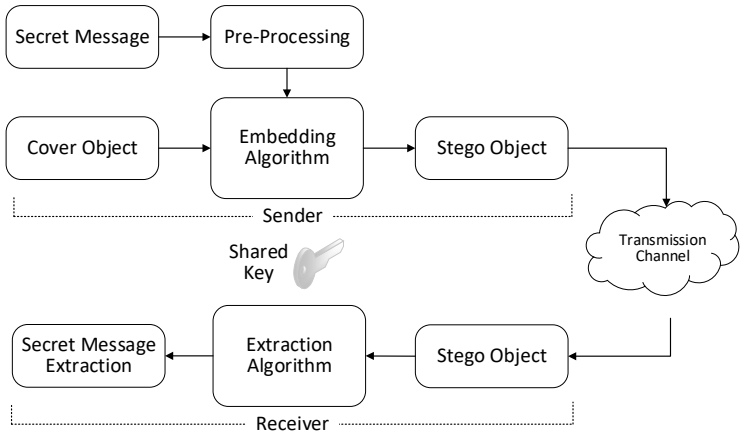

Figure 2 A typical steganography system.

3. Image Steganography

Image steganography refers to hiding secret payloads within digital images. It exploits redundancies in pixel data representation and limitations of human visual perception to embed messages. With the proliferation of images on social platforms and websites, image steganography offers immense potential for covert communication. Image steganography techniques can be categorized as:

1. Spatial Domain Techniques:

These techniques directly manipulate pixel intensity values in the image spatial domain to conceal data [10] [11] [12].

- *Least Significant Bit (LSB) Substitution*: A common approach that replaces the insignificant LSB bits of randomly or cautiously selected pixels with payload bits. Offers simplicity but vulnerable to statistical steganalysis attacks.
- *Pixel Value Differencing (PVD)*: Encodes data based on differences between neighborhoods of pixels. Provides better imperceptibility than LSB. More resilient against common image processing attacks than LSB techniques.
- *Histogram Shifting*: Shifts peak and minimum intensities on the image histogram to create vacant bins for hiding data. Reversible method but has limited capacity.
- *Pixel Pattern Matching*: Creates an adaptive dictionary key table mapping patterns of pixel intensities to payload bits allowing high density capacity. Fast extraction possible if key preserved.

2. Transform Domain Techniques:

These methods transform the image into frequency domain using mathematical functions before data hiding in coefficients [13] [14] [15] [16].

- *Discrete Cosine Transform (DCT)*: Divides image into 8x8 non-overlapping blocks and applies DCT. Hides bits in middle frequency coefficients for imperceptibility. Offers improved resilience to lossy JPEG compression over spatial techniques.
- *Discrete Wavelet Transform (DWT)*: Decomposes image into multi-resolution sub-bands using wavelet transforms. Payload embedded

by modifying coefficients in vertical, horizontal and diagonal details. Provides enhanced security with moderate capacity.

- *Discrete Fourier Transform (DFT)*: Transforms image pixels into sine and cosine spectral components. Hiding occurs in phase or magnitude elements of the frequency spectrum before inverse transform.

3. AI-driven Adaptive Techniques [17] [18]:

- *Visual Saliency Maps*: Train machine learning models like CNNs to score image regions by noticeability level. Guides adaptive capacity hiding in complex textures over flat areas.
- *Generative Adversarial Networks*: Steganographer and steganalyst neural nets compete to boost hiding capacity without detectability. The generator learns to create stego images closely resembling cover data distribution to fool warden's discriminator nets.
- *Metaheuristic Optimization*: Computational intelligence schemes like genetic algorithms guide optimal pixel modification for data hiding to escape visual artifacts and statistical detection.

With extensive options for covert data hiding to leverage, image steganography continues to be an active domain for contemporary research and innovation. However, embedding capacity and resilience to attacks remain persistent challenges in practical deployments.

4. Challenges and Issues

In the era of widespread digital communication and ubiquitous digital media, steganography finds ample opportunities. However, its effectiveness is countered by various challenges that warrant careful consideration.

