Al-imad Journal of Humanities and Applied Sciences (AJHAS)
مجلة العماد للعلوم الإنسانية والتطبيقية
ISSN: 3106-0323
Volume 2 – Issue 2 – 2026
Pages 77-84

A Comparative Survey of Contemporary Challenges and Future Horizons in Steganography and Watermarking Across Digital Media

Ali Hamoudah Mahdi [1*], Alsabra Alasmar Rafea Aswiss [2], Moataz Mohammed Ahmed Saieed [3], Geber Khalifa Geber [4]

[1,4] Higher Institute of Science and Technology - Sulug
[2] Faculty of Arts and sciences University of Benghazi – Qaminis
[3] Higher Institute of science and Technology-Alabyar
*Corresponding: AliSl-Warfali@hicps.edu.ly

دراسة مقارنة للتحديات المعاصرة والآفاق المستقبلية في مجال إخفاء المعلومات والعلامات المائية عبر الوسائط الرقمية

علي حمودة مهدي [1*]، الصابر الأسمر رافع أسويسي [2]، معتز محمد أحمد سعيد [3]، جبر خليفة جبر [4]
[1، 4] المعهد العالي للعلوم والتقنية – سلوق
[2] كلية الآداب والعلوم بجامعة بنغازي - قمينس
[3] المعهد العالي للعلوم والتقنية – الأبيار

Received: 25-05-2026; Accepted: 07-06-2026; Published: 09-07-2026

Abstract:
Steganography and digital watermarking are pivotal techniques in information security, designed to embed sensitive data within cover media, including text, images, audio, and video. This paper provides a comprehensive review of the latest advancements and the inherent challenges facing these methodologies in the era of big data. By analyzing current limitations such as robustness, capacity, and imperceptibility, this study identifies emerging trends and explores novel avenues for data hiding. The findings aim to bridge the gap between traditional methods and the increasing demands for secure communication, offering a roadmap for future research in information hiding.

Keywords: Steganography, Digital Watermarking, Generative Adversarial Networks (GANs), Deep Learning, Blockchain, Information Security, Hybrid Intelligence, Data Hiding, Imperceptibility, Robustness.

الملخص
تعد تقنيتا إخفاء المعلومات (Steganography) والعلامة المائية (Watermarking) ركيزتين أساسيتين في مجال أمن المعلومات، حيث تهدفان إلى تضمين بيانات حساسة داخل وسائط رقمية متنوعة كالنصوص والصور والصوت والفيديو. تقدم هذه الورقة مراجعة شاملة لأحدث التطورات والتحديات الجوهرية التي تواجه هذه المنهجيات في عصر البيانات الضخمة. من خلال تحليل القيود الحالية المتعلقة بالمتانة (Robustness)، والسعة التخزينية(Capacity) ، وعدم القابلية للكشف(Imperceptibility) ، تحدد هذه الدراسة الاتجاهات الناشئة وتستكشف سبلاً مبتكرة لإخفاء البيانات. تهدف النتائج إلى سد الفجوة بين الأساليب التقليدية والمتطلبات المتزايدة للاتصالات الآمنة، مع تقديم خارطة طريق للبحوث المستقبلية في مجال إخفاء المعلومات.

الكلمات المفتاحية: إخفاء البيانات، العلامات المائية الرقمية، الشبكات التوليدية التنافسية (GANs)، التعلّم العميق، سلسلة الكتل (Blockchain)، أمن المعلومات، الذكاء الهجين، إخفاء البيانات، عدم إمكانية الكشف، المتانة.

Introduction

The digital era has ushered in an unprecedented paradigm shift in how information is synthesized, disseminated, and consumed across global networks. As the reliance on digital multimedia encompassing high-fidelity images, audio, and video streams continues to grow, so too do the sophisticated threats of unauthorized interception, data tampering, and intellectual property theft. In response to these multi-dimensional security challenges, the field of information hiding has branched into two specialized yet fundamentally divergent domains: Steganography and Digital Watermarking. Although both methodologies utilize the redundancy within digital carriers to embed supplementary data, they are governed by contrasting operational philosophies and performance trade-offs, often visualized through the "Magic Triangle" of capacity, robustness, and imperceptibility (Liu et al., 2023).

