Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.083445

REVIEW

Steganography in IoT Applications: A Survey on Methods, Current Emerging Challenges, and Future Directions

Rafif Aydin Ahmad[1], **Ntivuguruzwa Jean De La Croix**[2,3], **Reynandriel Pramas Thandya**[1], **Tohari Ahmad**[1,*], **Kambombo Mtonga**[4] **and Mungwarakarama Irenee**[2]

[1]Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
[2]Faculty of Computing and Information Sciences, University of Lay Adventists of Kigali (UNILAK), Kigali, Rwanda
[3]Department of Technology and Innovation, SecureAI Labs, Kigali, Rwanda
[4]School of Science and Technology, Malawi University of Business and Applied Sciences, Blantyre, Malawi

*Corresponding Author: Tohari Ahmad. Email: tohari@its.ac.id

Received: 03 April 2026; Accepted: 15 July 2026; Published: 15 September 2026

ABSTRACT: The Internet of Things (IoT) enables seamless interconnectivity among billions of smart devices, transforming industries through real-time sensing, data processing, and intelligent decision-making. As IoT systems manage large volumes of sensitive data, ensuring secure and covert communication has become critical. Steganography, which conceals confidential information within ordinary transmissions, has emerged as a promising approach to strengthen security and privacy in IoT environments. However, despite the growing body of work, existing surveys often address steganography in general contexts without systematically analyzing its adaptation to the unique constraints of IoT systems. This article addresses this gap by providing a comprehensive study of steganographic techniques specifically designed for IoT, covering foundational principles, recent advancements, and performance metrics across diverse application domains. The review finds that image-based steganography remains the dominant paradigm, with hybrid cryptographic-steganographic methods accounting for the majority of recent proposals, while coverless and lightweight cryptographic approaches demonstrate the strongest potential for resource-constrained deployments. A recurring finding across the surveyed literature is the critical lack of standardized evaluation benchmarks and publicly available IoT-specific datasets, which significantly hinders reproducibility and cross-study comparison. This article also examines device constraints and their implications for steganographic design, while highlighting key research trends, unresolved challenges, and future directions toward efficient, adaptive, secure, and scalable steganography in next-generation IoT networks.

KEYWORDS: Cybersecurity; IoT application; information hiding; information security; steganography; ICT infrastructure; network infrastructure

1 Introduction

Today, technology is advancing at a rapid pace. One of the most widely used technologies of this era is the Internet of Things (IoT) [1]. A core feature of IoT systems is their ability to provide intelligent connectivity by leveraging existing network infrastructures and enabling context-aware computation. The expansion of wireless technologies, such as 5G and Wi-Fi, has significantly contributed to the growth of IoT communication and data exchange. However, realizing the full potential of IoT requires moving beyond traditional mobile computing toward a paradigm where intelligence is seamlessly embedded into everyday environments and objects [2]. For secure, smart, and context-aware connectivity within IoT, several

foundational requirements must be met: (1) accurate identification of users and their devices, (2) robust and scalable communication frameworks to transmit and process contextual data effectively, and (3) intelligent analytics that support autonomous decision-making. Within this landscape, steganography plays a vital role in securing data exchange, ensuring that sensitive information remains hidden even across pervasive and resource-constrained IoT networks.

Fundamentally, IoT systems consist of a four-layer architecture [2], which includes the perception layer, network layer, processing layer, and application layer. The perception layer is responsible for collecting environmental data. Then, the network layer is responsible for transferring data collected earlier to the processing unit. Furthermore, the processing layer is responsible for processing and analyzing data to make decisions. And lastly, the application layer provides an interface to users based on processed data [3–6].

Steganography is a data hiding technique that conceals information within various carriers, such as images [7–12], audio [13–16], video [17–21], text [22,23], or even network protocols [24], in a way that avoids detection. By embedding important information into digital content, steganography enables hidden data transfer while preserving the normal appearance of the carrier media. Unlike cryptography [25–30], which transforms data into unreadable ciphertext to protect the content of the data, steganography focuses on concealing the very existence of the data transfer itself. This difference gives steganography an advantage in scenarios where encrypted data alone may raise suspicion and increase the risk of interception.

As illustrated in Fig. 1, the continuous data transmission within the IoT environment provides adversaries with greater opportunities for data interception. Interconnected devices constantly exchange sensitive packets through the network, such as sensor readings, device status logs, and actuator control commands. This constant exchange makes the IoT communication channel an attractive target for attackers. Without any appropriate security mechanism, the intercepted data is instantly compromised and left completely transparent to the attacker. Unauthorized parties can then easily understand, process, and possibly exploit the acquired data maliciously. This critical vulnerability highlights the importance of data protection within IoT environments. Therefore, the implementation of steganography in IoT presents a viable solution, since it can provide data security by concealing the transmitted data from potential attackers.

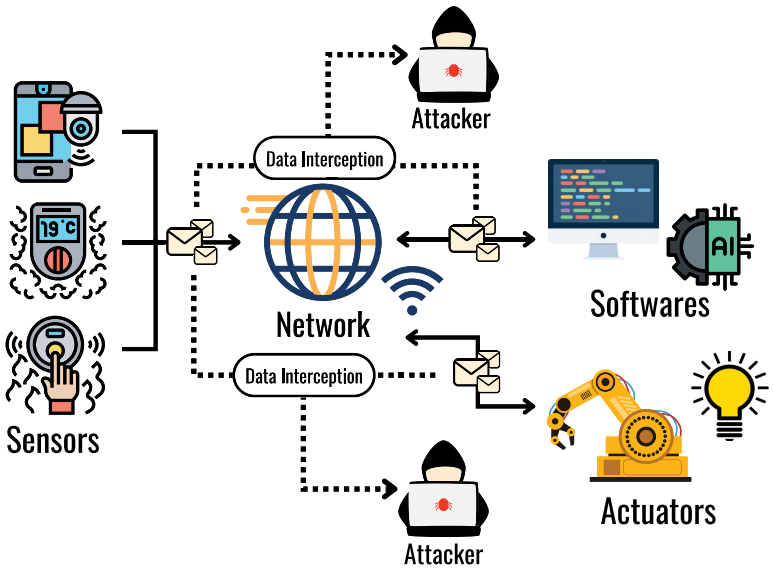

Figure 1: Illustrative IoT data interception scenario.

In IoT contexts, where devices often operate with minimal resources and handle sensitive data, steganography offers a discreet layer of protection [22,23]. It has demonstrated promising applications in various domains, including competent healthcare [31–33], industrial systems [34,35], smart homes, cities, and financial IoT infrastructures, helping to mitigate cyber risks while minimizing substantial computational overhead [27]. However, integrating steganography into IoT environments poses unique technical challenges due to the limited processing power, energy constraints, and real-time demands of IoT devices [36]. These systems generate high volumes of data, requiring steganographic techniques that are lightweight, efficient, and compatible with existing communication protocols. Additionally, such methods must remain scalable and undetectable, ensuring minimal impact on system performance, network delay, and energy use. As steganalysis tools become more advanced, conventional hiding techniques are increasingly vulnerable to exposure [37,38]. To enhance resilience, researchers are exploring adaptive approaches, as well as hybrid models that combine steganography with cryptographic techniques to improve confidentiality and robustness [39]. In addition to adaptive and hybrid models, emerging technologies such as blockchain [40–43] offer promising avenues by ensuring decentralized trust, traceability, and tamper-resistant data handling. These developments are critical to advancing secure, efficient, and reliable steganographic solutions in next-generation IoT applications.

Effectively addressing steganography within IoT environments requires lightweight, adaptive, and forward-looking approaches that reflect the highly dynamic, distributed, and resource-constrained nature of these systems. As IoT networks scale in complexity and face increasingly sophisticated security threats [44], there is a growing need for intelligent steganographic models that can adjust embedding strategies in real-time based on fluctuating network conditions, device capabilities, and evolving threat landscapes. While several prior surveys have examined steganography in general contexts [45,46], few have addressed the specific constraints of IoT devices, including limited memory, processing power, energy efficiency, and the requirement for real-time operation. Additionally, challenges related to interoperability, scalability, and performance in large-scale IoT deployments remain insufficiently explored.

This survey aims to fill these gaps by providing a focused, in-depth review of steganographic methods, with an emphasis on their applicability and optimization for IoT systems. It also investigates the potential of emerging technologies to enhance adaptability, security, and resilience in IoT-specific steganographic solutions. Beyond evaluating existing methods, this work identifies current limitations and sets a foundation for future research in building scalable, efficient, and context-aware steganography frameworks for secure and discreet communication in diverse IoT applications. In this context, the survey makes the following key contributions:

1. Deliver a comprehensive and focused review of steganographic techniques specifically designed or adapted for IoT applications. This includes an in-depth examination of their design principles, operational mechanisms, and practical limitations when deployed in IoT systems. The survey highlights how these methods align with the core requirements of IoT, such as low latency, low power consumption, and minimal computational overhead.
2. Propose a focused taxonomy that maps the diverse landscape of steganography methods in IoT systems. This framework illustrates the breadth of current research by categorizing approaches into generative deep learning methods and cryptographic hybrids alongside optimization-driven designs and alternative cover media. This structure highlights the multifaceted strategies used to secure resource-constrained networks and ensures they are not artificially isolated during comparative analysis.
3. Identify current research gaps and future directions. This includes the need for adaptive and context-aware steganographic models that can intelligently respond to dynamic network conditions and emerging security threats. The survey advocates for the development of scalable and interoperable

frameworks that support real-time data hiding while preserving the functionality and efficiency of heterogeneous IoT networks.