1. Detection Techniques
   - *Advancements in Steganalysis:* As steganography techniques evolve, so do steganalysis techniques. The ongoing cat-and-mouse game between steganographers and those trying to detect hidden information poses a significant challenge. New statistical and machine learning-based methods are continually developed to improve the detection of hidden data.
2. Capacity vs. Security Trade-off
   - *Payload Capacity*: Increasing the capacity to hide more data within a cover medium often comes at the cost of security. Higher payload capacity might make it easier for detection algorithms to identify

patterns or anomalies, reducing the overall effectiveness of the steganography.

3. Media Compatibility and Robustness
   - *Compatibility*: Steganography techniques are often designed for specific media types (images, audio, video). Adapting these techniques to different multimedia formats while maintaining effectiveness and security is a non-trivial task.
   - *Data Transmission and Transformation*: The robustness of steganography methods under various transformations (compression, cropping, resizing, etc.) is a significant concern. The hidden information should be able to withstand common data manipulations without being corrupted or lost.
4. Human Perception
   - *Human Sensitivity*: Some steganography methods rely on exploiting imperceptible changes in the cover medium. However, humans may still detect subtle alterations, especially when dealing with high-quality multimedia content.
5. Dynamic Environments and Advancements in Technology:
   - *Changing Network Conditions*: In the context of network steganography, where information is hidden in network traffic, variations in network conditions can impact the effectiveness of hiding and extracting data.
   - *Emerging Technologies*: The rapid advancement of technology, including the use of artificial intelligence and machine learning, can pose both opportunities and challenges for steganography. As detection methods become more sophisticated, steganography techniques need to evolve to stay ahead.
6. Legal and Ethical Concerns
   - *Misuse and Illegal Activities*: Steganography can be misused for illegal activities, such as hiding malware or facilitating covert communication for malicious purposes. This raises legal and ethical concerns, leading to increased scrutiny and regulations.
7. Authentication and Key Management
   - *Authentication and Encryption*: Authentication measures play a pivotal role in verifying the legitimacy of the steganographic payload. In the event of detection, encryption becomes a crucial layer of defense, preventing unauthorized parties from deciphering the concealed information, thereby preserving the integrity and confidentiality of the hidden data.
   - *Secure Key Distribution*: Ensuring a robust mechanism for securely distributing encryption keys is essential for safeguarding

steganographic communications. The secure exchange of keys between communicating parties prevents unauthorized access to hidden information.

5. Role of AI in steganography

Artificial intelligence has come to play a major role in boosting both modern steganography strategies as well as detection mechanisms [19]:

1. Automated embedding algorithms: AI models like generative adversarial networks (GANs) and autoencoders can learn statistical patterns in cover objects and manipulate their data representations to optimize hiding capacity and evade steganalysis.
2. Intelligent multimedia selection: Neural networks can be trained to suggest optimal cover image, audio and video file candidates from a database to match expected channel capacity constraints for hiding secret messages. This facilitates well-versed stego object creation.
3. Natural language generation: Recurrent neural network architectures like LSTMs can mimic patterns in human written stories and alter or generate message bearing cover text that escapes linguistic steganalysis detection by both AI and human examination.
4. Augmented steganalysis: Deep learning offers state-of-the-art performance in detecting presence of steganography that exceeds human analysis.

In essence, AI offers adaptive learning capabilities to substantially advance the potential of steganography while presenting challenges that require innovative research to address and contain risks.

6. Recent Advances in Steganography

In recent years, steganography has witnessed remarkable advancements, propelled by innovations in technology and the dynamic landscape of information security. Notable progress has been made in the realms of deep learning-based techniques, adversarial steganography leveraging powerful neural networks, specialized approaches like robust JPEG steganography, and intriguing experiments by entities such as OpenAI in the domain of text-based covert communication [20] [21] [22].

1. Deep Learning-Based Steganography:
   - Overview: Deep learning has revolutionized steganography by leveraging neural networks to enhance the hiding and extraction of information within digital content.
   - Techniques: Neural networks are employed to learn complex patterns and relationships in data, enabling the creation of more sophisticated and adaptive steganographic methods.
   - Advancements: Recent developments focus on improving the robustness of deep learning-based steganography against advanced detection techniques, ensuring a higher level of security in covert communication.

2. Adversarial Steganography:
   - Concept: Adversarial steganography integrates principles from adversarial machine learning, particularly the use of Generative Adversarial Networks (GANs), to improve the covert communication process.
   - Operation: GANs generate cover media that closely resembles real content, making it challenging for detection algorithms to distinguish between original and modified data.
   - Challenges: Researchers are actively addressing challenges such as maintaining the imperceptibility of modifications while enhancing the security of the hidden information.