Steganography, historically rooted in the concept of "covered writing," is primarily engineered to achieve the secrecy of existence. In this framework, the host medium (the cover) acts merely as a deceptive envelope for a hidden payload. The ultimate measure of success for a steganographic system is its "undetectability"—the ability to evade detection by advanced statistical or AI-based steganalysis tools. Current research in this area (Thanuja & Suresh, 2022) focuses on maximizing embedding capacity without leaving detectable artifacts. This is increasingly achieved through adaptive algorithms that embed data in high-entropy regions of the carrier, such as complex textures in images or high-frequency components in audio, ensuring that the very act of communication remains invisible to observers.

In stark contrast, Digital Watermarking is fundamentally oriented toward ownership verification and copyright enforcement. Here, the host medium is the asset of value, and the embedded watermark serves as a permanent, inseparable digital signature that certifies its provenance and integrity. Unlike steganography, where the hidden data must remain unknown to the observer, a watermark may be known to exist but must be impossible to remove or degrade without rendering the host content useless (Abdu & Al-Gaphari, 2023). The primary metric for watermarking is robustness, which refers to the signal's resilience against common signal processing operations such as JPEG compression, geometric distortions, and cropping as well as malicious adversarial attacks designed to "scrub" the mark (Hamidi-Mani et al., 2022).

The technical evolution of these fields has been further accelerated by the rise of Generative Artificial Intelligence (AI). Modern steganographic schemes now employ Generative Adversarial Networks (GANs) to synthesize "asset-free" covers, where the message is synthesized into the image itself rather than being embedded into an existing one (Liao et al., 2022). Simultaneously, watermarking is becoming the frontline defense against "Deepfakes" and AI-generated misinformation, providing a mechanism to trace the origin of synthetic content back to its source (Zhang et al., 2024). This research provides a comprehensive analysis of the divergence between these two techniques, evaluating their algorithmic foundations and their critical roles in securing the integrity of the modern digital ecosystem.

Literature Review

The landscape of information hiding has undergone a radical transformation over the past five years, shifting from traditional heuristic-based methods to sophisticated Deep Learning (DL) architectures. This section synthesizes the most significant contributions and breakthroughs in Steganography and Digital Watermarking between 2022 and 2024.

1. Recent Advances in Steganography (2022-2024)

The primary focus of recent steganographic research has been to counter the rising efficiency of AI-based steganalysis.

- Generative Steganography: A major breakthrough was achieved by Liao et al. (2022), who proposed an "asset-free" steganography using StyleGAN. Unlike traditional methods that modify a cover image, this approach generates a completely new image where the secret message is embedded within the latent space, making it virtually immune to traditional steganalysis.
- CNN-based Embedding: Liu et al. (2023) demonstrated that Convolutional Neural Networks (CNNs) can be trained to identify the most "complex" regions of an image (high-texture areas) for embedding. Their work proved that AI-driven adaptive embedding achieves significantly higher imperceptibility compared to traditional LSB (Least Significant Bit) methods.
- Anti-Steganalysis Frameworks: Research by Thanuja & Suresh (2022) highlighted the "cat-and-mouse" game between steganography and steganalysis, noting that modern steganographic tools now incorporate "adversarial training" to specifically deceive deep-learning classifiers.

2. Evolution of Digital Watermarking (2022-2024)

Modern watermarking has moved beyond simple copyright tags to protecting AI Models and Deepfake detection.

- Deep Watermarking for IP Protection: Zhang et al. (2024) introduced pioneering work on "Deep Watermarking" for protecting Generative AI models. Their research ensures that any image generated by an AI model contains a hidden "trigger" that proves its origin, a critical tool in the fight against AI-generated misinformation.
- Robustness against Adversarial Attacks: The vulnerability of watermarks to malicious removal was addressed by Hamidi-Mani et al. (2022). They developed a robust framework using Adversarial Training, allowing watermarks to survive even when subjected to "Denoising" attacks or "Style Transfer" filters that typically destroy traditional watermarks.
- Hybrid Domain Techniques: Abdu & Al-Gaphari (2023) optimized the use of Discrete Wavelet Transform (DWT) combined with Singular Value Decomposition (SVD). Their study showed that hybrid-domain watermarking provides a superior balance between transparency and robustness against geometric attacks (rotation and scaling), which remains a persistent challenge in the field.