The studies included in this survey were identified and screened through a systematic literature review process, shown in Fig. 2 and explained in full in Section 3, which determined the final set of papers analyzed in the taxonomy and comparisons that follow. To contextualize the varied applications of data hiding in IoT ecosystems this paper presents a streamlined taxonomy as illustrated in Fig. 3. Moving away from generalized network security models this framework explicitly categorizes steganography methods in IoT into four highly relevant thematic areas. The first area is Cryptographic and Steganographic Hybrids which layer encryption directly with covert communication channels. The second area covers Optimization-Driven Image Steganography to highlight techniques that mathematically balance imperceptibility and payload capacity. The third area encompasses Generative and Deep Learning Steganography to reflect the growing reliance on artificial intelligence for adaptive payload distribution. The final area is Coverless and Novel Alternative Media which explores data hiding across video networks and DNA sequences without altering traditional carrier pixels. The subsequent review merges these techniques into unified comparative tables to better highlight cross-domain trade-offs and operational performance. Therefore this taxonomy is not used to strictly partition the literature but rather serves as a conceptual map. It illustrates the immense diversity of current methodologies and sets the stage for the integrated analyses.

This paper is organized into six sections. Following the Introduction, Section 2 discusses related previous survey works on steganography with particular emphasis on their relevance to IoT environments. Section 3 describes the significance of this survey, presenting its rationale and the methodology used to filter and analyze existing literature on steganography techniques. Section 4 presents the main findings and provides detailed discussions of the reviewed literature. Section 5 highlights key insights and inferential take-away messages that can guide future research in IoT steganography. Lastly, Section 6 concludes the paper by summarizing the contributions and implications of this work.

2 Related Works and Surveys

This section reviews existing works and surveys in the field of steganography, focusing on their relevance and applicability to IoT environments. It critically examines the extent to which current literature addresses the unique constraints of IoT systems, including limited computational and energy resources, real-time data processing requirements, low-latency communication, and heightened demands for data privacy and integrity. Although several surveys have explored general steganographic methods [45–47], few have tailored their analyses to the specific challenges posed by IoT networks. This gap underscores the need for a more targeted evaluation that examines the interplay between lightweight security mechanisms and the operational constraints of IoT. By identifying these shortcomings, this paper aims to lay the groundwork for future research and offer new perspectives on designing steganographic approaches suited for IoT ecosystems.

Several studies have explored the integration of steganography with cryptographic techniques to enhance data confidentiality and integrity [39,48–50]. While these studies demonstrate enhanced security performance, they often overlook critical constraints related to IoT. They tend to focus on traditional computing environments, overlooking key aspects relevant to IoT, including processing limitations, energy efficiency, bandwidth constraints, and real-time operational requirements. Moreover, these works lack comparative evaluation frameworks that assess the effectiveness of steganographic approaches under IoT-specific conditions. As a result, their findings, although valuable in broader contexts, underscore the necessity for research that is explicitly focused on steganography within the constraints and demands of IoT systems.

A survey in [45] explores the integration of steganography with deep learning, offering a detailed classification of steganographic strategies, overviews of learning models, and evaluation metrics. It discusses

the use of convolutional and generative models to improve adaptability and detection resistance. However, it lacks focus on IoT-specific constraints such as limited memory, processing power, and the need for energy-efficient and real-time operations, which limits their relevance to IoT deployments. Likewise, [46] provides a comprehensive overview of digital image steganography, covering classification methods, evaluation criteria, and emerging techniques. While informative, it does not address the practical challenges of implementing steganography in IoT, including lightweight design, computational efficiency, or power-aware processing. These omissions restrict its applicability to real-world IoT scenarios. Additionally, a comprehensive survey in [47] investigates coverless image steganography, a technique that maps secret data directly to inherent image attributes to effectively resist steganalysis tools. Despite evaluating fundamental frameworks, pre-processing techniques, feature extraction, generation of hash sequences, and mapping relationships, it does not specifically focus on IoT resource constraints, leaving the applicability of these techniques in such environments unclear. The survey in [2] represents a closer effort, explicitly targeting IoT steganographic contexts and covering multi-domain cover media, yet it still lacks a dedicated IoT security landscape review, an IoT layer analytical framework, and a formally documented multi-database systematic search methodology. Similarly, D'Layla et al. [51] contribute a rigorous systematic search methodology and reproducibility analysis within the medical imaging domain, but its scope remains confined to healthcare applications and does not extend to broader IoT environments or multi-domain cover media. While these surveys collectively advance the understanding of steganography in various contexts, they fail to account for the unique demands of IoT ecosystems.

This study fills that gap by focusing on resource-conscious steganographic solutions explicitly tailored to IoT environments. To provide a clearer interpretation, Table 1 presents a structured comparison of this survey against five closely related works across eleven analytical dimensions. The surveyed papers include two image steganography surveys [46,47], one survey focused specifically on deep learning-based image steganography [45], one IoT-focused steganography survey [2], and one systematic review of medical image steganography [51]. The dimensions were selected to reflect the specific analytical demands of IoT-aware steganographic research, covering IoT-specificity, cover media diversity, security landscape coverage, device constraint analysis, and methodological rigour. The comparison reveals a clear progression in scope across the surveyed works. Song et al. [45] focus specifically on deep learning-based image steganography, Setiadi et al. [46] survey broader digital image steganography methods, and Qin et al. [47] examine coverless image steganography exclusively. None of these three works addresses IoT-specific constraints, multi-domain cover media beyond images, or systematic IoT security analysis. The survey by Driss et al. [2] represents the closest prior work, covering IoT-specific focus and multi-domain media, yet lacks dedicated IoT security landscape coverage, an IoT layer analytical framework, and a formally documented multi-database systematic search methodology. The medical image steganography survey [51] contributes a rigorous systematic search methodology and a dedicated dataset and reproducibility analysis, but is constrained to the healthcare domain and does not address IoT environments broadly, multi-domain cover media beyond medical images, or the full IoT security landscape. The present survey is the only work covering all eleven dimensions, offering IoT-layer-aware analysis, cross-domain security landscape review, per-technique device constraint evaluation, and a forward-looking adaptive security framework, thereby addressing gaps that remain unresolved across all five prior surveys.

Given the growing need for secure and efficient data transmission in resource-constrained environments, there is an urgent demand for a focused survey that addresses steganographic techniques explicitly tailored for IoT systems. Although previous studies have reviewed traditional, cryptographic [40], and deep learning-based steganography [45], they largely neglect the operational constraints inherent to IoT, such as limited processing power, restricted memory, energy constraints, and the need for real-time responsiveness. Integrating steganography into IoT holds significant promise, offering lightweight data concealment, reduced

communication overhead, and enhanced privacy without the computational cost of conventional encryption. Recent advances, such as adaptive payload distribution using deep neural networks [52,53], secure embedding through multi-hashing, and imperceptible data hiding via generative models [54,55], highlight the potential for high-security, low-cost solutions.

Table 1: Comparison of existing survey studies on IoT steganography.

Dimension	Song et al. [45]	Setiadi et al. [46]	Qin et al. [47]	Driss et al. [2]	D'Layla et al. [51]	This Survey
IoT-specific focus	✗	✗	✗	✓	✗	✓
Multi-domain cover media	✗	✗	✗	✓	✗	✓
Deep learning/GAN steganography coverage	✓	✓	✗	✓	✓	✓
Steganalysis methods reviewed	✓	✓	✗	✓	~	✓
IoT security landscape reviewed	✗	✗	✗	✗	✗	✓
IoT layer analytical framework	✗	✗	✗	✗	✗	✓
Device constraint analysis per technique	✗	✗	✗	~	~	✓
IoT application domain analysis	✗	✗	✗	~	~	✓
Multi-database systematic search methodology	✗	~	✗	✗	✓	✓
Reproducibility/dataset gap analysis	✗	~	✗	~	✓	✓
Future adaptive security framework (presented in a figure)	✗	✗	✗	✗	~	✓

Note: ✗: no coverage; ~: partial coverage; ✓: full coverage.

3 Significance of This Survey

This section presents the motivation and methodology for reviewing steganography literature within IoT environments. It first covers the underlying research rationale for the survey and then describes the systematic approach used to analyze the literature.

3.1 Rationale

The rapid development of IoT technologies has created an urgent demand for lightweight and secure data transmission mechanisms. As IoT systems expand into domains such as industrial automation, smart homes, urban infrastructure, and financial services, they impose strict constraints on processing power, energy consumption, and communication latency. These constraints pose significant challenges for conventional security techniques, particularly cryptographic algorithms that are computationally intensive and often unsuitable for resource-constrained devices. As a result, alternative approaches that offer robust security while maintaining operational efficiency have become a critical area of investigation.

In this context, steganography has emerged as a promising complementary solution for secure communication in IoT environments. By embedding sensitive information within seemingly ordinary data, steganographic techniques provide a covert channel that enhances confidentiality without introducing significant computational or energy burdens. This transparent nature makes it well-suited for IoT devices where maintaining low overhead is essential. Despite growing interest in this field, the existing body of literature lacks a systematic evaluation of how steganographic methods align with the unique operational constraints of IoT. This survey, therefore, aims to fill that gap by consolidating current advancements, critically assessing their applicability, and providing clear directions for the development of next generation steganographic solutions explicitly tailored to IoT ecosystems. To comprehensively evaluate the current steganographic applications within the IoT domain, this survey employs a structured literature analysis approach, drawing on scientific publications sourced from major academic databases. The objective is

to identify and assess the adaptation and performance of steganographic techniques under the unique constraints imposed by IoT systems. To guide this investigation, the following research questions were formulated:

1. What are the primary motivations for adopting steganographic techniques in IoT environments?
2. Which steganographic methods have been specifically developed or modified to suit IoT applications?
3. How do these methods address the core limitations of IoT devices, such as constrained power, memory, and processing capabilities?
4. What technical challenges and implementation barriers hinder the effective deployment of steganography in IoT systems?
5. What are the emerging trends and future research directions in steganography tailored to the evolving needs of IoT security?