3. Robust JPEG Steganography:
   - Focus: Robust JPEG steganography specifically targets concealing information within JPEG images, a widely used format known for its lossy compression.
   - Improvements: Recent efforts aim to enhance the robustness of hiding techniques within JPEG compression, considering factors like resistance to visual quality degradation and adaptability to various JPEG compression levels.
   - Applications: Robust JPEG steganography finds applications in scenarios where JPEG images are prevalent, such as web-based content, digital photography and social networking platforms.

4. Text-Based Steganography based on generative AI:
   - OpenAI's Initiative: OpenAI has undertaken an evaluation [23] of text-based steganography, examining the AI system's proficiency in encoding information within text without raising suspicion.

- Approach: The methodology involves implementing subtle modifications to text formatting, word choices, or linguistic structures to embed hidden messages discreetly, ensuring they escape casual observation.
- Applications: Text-based steganography demonstrates practical utility in communication channels where multimedia content may be unsuitable or restricted. It emerges as a versatile and inconspicuous method for covert communication.

7. Applications of steganography

Steganography has several present-day uses, and holds promise for many next-generation applications leveraging its covert communication capabilities.

1. Healthcare:
   - *Transmitting patient data securely*: Steganography enables hiding entire medical records or lab reports within scan or test images shared between certified hospital systems to prevent exposure of sensitive diagnoses while preserving formatting needs.
   - *Covert public health messaging*: Public health agencies can embed epidemic warnings and safety protocol updates within routine public information website banners using text and image steganography to avoid tendency for rumors while securely alerting certified district officials.

2. E-Governance:
   - *Circulation of confidential surveys*: Online municipal surveys of public spaces can conceal within map interface image files additional audit checklist forms for authorized inspectors allowing discrete sharing of draft compliance findings before final submission.
   - *Watermarking tender documents*: Government tender application pdf attachments can secretly encode applicant identity watermarks through text steganography. This allows tracking leak sources if any proposals surface publicly prior to bidding - thus protecting integrity of process.

3. Business:
   - *Concealing trade secrets*: Companies can use image stenography to embed confidential design documents and material samples within

routine catalog brochure graphics to securely share with offshore production partners without revealing core intellectual property.
- *Watermarking customer data*: By embedding customer account IDs within promotional coupon graphics using stenographic techniques, online retailers can track data breaches if the coupons surface on dark web marketplaces.

4. Covert Communication:
   - *Safe circulation of banned texts/media*: Dissidents trapped under autocratic regimes use audio, image and video steganography to share censored literature, art and humanitarian news stories through common social platforms avoiding direct attacks on freedom of speech.

5. Academia:
   - *Plagiarism tracking systems*: Universities can embed student ID watermarks within routinely submitted coursework documents using spaced text and image steganography allowing tracking of unreferenced third-party content reuse across anonymized submissions.

6. AI and Steganography:
   - *Automated high-volume broadcasting*: GAN powered models can generate natural looking image and video stego objects for hiding large encrypted payloads supporting mass covert transmission undetectable to humans.
   - *Multi-channel hybrid techniques*: AI can orchestrate combining linguistic, image, audio and video steganography dynamically based on content constraints for more secure information hiding.

7. Steganalysis Using AI:
   - *Automated detection models*: Deep neural networks now demonstrate high accuracy for hidden data across media types - countering AI scaled hiding and tracking activities.

8. Conclusion

In conclusion, steganography offers a potent means for covert communication in the present era of prolific digital content creation and exchange. While historical predecessors relied on rudimentary hiding in physical media, contemporary techniques securely embed information within diverse digital covers like images, audio, video and network

protocols. With capacities to conceal entire files within unsuspicious objects using subtle low-level encoding or AI-based generative models, steganography provides a crucial resource for privacy preservation and anonymous communication. However, the double-edged potential for misuse also merits thoughtful regulation. As detection mechanisms rapidly advance in tandem, the coming times promise ever more intriguing progress at this cross-section of information security, machine learning and perceptual hacking. By responsibly harnessing its capabilities while containing risks, steganography is poised to fundamentally transform secure communication spanning disciplines and industries in the twenty-first century's digital expanse.