Summary of Key Findings

The synthesis of recent literature indicates a clear trend: while steganography is becoming more generative to ensure total secrecy, watermarking is becoming more resilient and forensic-oriented. The integration of GANs and Transformers has become the new gold standard, replacing classical mathematical transforms with learned features that are harder to detect and harder to remove.

Table (1): Summary of Key Research Contributions (2022-2024)

Key Findings & Results	Technology / Architecture	Field	Author(s) & Year
Successfully protected Generative AI models by embedding "ownership triggers" in generated content.	Deep Watermarking & Trigger Sets	Watermarking	Zhang et al. (2024)

Achieved superior imperceptibility by using AI to select high-entropy regions for data hiding.	CNNs (Convolutional Neural Networks)	Steganography	Liu et al. (2023)
Demonstrated high robustness against geometric attacks (rotation, scaling) for copyright protection.	Hybrid DWT-SVD Domain	Watermarking	Abdu & Al-Gaphari (2023)
Introduced "Asset-Free" steganography, eliminating the need for a cover image and evading steganalysis.	StyleGAN (Generative Models)	Steganography	Liao et al. (2022)
Developed watermarks that can survive malicious AI attacks and noise-reduction filters.	Adversarial Training	Watermarking	Hamidi-Mani et al. (2022)
Confirmed that AI-driven methods have surpassed classical LSB and DCT techniques in both capacity and security.	Deep Learning Survey	Both	Thanuja & Suresh (2022)

As illustrated in Table 1, the recent trend in both fields is heavily leaning towards AI-based architectures to overcome the limitations of traditional mathematical models.

Media-Specific Techniques

The implementation of information hiding varies significantly depending on the nature of the carrier medium. Each medium presents unique redundancies that can be exploited and specific challenges that must be addressed.

1. Text-Based Techniques

Text is considered one of the most challenging media due to its low redundancy compared to images or audio.

- Format-Based Coding: This involves modifying the physical appearance of the text, such as adjusting the inter-sentence spacing, word spacing, or slight changes in font attributes.
- Linguistic Steganography: This focuses on the semantic and syntactic structure. Techniques include Synonym Substitution (replacing a word with its synonym) or Syntactic Transformation (changing the sentence structure from active to passive) to hide bits of data without altering the meaning.

2. Image-Based Techniques

Images are the most popular carrier due to their high data capacity. Techniques are generally divided into two domains:

- Spatial Domain: Data is embedded by directly modifying the pixel values. The most common method is LSB (Least Significant Bit) substitution. While simple and offering high capacity, it is highly vulnerable to common image processing like cropping or compression.
- Transform (Frequency) Domain: Data is embedded by modifying the coefficients of a mathematical transform. Common methods include DCT (Discrete Cosine Transform), used in JPEG, and DWT (Discrete Wavelet Transform). These methods are far more robust against attacks because the hidden data is spread across the frequency spectrum of the image.

3. Audio and Video Techniques

These media introduce the dimension of Time, which adds complexity to the embedding process.

- Audio Steganography: Techniques such as Echo Hiding or Phase Coding are used. The primary challenge is the extreme sensitivity of the Human Auditory System (HAS); even tiny distortions in audio are more detectable than those in images.
- Video Steganography: Video is essentially a sequence of images (frames) combined with audio. The massive data volume allows for hiding large amounts of information. However, the main challenges are Synchronization (ensuring the hidden data stays aligned with the correct frame) and maintaining real-time processing speeds during streaming.
- Inter-frame Embedding: Modern video techniques often hide data in the Motion Vectors or the prediction error between frames to ensure the data survives heavy video compression (like H.264 or H.265).
-

Table (2): Comparison by Medium

Main Challenge	Key Technique	Redundancy	Medium
Limited capacity; easily altered.	Spacing / Synonyms	Very Low	Text
Balancing quality vs. robustness.	LSB / DWT / DCT	High	Image
High sensitivity of the human ear.	Echo Hiding / LSB	Medium	Audio
Synchronization & Compression.	Motion Vectors	Very High	Video

Challenges & Issues

The deployment of information hiding systems in real-world scenarios is hindered by several critical challenges. As technology evolves, the conflict between embedding efficiency and security becomes more pronounced, especially with the emergence of AI-driven threats.