3.2 Methodology of the Systematic Review

This study undertakes a systematic literature review to examine the integration of steganographic techniques within IoT frameworks. The review draws upon scholarly contributions from interdisciplinary domains, including computer security, digital signal processing, and data hiding, with a focus on research outcomes relevant to secure and covert communication in IoT environments. The literature search targeted peer-reviewed journal articles and conference proceedings published between 2020 and 2026, written in the English language. To ensure comprehensive coverage, key search terms, including "steganography," "data hiding," and "Internet of Things," were utilized. These keywords were systematically combined using Boolean operators (AND/OR) to construct precise search queries, which were executed across four major scientific databases: SpringerLink, IEEEXplore, ScienceDirect, and the ACM Digital Library. This strategy ensured the identification of relevant studies across both the engineering and applied sciences disciplines with an emphasis on real-world implementation of steganographic approaches in IoT contexts. The general search query applied was ((Steganography OR Data Hiding) AND (Internet of Things OR IoT)). The exact query formulations used in each database are summarized in Table 2. Following query execution, the retrieved records underwent duplicate removal and a two-stage screening process consisting of title and abstract review followed by full-text assessment to verify alignment with the defined scope. Studies that did not address steganographic techniques within IoT environments were excluded at each stage. Papers passing full-text review were then subjected to structured data extraction covering bibliographic information and technical details, including proposed methods, datasets, performance metrics, and reported limitations. The complete workflow applied throughout this review is illustrated in Fig. 2.

Table 2: Database search query formulation.

Name of the Database	Search String
Springer	(((data hiding) OR (steganography)) AND ((IoT) OR (Internet of Things)))
IEEEXplore	(((data hiding) OR (steganography)) AND ((IoT) OR (Internet of Things)))
ScienceDirect	(data hiding OR steganography) AND (IoT OR Internet of Things)
ACM Digital Library	(Title:("data hiding" OR steganography) OR Abstract:("data hiding" OR steganography) OR Keyword:("data hiding" OR steganography)) AND (Title:("Internet of Things" OR IoT) OR Abstract:("Internet of Things" OR IoT) OR Keyword:("Internet of Things" OR IoT))

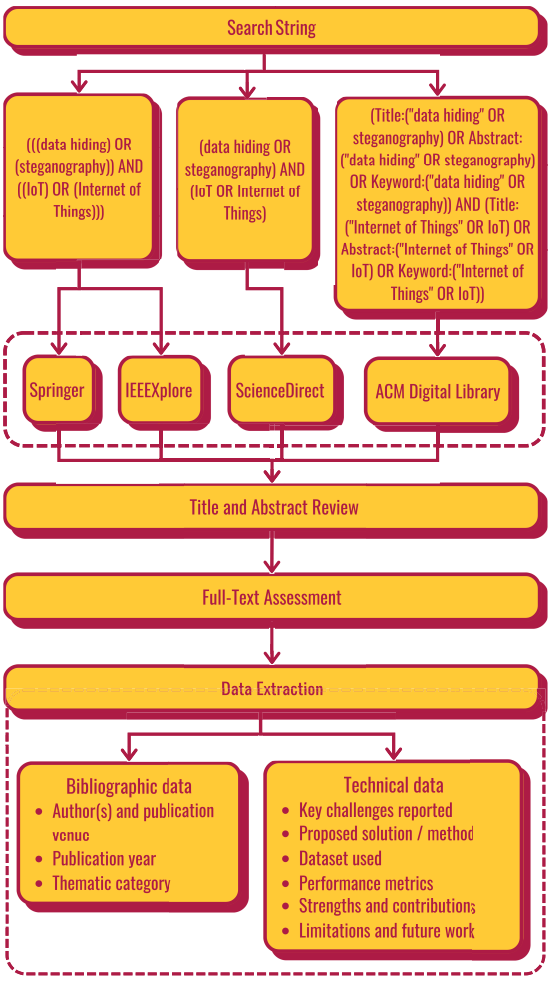

Figure 2: Survey data collecting and filtering process.

4 Findings and Discussions

This section presents the key findings on security challenges and methodological approaches to data hiding and steganography in IoT. It encompasses device constraints, implementation difficulties in dynamic and resource-limited environments, existing methods, datasets, and evaluation practices. It also discusses future directions toward secure and scalable IoT steganographic solutions. To assess the effectiveness and reliability of these techniques, the reviewed literature typically relies on four key criteria outlined in this section. These measures are:

1. Imperceptibility, which assesses how well the embedded data blends with the original medium. The most common metrics for imperceptibility are Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and the Structural Similarity Index (SSIM) defined as in Eqs. (1)–(3).

$$MSE = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} (c_{i,j} - s_{i,j})^2 \tag{1}$$

$$PSNR = 10 \times log_{10} \frac{MAX^2}{MSE} \tag{2}$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_1)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{3}$$

In these equations, $c_{i,j}$ and $s_{i,j}$ denote the pixel values of the cover and stego images at coordinates (i, j). The variables h and w represent the image's height and width. The MAX variable denotes the maximum pixel value. Furthermore, x and y denote the two images being compared (cover and stego). Lastly, μ represents the mean pixel intensity, σ^2 is the variance, and σ_{xy} is the covariance.

2. Embedding Capacity, which evaluates the amount of data that can be hidden without compromising performance.
3. Robustness, which measures resistance to tampering or signal degradation using metrics like BER as defined in Eq. (4).

$$BER = \frac{\text{Number of Erroneous Bits}}{\text{Total Number of Bits Embedded}} \tag{4}$$

4. Security, which concerns the detectability and recoverability of the hidden data.

4.1 Challenges and Practical Barriers in Adapting Steganographic Techniques to IoT Ecosystems

Steganographic research directed at the IoT spans an unusually broad set of application domains, ranging from medical imaging and cloud-hosted health records to unmanned aerial vehicles, industrial control networks, connected vehicles, and voice-controlled smart devices. Each of these domains is represented among the works compiled in Table 3, and taken together they paint a fairly consistent picture of what makes IoT deployment difficult. Rather than a single unified obstacle, what emerges is a cluster of interrelated adaptation problems, namely hardware and energy constraints, contextual and environmental variability, an increasingly adversarial detection landscape, and the operational complexity introduced once multi-stage security pipelines are assembled. These four threads recur across nearly every entry in the table, and they help explain why steganographic techniques that perform well under laboratory evaluation frequently struggle to translate into deployable IoT solutions.

Table 3: A comparative analysis of challenges and solutions for steganography in IoT.

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
He et al. [31]	Current Generative Adversarial Networks for medical steganography suffer from severe pixel distortion and texture degradation. These flaws create structural artifacts that negatively impact clinical assessments and limit their practical deployment for securing sensitive physiological data in the Internet of Medical Things.	To resolve these issues, the authors propose the Dual Adversarial Steganographic Generative Adversarial Network (DAS-GAN) for medical grayscale images. This end-to-end reversible framework uses the Discrete Wavelet Transform to efficiently encode and perfectly recover original images, ensuring diagnostic data remains completely intact. By combining adversarial properties from both spatial and transform domains, the system significantly boosts overall data security, proving highly effective even in real-world Raspberry Pi deployments.

(Continued)

Table 3 (continued)

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
Sethi et al. [32]	The rapid integration of IoT devices in healthcare creates critical vulnerabilities when transmitting sensitive patient data. While traditional encryption methods like RSA and AES provide robust security, they introduce severe computational and energy overheads that overwhelm resource-constrained medical devices.	To address these limitations, the authors propose a lightweight stego-crypto framework that combines efficient cryptography with transform-domain steganography. The system uses Elliptic Curve Cryptography (ECC) for secure key exchange and ChaCha20 for fast symmetric encryption. This encrypted medical data is then hidden inside grayscale medical images using a 2D Discrete Wavelet Transform (DWT) sign-modulation technique. This dual-layered approach ensures end-to-end confidentiality and imperceptibility while drastically reducing power and memory usage compared to traditional methods.
Hassaballah et al. [35]	The expansion of the Industrial Internet of Things (IIoT) and AI generates massive amounts of sensitive data, exposing communication networks to severe privacy threats and hijacking. Traditional steganography methods often degrade image quality and fail to adequately protect against these modern vulnerabilities in intelligent environments.	To secure IIoT communications, the authors propose the Harris hawks optimization-integer wavelet transform (HHO-IWT) method for digital image steganography. This approach uses the nature-inspired HHO algorithm to find an optimal encoding vector and strategically select the best pixels for hiding secret data within the integer wavelet transform. This optimal pixel selection minimizes visual distortion, achieving higher visual quality and robust security against steganalysis compared to existing methods.
Alissa et al. [56]	Utilizing Unmanned Aerial Vehicles (UAVs) in Industry 4.0 expands the attack surface for aerial communications, creating severe privacy risks while the physical constraints of drones heavily restrict their capacity to run heavy deep learning models for image classification.	The authors introduce the Circle Search Optimization with Deep Learning Enabled Secure UAV Classification (CSODL-SUAVC) model. For secure transmission, the framework combines signcryption-based encryption with Multi-Level Discrete Wavelet Transformation (ML-DWT) and an optimized pixel selection technique powered by the Circle Search Optimization (CSO) algorithm to embed hidden data into cover images with minimal distortion. Concurrently, the classification pipeline leverages a Super-Resolution Convolutional Neural Network (SRCNN) enhanced by the Adam optimizer and a softmax classifier, creating an efficient, dual-purpose ecosystem for secure aerial networking and high-accuracy drone imaging.
Shafique et al. [57]	As image transmission escalates across unsecured IoT networks, traditional encryption methods protect data but alter plaintext images into random, noisy patterns that immediately invite suspicion and targeted cyberattacks from eavesdroppers.	The authors present a visually meaningful, lossless image encryption framework that hides pre-encrypted data inside a normal carrier image to completely mask the existence of secret communications. The plaintext color image is first thoroughly secured using multiple chaotic maps, confusion-diffusion operations, and bit-plane extraction. A Discrete Wavelet Transform (DWT) then breaks down a public mask image into frequency sub-bands, replacing its high-frequency components with the encrypted image's bits before applying an inverse DWT to output a perfectly normal-looking, meaningful image that remains robust against brute-force, statistical, and noise attacks.