References

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[2] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge; New York: Cambridge University Press, 2010.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[4] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A Review on Text Steganography Techniques," *Mathematics*, vol. 9, no. 21, p. 2829, Nov. 2021, doi: 10.3390/math9212829.

[5] S. Mishra, V. K. Yadav, M. C. Trivedi, and T. Shrimali, "Audio Steganography Techniques: A Survey," in *Advances in Computer and Computational Sciences*, vol. 554, S. K. Bhatia, K. K. Mishra, S. Tiwari, and V. K. Singh, Eds., in Advances in Intelligent Systems and Computing, vol. 554. , Singapore: Springer Singapore, 2018, pp. 581–589. doi: 10.1007/978-981-10-3773-3_56.

[6] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *J AUDIO SPEECH MUSIC PROC.*, vol. 2012, no. 1, p. 25, Dec. 2012, doi: 10.1186/1687-4722-2012-25.

[7] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, Mar. 2019, doi: 10.1016/j.neucom.2018.09.091.

[8] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 225–229, May 2014, doi: 10.1109/MCOM.2014.6815916.

[9] M. Smolarczyk, K. Szczypiorski, and J. Pawluk, "Multilayer Detection of Network Steganography," *Electronics*, vol. 9, no. 12, p. 2128, Dec. 2020, doi: 10.3390/electronics9122128.

[10] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and classification of image steganography techniques," in *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India: IEEE, Mar. 2014, pp. 870–875. doi: 10.1109/IndiaCom.2014.6828087.

[11] S. Kaur, S. Bansal, and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," *Multimed Tools Appl*, vol. 80, no. 5, pp. 7749–7769, Feb. 2021, doi: 10.1007/s11042-020-09939-7.

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

[13] S. Bansal, R. K. Bansal, and R. Kumar, "A Novel Upgraded Uniform Embedding Technique for JPEG Steganography," in *Intelligent Sustainable Systems*, vol. 333, A. K. Nagar, D. S. Jat, G. Marín-Raventós, and D. K. Mishra, Eds., in Lecture Notes in Networks and Systems, vol. 333, Singapore: Springer Nature Singapore, 2022, pp. 723–730. doi: 10.1007/978-981-16-6309-3_68.

[14] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," *IEEE Trans.Inform.Forensic Secur.*, vol. 10, no. 12, pp. 2669–2680, Dec. 2015, doi: 10.1109/TIFS.2015.2473815.

[15] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. on Info. Security*, vol. 2014, no. 1, p. 1, Dec. 2014, doi: 10.1186/1687-417X-2014-1.

[16] A. K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," *Open Computer Science*, vol. 10, no. 1, pp. 296–342, Oct. 2020, doi: 10.1515/comp-2020-0136.

[17] J. Liu *et al.*, "Recent Advances of Image Steganography With Generative Adversarial Networks," *IEEE Access*, vol. 8, pp. 60575–60597, 2020, doi: 10.1109/ACCESS.2020.2983175.

[18] D. Ye, S. Jiang, and J. Huang, "Heard More Than Heard: An Audio Steganography Method Based on GAN." arXiv, Jul. 10, 2019. Accessed: Nov. 30, 2023. [Online]. Available: http://arxiv.org/abs/1907.04986.

[19] Z. Fu, F. Wang, and X. Cheng, "The secure steganography for hiding images via GAN," *J Image Video Proc.*, vol. 2020, no. 1, p. 46, Dec. 2020, doi: 10.1186/s13640-020-00534-2.

[20] K. Zeng, K. Chen, W. Zhang, Y. Wang, and N. Yu, "Robust Steganography for High Quality Images," *IEEE Trans. Circuits Syst. Video Technol.*, pp. 1–1, 2023, doi: 10.1109/TCSVT.2023.3250750.

[21] S. Rahman *et al.*, "A Comprehensive Study of Digital Image Steganographic Techniques," *IEEE Access*, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.

[22] V. Kumar, S. Laddha, Aniket, and N. Dogra, "Steganography Techniques Using Convolutional Neural Networks," *RCES*, vol. 7, no. 3, pp. 66–73, Sep. 2020, doi: 10.18280/rces.070304.

[23] "evals/evals/elsuite/steganography/readme.md at main · openai/evals · GitHub." Accessed: Nov. 30, 2023. [Online]. Available: https://github.com/openai/evals/blob/main/evals/elsuite/steganography/readme.md