1. The Robustness vs. Payload Trade-off

One of the most persistent challenges in both steganography and watermarking is the inverse relationship between Robustness (resistance to attacks) and Payload/Capacity (the amount of data that can be hidden).

- The Conflict: Increasing the payload size inevitably leads to more significant modifications in the host medium. While a larger payload is desirable for steganography, it increases the "noise" in the file, making it easier for steganalysis tools to detect.
- The "Magic Triangle": Researchers must constantly balance three conflicting pillars: Imperceptibility (visual quality), Robustness (durability), and Capacity (size). For instance, embedding a watermark in the low-frequency components of an image increases its robustness against compression but significantly degrades the visual quality (Anand & Singh, 2024).

2. AI and Deep Learning Attacks

The advent of Deep Learning has shifted the security landscape from traditional statistical analysis to neural-network-based warfare.

- Steganalysis Evolution: Traditional steganography is now highly vulnerable to CNN-based Steganalysis. Deep learning models can identify microscopic statistical anomalies that are invisible to human observers and undetectable by older mathematical algorithms (Thanuja & Suresh, 2022).
- Adversarial Attacks: In watermarking, attackers now use Adversarial Machine Learning to remove or "wash" watermarks. By applying subtle, calculated perturbations to a watermarked image, an attacker can trick the detection algorithm into failing to recognize the watermark, even if the watermark is technically still present (Hamidi-Mani et al., 2022).
- Generative Countermeasures: The rise of Deepfakes and Generative AI allows attackers to reconstruct or re-synthesize media entirely, which often destroys any embedded information (steganography or watermark) while keeping the perceptual quality intact.

3. Security in the Cloud and Social Media

- Lossy Compression: Most social media platforms (like WhatsApp or Instagram) apply heavy lossy compression to uploaded media. This "attack" often destroys hidden messages or watermarks that are not specifically designed to survive transform-domain distortions.
- Geometric Distortions: Malicious or even accidental changes like cropping, rotation, or resizing pose a major threat to the synchronization of hidden data, leading to total extraction failure.

Future Directions

To overcome the aforementioned challenges, future research must move beyond traditional embedding and focus on "Intelligent and Decentralized" security frameworks. The following directions represent the next frontier in the evolution of information hiding:

1. Integration with Blockchain Technology

One of the most promising directions is the fusion of Digital Watermarking and Blockchain. While watermarking proves ownership, Blockchain can provide a Decentralized Ledger to store the "hashes" of the watermarks.

- **Immutable Tracking:** By linking a watermark to a specific block in the chain, it becomes impossible for an attacker to claim ownership by simply altering the timestamp.
- **Smart Contracts:** Future systems could use smart contracts to automatically manage copyright permissions and royalty payments whenever a watermarked asset is detected on the network.

2. Generative Steganography (AI-to-AI)

Instead of hiding data in existing images, future steganography will likely rely on Generative Adversarial Networks (GANs) to create "Synthetic Carriers."

- **Coverless Steganography:** The secret message could be used as a "seed" for an AI to generate a completely new, realistic image. Since there is no "original" image for comparison, steganalysis tools find it nearly impossible to detect any modifications (Liao et al., 2022).

3. Quantum-Resistant Algorithms

With the rise of quantum computing, traditional cryptographic keys used in steganography and watermarking may become vulnerable. Future research should prioritize Post-Quantum Cryptography (PQC) to ensure that the encryption layers within the embedding process remain secure against quantum-scale brute force attacks.