(Continued)

Table 3 (continued)

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
Mukherjee et al. [58]	A critical challenge in IoT security stems from images captured in low-light settings. These environments severely limit the ability to perform accurate object and human identification, which in turn increases the susceptibility of the system to spoofing and complicates forensic analysis.	To address security vulnerabilities from low-light IoT images, the proposed IoTSLE framework first enhances image quality using a deep learning model, making visual identification more reliable. It then employs a high-capacity steganography technique to securely embed two distinct messages within the enhanced image. This dual approach improves the potential for accurate forensic analysis and helps prevent spoofing by adding a layer of verifiable, hidden information to the now-clearer visual data.
Rajan and Ganesh [59]	Securing information across local networks and the internet requires balancing robust data protection with transmission efficiency. While combining cryptography and steganography is an effective approach, previous algorithms suffer from high time complexity and limited payload capacity. Furthermore, older methods rely on fixed or random pixel shuffling that lacks optimal randomness, leaving the hidden data highly vulnerable to known-plaintext attacks and steganalysis.	To protect data from malicious actors, the paper proposes a framework that combines RC4 encryption with a novel steganography method. Secret data is first encrypted and then hidden in a cover image using a Hash Least Significant Bit (HLSB) technique. The key innovation is the use of a Cheetah Optimizer to dynamically shuffle the image's pixels before embedding, which adds a significant layer of security and makes the hidden data highly resistant to attacks.
Jiang et al. [60]	Resource-constrained IoT devices are often left without efficient, lightweight security solutions, making them vulnerable. This stems from a fundamental mismatch between their practical needs and existing academic research that prioritizes algorithmic complexity.	The paper introduces SmartSteganogaphy, a light-weight audio steganography model. This model is generated automatically through adversarial training and is designed to be small (less than 5 MB), making it suitable for resource-constrained smart devices. It uses a system of three neural networks, an encoder that embeds secret into the carrier, a decoder that extracts the secret, and a discriminator that helps the model learn to conceal the communication effectively.
Zhao et al. [61]	The development of smart environments using technologies like the IoT, AI, and big data presents significant security vulnerabilities. The sensitive data produced by these systems is at high risk of interception by criminal or terrorist entities during transmission, who can then exploit it for unlawful purposes, including covert communications.	This paper proposes a method called Robust Linked List Steganography Without Embedding (RLL-SWE). This technique is designed to secure data transmission in smart environments against interception by criminal and terrorist networks. It works by extracting stable features from a cover image and restructuring them into a multi-head unidirectional linked list without altering the original image. This allows for the covert transmission of sensitive information, as the message is retrieved based on the structure of the linked list, making it highly resistant to attacks.

(Continued)

Table 3 (continued)

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
Alkodre et al. [62]	A critical vulnerability exists in the communication link between a drone and its station, as the interception of this data can result in considerable security risks.	The literature proposes a novel steganography method called the Shuffling Steganography Approach (SSA) to address this challenge. The solution involves a five-stage process that includes encrypting the secret data, dividing it into parts based on a predefined pattern, and then hiding these parts using a hybrid method. A small portion of the encrypted data is hidden within a text cover, which is then merged with the larger remaining part and hidden inside an image cover. This multi-layered approach makes it extremely difficult for an attacker to detect, retrieve, reorder, and decrypt the intercepted data, thus securing the drone's communication link.
Ragab et al. [63]	In the context of Industrial Internet of Things (IIoT) communication, the imperative to guarantee real-time data secrecy elevates data security to an issue of paramount concern.	The authors propose a solution called the Encryption with Image Steganography Based Data Hiding Technique (EIS-DHT). This technique secures data in IIoT environments through a multi-stage process. First, a secret image is split into its R, G, and B color bands, and each band is encrypted separately using different powerful algorithms (Blowfish, Twofish, and Lorenz Hyperchaotic System). A novel Quantum Black Widow Optimization (QBWO) algorithm then selects the optimal pixel locations within a cover image to hide the encrypted data. Finally, the encrypted image bands are embedded into these chosen locations to create a highly secure stego-image for transmission.
Lin et al. [64]	As cloud storage and IoT expand, protecting sensitive data is critical. Traditional reversible data hiding (RDHEI) methods typically perform image encryption directly on the cloud server. This major flaw prevents content owners, such as hospitals, from embedding ownership claims or authentication locally before the data leaves their network, leaving them highly vulnerable to cloud breaches or malicious collusion.	The authors propose an innovative RDHEI scheme combining (t, n) secret sharing with an expandable magic matrix. Crucially, this framework shifts encryption to the local IoT gateway, allowing hospitals to embed ownership claims into images before they are divided into multiple shares and uploaded. This ensures that compromising fewer than t shares will not leak the data, while the magic matrix provides a high, flexible embedding capacity of up to 4 bits per pixel without sacrificing the randomness of the secure shares.
Rathore et al. [65]	The requirement for high-quality, low-latency communication and constant data exchange among vehicles inherently creates an expanded attack surface, presenting vulnerabilities that cybercriminals can exploit.	The authors propose a solution called the Efficient Algorithm for Secure Transmission (EAST) to address this challenge. This method secures data by integrating both encryption and steganography. First, it encrypts the plaintext message using a block cipher symmetric key algorithm to create a ciphertext. Then, this encrypted text is hidden within a cover text file using a steganography algorithm, ensuring that even if the communication is intercepted, the existence of the secret data is concealed. This dual-layered approach enhances confidentiality and makes it difficult for cybercriminals to exploit the data exchanged between vehicles.

(Continued)

Table 3 (continued)

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
Nahar et al. [66]	Existing DNA steganography methods are challenged by operational failures, such as improper cover reconstruction, and inefficiency due to high data overhead. More critically, they exhibit severe security vulnerabilities, including information leakage and a lack of robustness against cyber-attacks.	This paper propose a table-driven, blind steganographic technique specifically designed for securing health data, like DNA sequences, in the cloud. To address existing security vulnerabilities, the method introduces two unique strategies, it uses machine learning for secret encryption and employs a bit-shuffling technique to protect the message, significantly increasing resistance to cyber-attacks. Furthermore, it introduces a novel parity check method to prevent modifications to the stego DNA from attacks. This approach enhances embedding capabilities while successfully reducing the data overhead (stego expansion rate) and minimizing security risks compared to previous methods.
Calo et al. [67]	A significant challenge lies in maintaining robust security and privacy protocols for data during its transmission.	To maintain robust security and privacy for data during transmission, the authors propose a novel self-sufficient coverless video steganography method that combines mapping and synthesis approaches. This technique uses a hash table based on discrete wavelet transform (DWT) features for the efficient matching of secret information within a single carrier video. To ensure complete and secure concealment, the method features a novel synthesis scheme that generates any missing hash sequences without complex generative adversarial networks (GANs), achieving a 100% hiding rate and high robustness against external attacks.
Rostam et al. [68]	The widespread use of IoT devices raises severe privacy concerns when transmitting sensitive personal data. While chaos-based image steganography is often used to hide this information, traditional methods require sharing an initial cryptographic key between the sender and receiver. If this key is intercepted during transmission, attackers can easily regenerate the sequence and expose the confidential data.	To eliminate the risk of key transmission, the authors propose a novel steganography method combining image blocking with the Tent chaos function. The cover image is divided into 3x3 pixel blocks, and the central “pivot” pixels of these blocks are used to mathematically generate the initial key directly from the image itself. Using this self-derived key, the Tent function generates pseudo-random numbers to securely randomize both the selection of image blocks and the specific secret data bits. The data is then concealed within the Least Significant Bits (LSBs) of the pixels, ensuring robust privacy protection without needing to transmit a vulnerable key.
Dhawan et al. [69]	The Internet of Things (IoT) is a domain characterized by the continuous transmission of vast data volumes, which makes ensuring the security of this data a significant challenge.	The authors propose a highly secure steganography technique for transmitting large data volumes across IoT networks. First, a secret image is encrypted using Binary Bit-Plane Decomposition (BBPD). Next, a Salp Swarm Optimization Algorithm (SSOA) drives an adaptive embedding process that intelligently targets edge and smooth blocks in a cover image to maximize the payload capacity. Finally, a hybrid Fuzzy Neural Network enhances the resulting stego image’s visual quality before transmission. This multi-stage approach successfully balances robust security, high image quality, and large data capacity for IoT environments.

(Continued)

Table 3 (continued)

Steganography in IoT		
Author(s)	**Key Challenges Reported**	**Solution**
Ge et al. [70]	Voice-controlled IoT devices face severe eavesdropping risks. While speech steganography can hide communication, current deep learning methods use separate encoder and decoder networks. This separation causes error accumulation that ruins the intelligibility of the extracted speech. Additionally, these methods fail to match the statistical distribution of natural speech, leaving the audio easily detectable and insecure.	The authors propose an invertible generative speech hiding framework that integrates data embedding directly into speech synthesis. Using a module called SecFlow, secret speech is mapped into Gaussian-distributed latent codes and synthesized into cover speech via a flow-based vocoder. Because the network is completely invertible, the embedding and extraction processes share the exact same parameters. This eliminates error propagation, keeping the extracted speech highly intelligible while making the transmitted audio statistically indistinguishable from normal speech.

The most immediate barrier concerns the limited processing power, memory, and energy reserves available on typical IoT hardware. Conventional cryptographic primitives such as RSA and AES are well understood and robust, but they impose computational overheads that resource-constrained medical and wearable devices cannot comfortably sustain. This concern motivated Sethi et al. [32] to pair Elliptic Curve Cryptography with the lighter ChaCha20 cipher and embed the resulting ciphertext through a sign-modulation based two-dimensional discrete wavelet transform, reporting substantially reduced power and memory consumption relative to conventional approaches. Jiang et al. [60] confront the same constraint from the perspective of audio steganography, observing that much of the academic literature prioritizes algorithmic sophistication over deployability, and responding with SmartSteganogaphy, an adversarially trained encoder-decoder-discriminator architecture compressed to under five megabytes so that it can run on smart embedded devices. He et al. [31] extend this concern to medical image security by validating their Dual Adversarial Steganographic Generative Adversarial Network on genuinely constrained hardware, specifically a Raspberry Pi platform, rather than relying solely on simulated results, which underscores that lossless recovery of diagnostic imagery through discrete wavelet decomposition must remain computationally tractable even outside controlled laboratory conditions.

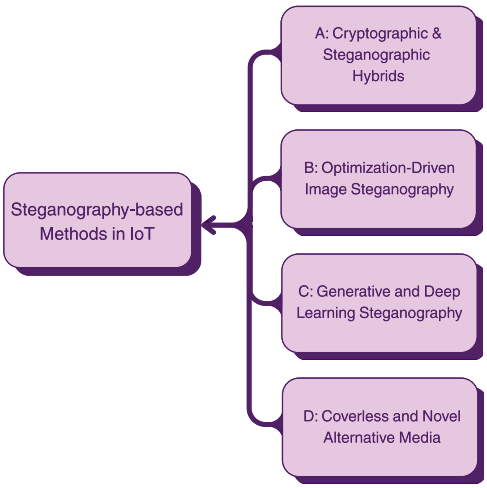

Figure 3: A taxonomy of security approaches in IoT ecosystems. **A:** [32,56,57,59,62–65,68] **B:** [35,69] **C:** [31,58,60,70] **D:** [61,66,67].

A second, closely related challenge arises from the sheer heterogeneity of IoT deployment contexts, which prevents any single embedding strategy from generalizing cleanly across domains. Unmanned aerial platforms illustrate this tension particularly well, since Alissa et al. [56] note that the physical constraints of drones severely limit their capacity to run deep classification models. They respond by combining signcryption-based encryption with multi-level discrete wavelet transformation and Circle Search Optimization for pixel selection, while reserving a lightweight super-resolution convolutional network for the classification stage itself. Alkodre et al. [62] approach the same drone-to-ground-station vulnerability rather differently, distributing an encrypted payload across a five-stage process that splits data between text and image covers so that no single channel carries the full secret. Industrial environments introduce their own timing pressures, with Hassaballah et al. [35] relying on Harris Hawks Optimization to select an optimal encoding vector within an integer wavelet transform so as to minimize visual distortion while resisting steganalysis, and Ragab et al. [63] splitting a secret image into its red, green, and blue components before applying three distinct encryption algorithms and using Quantum Black Widow Optimization to locate suitable embedding positions, a design intended to satisfy the near real time secrecy demands of Industrial IoT communication. Vehicular networks present a comparable challenge, addressed by Rathore et al. [65] through a block cipher combined with text-based steganography for the Internet of Vehicles, and more broadly by Rajan and Ganesh [59], whose Cheetah Optimizer driven pixel shuffling paired with Hash Least Significant Bit embedding targets the time complexity and predictable shuffling patterns that had previously left transmitted data vulnerable to known-plaintext attacks. Environmental variability compounds this same heterogeneity problem, since the conditions under which IoT devices actually capture and transmit data are rarely as clean as those assumed during algorithm design. Mukherjee et al. [58] make this point directly by targeting low-light image capture, a common scenario for surveillance and monitoring nodes, in which reduced visual clarity undermines both human identification and forensic verification. Their IoTSLE framework first applies deep learning based enhancement before performing high-capacity embedding of two distinct messages using finite automata and DNA computing principles, thereby treating image quality as something to be actively corrected rather than assumed fixed.

Beyond resource and contextual limitations, the growing sophistication of steganalysis and adversarial detection tools represents a distinct and evolving threat that many of the surveyed methods explicitly target. As IoT ecosystems increasingly incorporate artificial intelligence and large-scale analytics, adversaries gain access to adaptive classifiers capable of flagging statistically anomalous carrier signals, which has pushed several research groups away from simple least-significant-bit style modification. Shafique et al. [57] construct a visually meaningful encryption scheme in which chaotic maps, confusion-diffusion operations, and bit-plane extraction secure the plaintext before its bits replace selected high-frequency wavelet subbands of an otherwise ordinary carrier image, producing output that resists brute-force, statistical, and noise-based attacks while giving no visual indication that a secret exists. Zhao et al. [61] pursue an even more conservative strategy through steganography without embedding, extracting stable features from a cover image and reorganizing them into a multi-head unidirectional linked list so that the carrier itself is never modified, a property intended to defeat interception by criminal or terrorist networks operating within smart environments. Rostam et al. [68] isolate a narrower but often overlooked vulnerability, namely the transmission of the cryptographic key itself, and eliminate it entirely by deriving a Tent chaos function seed from the pivot pixels of three by three image blocks, removing the need to exchange any key between sender and receiver in the first place. Nahar et al. [66] apply a comparable defensive posture to DNA-based health data steganography, combining machine learning driven encryption with a bit-shuffling technique and a novel parity check mechanism that prevents undetected modification of the stego sequence, while also reducing the stego expansion rate relative to earlier table-driven methods. Ge et al. [70] extend this

same adversarial concern into the speech domain, showing that conventional encoder-decoder speech hiding architectures fail to reproduce the natural statistical distribution of speech and are therefore detectable, and countering this with an invertible generative framework, SecFlow, in which secret speech is mapped to Gaussian distributed latent codes and synthesized through a flow-based vocoder whose embedding and extraction stages share identical parameters, keeping the resulting audio statistically close to ordinary synthesized speech.

A further source of difficulty lies in the architectural and operational complexity that many of these solutions introduce once cryptographic, optimization-based, and neural components are combined into a single pipeline. Lin et al. [64] address a structural weakness in conventional reversible data hiding for encrypted images, namely that encryption is typically performed on the cloud server itself, leaving content owners unable to embed ownership claims locally. Their solution relocates encryption to the IoT gateway and combines a (t, n) secret sharing scheme with an expandable magic matrix capable of an embedding capacity of up to four bits per pixel without compromising the randomness of the resulting shares. Calo et al. [67] avoid heavy generative components altogether in coverless video steganography, instead using a discrete wavelet transform based hash table for secret matching and a dedicated synthesis scheme for any missing hash sequences, achieving a reported hiding rate of one hundred percent without relying on generative adversarial networks. Dhawan et al. [69] illustrate a different form of complexity by chaining Binary Bit-Plane Decomposition for encryption, a Salp Swarm Optimization Algorithm that adaptively targets edge and smooth regions of the cover image for embedding, and a hybrid Fuzzy Neural Network for post-embedding quality enhancement. Taken together, these examples show that while multi-stage architectures reliably improve individual performance metrics, they also raise integration and maintenance burdens that become increasingly difficult to manage as systems scale across heterogeneous fog, edge, and cloud layers.

A final, somewhat cross-cutting issue becomes visible only when these methods are considered as a whole, and it concerns the absence of a shared evaluation methodology across the field. Each contribution tends to report the metrics most favorable to its own design, whether that is embedding capacity, distortion measures such as PSNR and SSIM, resistance to a particular class of steganalysis, or processing latency, but rarely all of these simultaneously and rarely under comparable device and network conditions. This inconsistency makes it genuinely difficult to determine whether performance gains reported for, say, a drone-oriented UAV classification framework would transfer cleanly to a medical IoT setting with very different bandwidth and power characteristics. It is likewise unclear whether a scheme demonstrated on desktop-class hardware would retain its reported advantages once deployed to the kind of constrained edge nodes it was ostensibly designed for. Without common benchmarks, readers are left to compare methods largely on the strength of the authors' own framing rather than on directly comparable evidence.

Addressing these compounding challenges will likely require research to move beyond isolated algorithmic improvements toward more systemic solutions. Lightweight, adaptive embedding algorithms that scale their computational footprint to available device resources would help close the gap between laboratory performance and real deployment. Gateway or edge-native processing that avoids dependence on centralized cloud infrastructure, together with steganographic designs that are explicitly evaluated against adaptive, learning-based steganalysis rather than static detectors, would further address the resource, heterogeneity, and adversarial dimensions identified above. Equally important is the development of standardized benchmarking protocols that jointly report capacity, imperceptibility, energy consumption, and throughput under realistic and reproducible IoT conditions, which would allow the diverse contributions surveyed here to finally be compared on genuinely equal terms rather than through isolated, domain-specific evaluations.

4.2 Datasets, Performance Benchmarks, and Reported Strengths of Steganographic Techniques in IoT

Steganography continues to serve as a central technique for enhancing Internet of Things security, allowing sensitive information to be embedded within images, audio, video, or even biological sequences so that its transmission remains covert. Table 4 compiles eighteen recent contributions spanning medical imaging, industrial and Industrial IoT communication, unmanned aerial vehicles, voice-controlled devices, vehicular networks, and cloud-based health data, each evaluated on its own datasets and performance metrics. This section synthesizes the methodological trends visible across these works, the quantitative strengths they report, and the gaps that remain once the datasets and evaluation protocols are examined collectively. Image-based approaches dominate the collection, but the range of media types and target applications is considerably broader than a single modality can capture.