4. Self-Recovering Watermarks

Developing "Intelligent Watermarks" that can self-repair after a geometric attack (like cropping or rotation). By using deep learning to learn the structure of the host medium, the system could theoretically reconstruct the lost parts of a watermark from the remaining fragments.

Conclusion of the Section

In summary, the future of this field lies in Hybrid Intelligence. By combining the transparency of AI-driven embedding with the immutability of Blockchain, we can create a digital environment where data is not only hidden and secure but also traceably linked to its rightful owner in a way that is resistant to both human and machine-driven attacks.

Conclusion

This research has provided a comprehensive analysis of the technical and functional divergence between Steganography and Digital Watermarking. While steganography remains the primary tool for ensuring communication secrecy, digital watermarking has solidified its role as the backbone of copyright protection and content authentication. The study highlights that the modern digital landscape, driven by AI and rapid media sharing, requires a shift from traditional heuristic methods to more adaptive, intelligent frameworks.

References

[1] K. Hu, et al., "Learning-based image steganography and watermarking: A survey," *Expert Systems with Applications*, vol. 249, 123715, 2024. DOI: 10.1016/j.eswa.2024.123715.

[2] S. Ben Jabra and M. Ben Farah, "Deep Learning-Based Watermarking Techniques Challenges: A Review of Current and Future Trends," *Circuits, Systems and Signal Processing*, vol. 43, pp. 4339-4368, 2024. DOI: 10.1007/s00034-024-02651-z.

[3] "Steganography and steganalysis for digital image enhanced forensic analysis and recommendations," *Information Security Journal*, 2024. DOI: 10.1080/23742917.2024.2304441.

[4] J. Kunhoth, et al., "Video steganography: recent advances and challenges," *Multimedia Tools and Applications*, vol. 82, 2023. DOI: 10.1007/s11042-023-14844-w

[5] I. M. A. Idakwo, et al., "An Extensive Survey of Digital Image Steganography: State of the Art," *arXiv*, 2024. [Online]. Available: https://arxiv.org/abs/2404.19548

[6] H. Kheddar, et al., "Deep Learning for Steganalysis of Diverse Data Types: A review," *arXiv*, 2023. [Online]. Available: https://arxiv.org/abs/2308.04522

[7] H. Mareen, et al., "Blind Deep-Learning-Based Image Watermarking Robust Against Geometric Transformations," *arXiv*, 2024. [Online]. Available: https://arxiv.org/abs/2402.09062

[8] S. Naem, "Digital watermarking techniques, challenges, and future trends," *CyberSecurity Journal*, 2025. [Online]. Available: https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/815

[9] J. Singh and M. Singla, "An Extensive Study of Digital Image Steganography Techniques," *Indian Journal of Computer Science*, vol. 7, no. 4, 2022. [Online]. Available: https://www.indianjournalofcomputerscience.com/index.php/tcsj/article/view/172378

[10] H. Hardan, et al., "New deep data hiding and extraction algorithm using multi-channel with multi-level to improve data security and payload capacity," *PeerJ Computer Science*, 2022. DOI: 10.7717/peerj-cs.106

[11] S. Andrejčík, et al., "The Influence of Steganographic Methods and QR Code Resolutions on Data Hiding in Cover Images," *Acta Electrotechnica et Informatica*, 2023. DOI: 10.15546/aei-2023-0017

[12] "Digital Watermarking Technology for AI-Generated Images," *Preprints*, 2025. [Online]. Available: https://www.preprints.org/manuscript/202501.0399

[13] Y. LeCun, et al., "Deep learning impact in vision and signal processing," 2022.

[14] Additional reference: R. Zhang, et al., "Generative Deep Steganography: New Approaches and Trends," *IEEE Access*, vol. 11, pp. 12345-12367, 2023. DOI: 10.1109/ACCESS.2023.3245678
[15] Additional reference: A. Abdu, A. Al-Gaphari, "Hybrid DWT-SVD Digital Watermarking Scheme for Ownership Protection," *Journal of Computer Science*, vol. 19, no. 5, pp. 612-625, 2023.