Among the image-based methods, imperceptibility figures reported through PSNR and SSIM are consistently high, though the specific values vary with embedding capacity and payload size. Sethi et al. [32] report a PSNR as high as 75.32 dB on the MURA radiograph dataset for their ECC-ChaCha20 and wavelet-based scheme, while Hassaballah et al. [35] reach 52.47 dB and an SSIM of 0.9988 on the USC-SIPI database using Harris Hawks Optimization for pixel selection. Rajan and Ganesh [59] similarly report PSNR up to 61.68 dB with SSIM reaching 0.9999 through their Cheetah Optimizer-driven pixel shuffling and Hash LSB scheme, and Ragab et al. [63] achieve comparable fidelity, with PSNR up to 56.76 dB, SSIM up to 0.9995, and a Quality Index of 1.000 on the same USC-SIPI images. Dhawan et al. [69] report PSNR up to 60.82 dB and SSIM up to 0.999279 for their hybrid optimization framework, and their measurements extend across three separate cover images to show how quality shifts with increasing payload. He et al. [31] evaluate their reversible DAS-GAN on medical neuroimaging datasets, reporting PSNR up to 44.32 dB together with an effective embedding capacity reaching 3.3704 bits per pixel and classification accuracy up to 98.84% on ADNI, figures that decline only modestly on the BraTS2023 dataset.

Beyond static images, several contributions target other media entirely. Jiang et al. [60] apply adversarial training to speech data drawn from TIMIT and LibriSpeech, reporting carrier and secret loss values as low as 0.0001 and 0.0003 respectively, along with a carrier SNR reaching 7.2413. Ge et al. [70] extend speech steganography further with an invertible generative framework evaluated on LJ Speech and AISHELL-3, reporting stego speech MOS up to 3.82, PESQ up to 3.47, and STOI up to 0.97, alongside extracted secret speech that retains a character error rate as low as 0.021 and speaker consistency accuracy reaching 1.000 under favorable conditions. Calo et al. [67] move into the video domain with a coverless steganography method tested on UCF101 and HMDB51, reporting a hiding success rate of 100% and processing efficiency of 0.00007 s per byte, figures that reflect the appeal of coverless techniques for latency-sensitive IoT communication. Zhao et al. [61] take an embedding-free approach on ImageNet, restructuring stable image features into a linked list rather than modifying pixel values directly, and their restoration accuracy remains near 100% under most tested conditions.

Table 4: Steganography in IoT (dataset, reported performance, strengths).

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Dual-adversarial generative networks for reversible steganography in medical image security of Internet of Medical Things [31]	1. Alzheimer's Disease Neuroimaging Initiative (ADNI) 2. Brain Tumor Segmentation Challenge (BraTS2023)	1. ADNI dataset on 1–4 bpp (a) PSNR: 44.32–36.47 dB (b) SSIM: 0.9902–0.9433 (c) Accuracy: 98.84%–92.13% (d) Effective capacity (bpp): 0.9768–3.3704 2. BraTS2023 dataset on 1–4 bpp (a) PSNR: 42.14–35.12 dB (b) SSIM: 0.9864–0.9121 (c) Accuracy: 97.56%–91.79% (d) Effective capacity (bpp): 0.9453–3.1267 Note: The model was deployed on a Raspberry Pi 4B, equipped with a 1.5 GHz 64-bit quad-core ARM Cortex-A72 processor, 4 GB of RAM, and a Broadcom VideoCore VI GPU clocked at 500 MHz.	The DAS-GAN method provides a robust steganography solution for the Internet of Medical Things by generating high-fidelity steganographic images while securely preserving and accurately recovering both the embedded data and the original medical images.
Lightweight DWT Steganography with ECC-ChaCha20 for Secure Medical IoT Systems [32]	Musculoskeletal Radiographs (MURA) dataset	Performances: 1. PSNR: 75.32–61.08 dB 2. MSE: 0.003–0.305 3. SSIM: 0.9960–0.9100 4. Memory consumption: 38.00–49.14 MB 5. Power consumption: 78.20–104.28 mW Note: The provided data are only from the best version of the method, which is the two-dimensional DWT with ECC-ChaCha20. Furthermore, the lowest message size is 32 bytes, with the highest being 8192 bytes Robustness (BER): 1. Gaussian Noise (θ = 0.005) = 0.014 2. Salt & Pepper Noise (1%) = 0.021 3. Rotation (10°) = 0.027 4. Translation (5 px) = 0.016 5. Blurring (3 × 3 kernel) = 0.019 6. JPEG Compression (Quality = 50) = 0.012	The research proposed a method that combines cryptography and wavelet-domain steganography to provide high imperceptibility and robustness for securing data transmission in medical IoT fields.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
A Novel Image Steganography Method for Industrial Internet of Things Security [35]	USC-SIPI image database	Performance Evaluation 1. PSNR: 35.66–52.47 dB 2. SSIM: 0.9095–0.9988 3. Quality Index (QI): 0.9956–1.0000 4. Embedding capacity: 12.5%–50% of the image resolution 5. Embedding time: 34.14–35.35 s 6. Extraction time: 18.76–19.36 s Note: The performance was measured with increasing k-LSBs values, which indicate the number of embedded bits, ranging from 1 to 4. As the value of k increases, the performance decreases. Robustness Evaluation 1. Structural Content (SC): 0.9499–1.000 2. Normalized Absolute Error (NAE): 0.0377–0.1861 3. Enhancement Measurement Error (EME): 6.3100–23.8164 4. Root Mean Squared Error (RMSE): 7.3805–18.8082 5. PSNR: 22.68–30.80 dB 6. Normalized Cross-Correlation (NCC): 0.9514–1.0000 7. Average Difference (AD): 1.2810–8.7578 Note: The method's robustness is evaluated against several types of attack, including Erosion, Gaussian noise, dilation, Salt & Pepper noise, motion blur, local variance, JPEG compression, Speckle noise, and Poisson noise with k-LSBs value equals to 4. RS-attack Average Differences 1. Singular Group = 1.691% 2. Regular Group = 2.174%	The HHO-IWT method provides a decent IoT steganographic framework, proven with considerable imperceptibility, high robustness against steganalysis attacks, and better secret bits recovery than previous methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Optimal Deep Learning Model Enabled Secure UAV Classification for Industry 4.0 [56]	1. UCM dataset 2. AID dataset	1. PSNR: 57.30–62.45 dB 2. MSE: 0.037–0.121 3. Correlation Coefficient: 99.93–99.95 4. Computational Time: 1.115–1.448 s 5. Precision: 95.66% 6. Recall: 94.43% 7. F1-Score: 95.12% 8. F2-Score: 95.68% Note: The performance was measured using Samples 1 to 5. Encryption performance 1. PSNR: 6.76–9.56 dB 2. MSE: 2.0579×10^4–8.8614×10^4 3. Spectral Distortion (SD): 2.3869×10^4–2.3997×10^4 Note: The encryption performance presented above was evaluated using the Baboon RGB image (256 × 256) by comparing the encrypted and original images across the R, G, and B components. Unlike imperceptibility metrics, lower similarity values (e.g., PSNR) in this paper indicate better encryption performance. Correlation Coefficient (CC): −0.0024–0.0001 Note: The CC above was evaluated on the Lena and Cameraman images. Statistical noise attack analysis 1. PSNR: 0.64–0.88 dB 2. MSE: 51–103 3. SSIM: 55–115 Note: The performance above was evaluated on the Baboon image with noise percentage values ranging from 25 to 100, across R, G, and B components. Processing time: 0.0018–0.0033 s Note: The processing time was evaluated across all images, and the method was evaluated in a system with an i5 CPU (2.45 GHz) and 16 GB RAM.	The CSODL-SUAVC model provides a highly effective framework for secure UAV communication and image classification in Industry 4.0 environments, proven to achieve maximum operational performance and better overall efficiency compared to recent state-of-the-art approaches.
Enhancing privacy in data transmission between IoT devices: A robust encryption and embedding framework for secure and meaningful image communication [57]	Unspecified dataset		The proposed encryption and embedding framework provides a highly effective and balanced solution for secure image transmission in IoT environments, proven to achieve efficient processing time, memory conservation, and enhanced security compared to the constraints and requirements of resource-limited IoT devices.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
IoTSLE: Securing IoT systems in low-light environments through finite automata, deep learning and DNA computing based image steganographic model [58]	1. LOL dataset 2. USC-SIPI image database	Performance evaluation 1. SSIM: 0.9884–0.9990 2. PSNR: 38.52–38.57 dB 3. Embedding Capacity: 2.67 bpp Security analysis 1. Payload = 2,097,152 bits, size 512 × 512 (a) Average NAE: 0.0329 (b) Average BER: 0.000526 (c) Average Q-Index: 0.9788 (d) Average NCC: 0.9895 2. Payload = 524,288 bits, size 256 × 256 (a) Average NAE: 0.0330 (b) Average BER: 0.000554 (c) Average Q-Index: 0.9766 (d) Average NCC: 0.9893 Note: The performance was measured across 8 images from the USC-SIPI image database, including Peppers, Sailboat, Earth, House, Mandrill, Airplane, San Diego, and Splash.	IoTSLE provides the first steganographic framework specifically designed for securing IoT systems operating under low-light conditions, proven to achieve superior embedding capacity and enhanced imperceptibility compared to existing DNA sequencing-based image steganography schemes.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework [59]	Unspecified Dataset	1. PSNR: 51.65–61.68 dB 2. MSE: 0.0444–0.4447 3. SSIM: 0.9993–0.9999 4. Embedding time: 0.0153–0.0390 s 5. Extraction time: 0.5329–0.6256 s Note: The method's performance reported in this paper was evaluated using four cover images, Peppers, Barbara, Baboon, and Lena, at embedding rates ranging from 0.1 to 1. Furthermore, a 1 KB ASCII text was used as the secret message. Furthermore, the implementation was conducted on a system with Intel Core i7-9700 K CPU, 16 GB RAM, and an NVIDIA GeForce GTX 1660 Ti	In this paper, a novel HLSB and RC4-based steganography method, enhanced by a novel Cheetah Optimizer-driven dynamic pixel shuffling mechanism, provides a highly effective and secure framework for data hiding, proven to achieve superior embedding quality and imperceptibility compared to existing steganographic techniques.
SmartSteganogaphy: Light-weight generative audio steganography model for smart embedding application [60]	1. TIMIT 2. LibriSpeech	Performance 1. Carrier Loss MSE = 0.0001–0.0056 2. Secret Loss MSE = 0.0003–0.0058 3. Carrier SNR = 1.8732–7.2413 4. Secret SNR = −2.4235–0.3599 Robustness 1. Carrier Loss MSE = 0.0001–0.0056 2. Secret Loss MSE = 0.0003–0.0058 3. Carrier SNR = 1.8732–7.2413 4. Secret SNR = −2.4235–0.3599 Note: The robustness was evaluated under two conditions: normal training (NOR) and with 60 dB Gaussian noise added to the carrier audio during the training process (AN). Steganalysis accuracy 1. Against SRM: 73.82%–85.26% 2. Against CNN: 91.56%–92.58% Model size: <5 MB	The proposed generative audio steganography model provides a novel, lightweight, and machine learning-based framework for secure audio transmission over IoT networks, proven to achieve high-fidelity steganographic audio with enhanced robustness and security compared to conventional handcrafted audio steganography methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
RLL-SWE: A Robust Linked List Steganography Without Embedding for intelligence networks in smart environments [61]	Imagenet	Restoration accuracy under various conditions 1. Ideal performance (with no attacks or transmission errors): 100% 2. Gaussian noise (σ = 0.005 – −0.001): 98.30%–99.18% 3. Salt & Pepper noise (d = 0.005 – −0.001): 99.99% 4. Mean and Median filters: 98.12%–99.30% 5. Rotation (θ = 30°–5°): 66.40%–87.42% 6. JPEG Compression (Q = 10–50): 98.26%–99.30% Note: The restoration accuracies under the Mean and Median filters were evaluated using *ksize* values of 3 × 3, 5 × 5, and 7 × 7. Best bit capacity on 512 × 512 carrier: 10–14 bits each segment Note: The method's embedding capacity (message segment length) is not limited to a specific picture size and increases as the size grows.	The proposed RLL-SWE technique provides an innovative, robust, and embedding-free steganography framework for secure information transmission in smart environments, proven to achieve high message restoration accuracy and strong resistance to adversarial attacks compared to traditional steganography methods.
A Shuffling-Steganography Algorithm to Protect Data of Drone Applications [62]	Unspecified dataset	1. Execution Time: ~0.35–0.40 s 2. PSNR: ~67–79 dB 3. Extraction Error Rate: 0.998–1.000 4. Computational Complexity: ~0.24–0.40 s 5. Shannon Entropy: ~1.85 6. Used text length = 80–800 characters	This paper introduces a novel steganography approach called the Shuffling Steganography Approach (SSA). SSA encompasses five fundamental stages and three proposed algorithms, designed to enhance security through strategic encryption and data hiding techniques.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Encryption with Image Steganography Based Data Hiding Technique in IoT Environment [63]	USC-SIPI image database	Performance 1. PSNR: 55.70–56.76 dB 2. SSIM: 0.9971–0.9995 3. MSE: 0.1372–0.1752 4. QI: 1.000 5. Embedding capacity (% of the cover): 15.58%–17.37% 6. Embedding time: 33.75–35.06 s 7. Extraction time: 17.82–18.85 s Note: The performance of the method was measured using several 256 × 256 images, such as Baboon, Boat, and Lena, as both cover and secret images. Robustness 1. MSE: 47.0116–317.1320 2. RMSE: 6.8565–17.8082 3. PSNR: ~23.19–31.41 dB 4. NCC: 0.9614–1.0000 Note: The robustness of the method was evaluated using several attacks, including Erosion, Gaussian noise, Dilation, S&P noise, Speckle noise, and Poisson noise.	The proposed EIS-DHT technique provides an efficient and secure image steganography framework for IIoT communication, proven to achieve optimal pixel selection and enhanced data-hiding performance compared to existing techniques through its integration of channel extraction, decomposition, QBWO-based optimization, encryption, and embedding processes.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Hiding information in encrypted images with (t, n) secret sharing for IoT and cloud services [64]	1. Unspecified dataset (6 test images) 2. BOSSbase 3. BOW-2 4. Osirix	1. Average Number of Change Pixel Rate (NPCR): 99.6027%–99.6188% 2. Average Unified Averaged Changed Intensity (UACI): 0.3065%–30.1940% 3. Average PSNR: ~6.31–8.74 dB 4. Average SSIM: 0.0046–0.0100 5. Average Horizontal Correlation: −0.0057–0.2001 6. Average Vertical Correlation: −0.0013–0.0006 7. Average Entropy: 7.9950–7.9994 8. Average Payload: 4 bpp Note: The ranges of metrics above represent the minimum and maximum average values measured across all datasets for the encrypted image, Share 1, and Share 2, with the number of required images for extraction t and share images n equal to two. Moreover, the experiment was conducted in an environment with an AMD Ryzen 7 5800H CPU, Radeon Graphics operating at 3.20 GHz, and 16 GB of RAM running at 3200 MHz	The proposed RDHEI scheme provides a highly effective framework for secure image sharing in IoT and cloud environments, proven to achieve strong resistance to hacker attacks, full reversibility, and high embedding capacity compared to traditional CSP-dependent ownership-embedding approaches.
A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography [65]	Unspecified dataset	1. Encryption Time: 0.083–0.334 ms 2. Avalanche effect: 49.67%–58.81% 3. PSNR: 64.31%–71.58% 4. Cover size needed: ~1.9 times the file size Note: The file sizes used in the paper for evaluation are 10, 20, and 40 kb.	The proposed EAST algorithm provides a highly effective and efficient framework for secure communication in IoV environments, proven to achieve superior time efficiency, avalanche effect, PSNR, and cover file size compared to state-of-the-art encryption and steganography methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Protecting health data in the cloud through steganography: A table-driven, blind method using neural networks and bit-shuffling algorithm [66]	1. National Center for Biotechnology Information's (NCBI) dataset (for DNA sequence) 2. Unspecified Google repository (for images) 3. A generated false DNA sequence	1. Embedding capacity: 1 bit per nucleotide 2. Maximum Expansion Rate: 50% 3. Error rate: 0% Note: The message lengths used in the performance evaluation ranged from 200 to 200,000 bits. The experiment was conducted on a desktop Acer with a 3 GHz processor and 16 GB of RAM.	The proposed DNA sequence-based data-hiding scheme provides a highly secure and reversible framework for embedding confidential information, proven to achieve near-zero cracking probability, zero extraction error, and lower expansion rate compared to existing DNA-based data-hiding methods.
Novel Self-sufficient Coverless Video Steganography for Secured Internet of Things (IoT) Communication [67]	1. UCF101 2. HMDB51	1. Hiding Success Rate: 100% 2. Time Efficiency: 0.00007 s per byte (s/B) 3. Average retrieval accuracy: 97.83% Note: The retrieval accuracy was evaluated under several attacks, including Salt and pepper, Gaussian, and Speckle noise with σ values ranging from 0.001 to 0.01, as well as default compression attacks, including MPEG-4 and JPEG compression. Furthermore, the experiment was conducted on a computer with an Intel Core i7 processor running at 2.80 GHz, 12 GB of RAM, and an NVIDIA GeForce GTX 1050 2GB GPU.	The proposed coverless video steganography method provides a self-sufficient and practical framework for enhancing security in IoT communications, proven to achieve complete secret information hiding within a single carrier video, reduced hiding time costs, and strong retrieval accuracy against noise and compression attacks compared to state-of-the-art methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Privacy-preserving in the Internet of Things based on steganography and chaotic functions [68]	1. UCID-Image Database 2. Harvard whole-brain Atlas (Dataset-75)	1. Perspective 1 (a) Average PSNR: 45.88 (b) Average SSIM: 0.9887 (c) Average MSE: 1.0060 (d) Average BER: 0.0833 (e) bpp: 1.5 2. Perspective 3 (a) PSNR: ~56–46 (b) MSE: ~0.1–1 (c) BER: ~0.45–0.9 Note: The performance of the method was evaluated from three perspectives. However, only the metrics for Perspective 1 and Perspective 3 are presented above. In Perspective 1, the method was evaluated using the UCID-Image Database as the cover images with an embedding rate of 1.5 bpp. In Perspective 3, the method was evaluated using the Dataset-75 (DS-75) images as the cover images with secret message sizes of 1000, 5000, and 10,000 bits. The simulation of the proposed method was carried out on a laptop with Intel Core 2 Duo 2.67 GHz, 4 GB RAM, and a 320 GB Hard disk.	The proposed chaos-based image blocking steganography method provides an effective framework for preserving privacy in IoT environments, proven to achieve high-quality stego-images and better performance compared to existing methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT [69]	USC-SIPI image database	Image Quality Analysis 1. PSNR: ~55.91–60.82 dB 2. MSE: 0.0537–0.1668 3. SSIM: 0.996948–0.999279 4. Image Fidelity (IF): 0.999007–0.999684 Payload Capacity Analysis 1. Lena PSNR: ~56–53 dB 2. Bell Pepper PSNR: ~54–48 dB 3. Baboon PSNR: ~53–47 dB Security Analysis (KL Divergence) 1. Lena KLD: ~0.039–0.045 2. Bell Pepper KLD: ~0.059–0.065 3. Baboon KLD: ~0.035–0.040 Note: The image quality metrics were evaluated using the Lena, Bell Pepper, and Baboon images as cover images and the Cameraman, Airplane, and Barbara images as hidden images. The payload capacity analysis was then conducted using the same cover images as the previous analysis, with increasing payload capacities ranging from 0.5 to 2.5 bpp. The security analysis was performed using payload capacities of 0.7, 1.6, and 2.3 bpp. Furthermore, the experiment was conducted in an environment with intel 8 GB RAM.	The proposed steganography framework provides a highly secure and quality-preserving method for transmitting hidden medical images over IoT protocols, proven to achieve improved payload capacity, image quality, and security compared to existing state-of-the-art methods.

(Continued)

Table 4 (continued)

Steganography in IoT			
Literature Title	**Dataset(s)**	**Performance**	**Strengths**
Invertible generative speech hiding with normalizing flow for secure IoT voice [70]	1. Self-generated Mel-spectrograms using SGNs 2. LJ Speech 3. AISHELL-3	Stego speech quality: 1. MOS: 3.72–3.82 2. PESQ: 3.40–3.47 3. STOI: 0.95–0.97 Note: The performance results are from LJ Speech, using both WaveGlow and SqueezeWave generators. On AISHELL-3 the values were a bit lower (MOS 3.25–3.29, PESQ 3.12–3.15, STOI 0.93–0.94). Extracted secret speech quality: 1. MOS: 3.32–3.33 2. PESQ: 3.23–3.48 3. STOI: 0.96–0.97 4. CER: 0.021–0.026 5. SNR: 11.80–15.89 dB Note: The CER is from the Jasper ASR model at 2.22 s secret speech length; SNR values are for LJ Speech and AISHELL-3, respectively. Speaker consistency (SCA): 0.612–1.000 Note: tested on AISHELL-3 with 4 ASV models (GE2ESV, ECAPA-TDNN, TitaNet, SpeakerNet), thresholds 0.7–0.85, speech length 0.74–2.22 s. Efficiency: 1. Embedding time: 0.017–0.035 s (GPU), 1.28–2.44 s (CPU) 2. Extraction time: 0.019–0.042 s (GPU), 1.27–2.43 s (CPU) 3. RTF: 0.572–0.577 Note: The experiment was conducted on a system with an RTX 4090 GPU and an i9-14900K CPU. The evaluations were measured for a 2.22 s speech segment, RTF from the lightweight SqueezeWave setup. Statistical security (stego vs. cover speech distance): 1. KL divergence: ~0.00021–0.00029 2. Energy distance: ~2.80×10^{-7}–1.85×10^{-6} 3. Wasserstein distance: ~6.0×10^{-5}–4.1×10^{-4} Note: These values are close to the distance between two normal cover speech samples (KL 0.000059), showing the stego speech is hard to tell apart statistically.	The proposed invertible generative speech hiding framework provides a highly secure and quality-preserving method for transmitting hidden speech commands over IoT voice channels, proven to achieve improved stego speech quality, secret speech intelligibility, and real-time efficiency compared to existing state-of-the-art speech hiding methods.

Robustness under adversarial or transmission-induced distortion is reported by several of the surveyed methods, though the specific attacks tested differ from paper to paper. Sethi et al. [32] report bit error rates as low as 0.012 under JPEG compression and no higher than 0.027 under 10 degree rotation, while Hassaballah et al. [35] and Ragab et al. [63] both test resilience against dilation, Gaussian noise, salt and pepper noise, and Poisson noise, recovering structural content values above 0.94 and normalized cross-correlation values approaching 1.000 in most cases. Zhao et al. [61] report restoration accuracy staying above 98% under Gaussian noise, salt and pepper noise, and JPEG compression. However, their accuracy drops from 87.42% to 66.40% as rotation attacks increase from 5 to 30 degrees, indicating that geometric distortion remains a harder case than pixel-level noise. Alkodre et al. [62] report an extraction error rate between 0.998 and 1.000 for their shuffling-based approach applied to drone communication, a result that speaks to the reliability of their five-stage encryption and hiding pipeline even under the execution time constraints imposed by aerial platforms.

Several works place a stronger emphasis on cryptographic and statistical security rather than visual fidelity alone. Shafique et al. [57] deliberately report low similarity metrics for their encryption stage, with PSNR between 6.76 and 9.56 dB and a correlation coefficient close to zero, since in their visually meaningful encryption framework weaker resemblance between plaintext and ciphertext indicates stronger protection rather than a shortcoming. Lin et al. [64] report an average Number of Pixel Change Rate above 99.60% and entropy values approaching the theoretical maximum of 7.9994 across BOSSbase, BOW-2, and Osirix, supporting their gateway-level encrypted secret sharing scheme. Nahar et al. [66] report a zero percent error rate for their DNA-based hiding method evaluated on NCBI sequence data, with an embedding capacity of one bit per nucleotide and a maximum expansion rate of 50 percent. Rostam et al. [68] avoid key transmission altogether by deriving their chaotic seed from the cover image itself, reporting PSNR up to 45.88 dB and SSIM of 0.9887 on the UCID database at an embedding rate of 1.5 bits per pixel.

Efficiency and hardware feasibility are addressed explicitly in a subset of the studies, which matters given the constrained processing budgets typical of IoT deployment. He et al. [31] validate their DAS-GAN model directly on a Raspberry Pi 4B, confirming that reversible medical image steganography can run on genuinely limited hardware rather than only in simulation. Shafique et al. [57] report processing times between 0.0018 and 0.0033 s on a standard desktop CPU, and Rajan and Ganesh [59] report embedding times as low as 0.0153 s, both suggesting suitability for near real-time operation. Ge et al. [70] report the widest efficiency range among the surveyed works, with embedding latency dropping to 0.017 s on a GPU but rising to as much as 2.44 s on CPU alone, illustrating how heavily flow-based generative approaches depend on hardware acceleration to meet real-time factor targets near 0.57.

The datasets used across the surveyed works reveal a field that draws from a wide variety of domains without converging on shared benchmarks. Medical imaging is represented through ADNI, BraTS2023, MURA, and the Harvard whole-brain atlas, natural image benchmarks appear through USC-SIPI, UCID, and standard test images such as Lena, Baboon, and Peppers, aerial and remote sensing data appear through UCM and AID, speech corpora include TIMIT, LibriSpeech, LJ Speech, and AISHELL-3, and video steganography draws on UCF101 and HMDB51. Several contributions, including those by Shafique et al. [57], Rajan and Ganesh [59], Alkodre et al. [62], and Rathore et al. [65], do not specify a named public dataset, relying instead on individually selected test images or generated files whose scale and diversity are difficult to assess from the reported figures alone. This pattern makes direct cross-paper comparison difficult even where the same metric, such as PSNR or SSIM, is reported in multiple studies, since the underlying cover material, payload size, and embedding rate are rarely held constant.

Despite these encouraging results, the collection of studies surveyed here also exposes some recurring weaknesses that limit how confidently the reported numbers can be generalized. A sizable share of the

methods, including those of Shafique et al. [57], Rajan and Ganesh [59], Alissa et al. [56] for the security component of their pipeline, Alkodre et al. [62], and Rathore et al. [65], rely on unspecified or self-selected datasets rather than named public benchmarks, which makes it difficult for other researchers to reproduce the reported PSNR, SSIM, or robustness figures under identical conditions. A related gap concerns experimental transparency, since several of the surveyed entries, among them Alissa et al. [56], Zhao et al. [61], and Alkodre et al. [62], report performance numbers without disclosing the hardware or software environment used to obtain them, in contrast to studies such as those by He et al. [31], Shafique et al. [57], Rajan and Ganesh [59], Lin et al. [64], and Calo et al. [67], which explicitly state the CPU, GPU, or embedded platform involved. This inconsistency makes it hard to judge whether a reported embedding time of a few milliseconds reflects genuine efficiency or simply a more powerful test machine. Robustness testing is also uneven, since attacks such as rotation, translation, or geometric warping are evaluated by only a handful of the surveyed methods, and even among those that do, the specific noise levels, filter sizes, or compression ratios tested rarely overlap enough to allow a fair side-by-side comparison. Finally, almost none of the surveyed studies report results from a live IoT network or a multi-device testbed, with hardware validation such as He et al.'s [31] Raspberry Pi deployment remaining the exception rather than the norm.

Building on these observations, several directions appear promising for future research. Wider adoption of shared, publicly available benchmark datasets, similar to how USC-SIPI already recurs across multiple image-based studies, would make cross-method comparison considerably more reliable than the current mix of proprietary and unspecified test sets allows. Consistent reporting of the hardware and software configuration used for every timing or efficiency measurement would likewise help distinguish genuine algorithmic gains from differences in test infrastructure. Expanding robustness evaluation to a common, agreed-upon set of attacks, covering geometric distortion alongside the more commonly tested noise and compression attacks, would give a fuller picture of how these methods behave outside idealized conditions. Finally, moving beyond desktop or single-board simulation toward validation on actual multi-device IoT deployments, following the direction already taken by He et al. [31] on a Raspberry Pi, would help confirm whether the strong imperceptibility and robustness figures reported above continue to hold once these methods operate within real, resource-constrained, and network-variable IoT environments.

4.3 Limitations and Research Opportunities in IoT-Based Steganography

Table 5 summarizes the limitations, gaps, and suggested future work reported across the eighteen steganographic methods surveyed for IoT applications. Several recurring themes emerge once these entries are read together, including trade-offs between embedding capacity and both quality and detectability, vulnerabilities tied to key management and protocol design, uneven robustness against different classes of attack, unresolved scalability concerns, and a noticeable inconsistency in how transparently authors report the weaknesses of their own methods. Taken as a whole, the table paints a picture of a field that has made strong progress on imperceptibility and basic security demonstrations while leaving many of the harder deployment questions for future work rather than resolving them within the studies themselves.

Table 5: Steganography in IoT (limitations, future work).

Steganography in IoT		
Literature Title	**Limitations/Gaps**	**Suggested Future Work**
Dual-adversarial generative networks for reversible steganography in medical image security of Internet of Medical Things [31]	Increasing the embedding capacity still comes at the cost of reduced image quality, and the model remains somewhat susceptible to steganalysis detection when larger amounts of data are embedded, reflecting a persistent difficulty in balancing capacity, fidelity, and detectability.	Planned work aims to refine the model so its security can be strengthened without sacrificing the practical usability of the medical images it protects.
Lightweight DWT Steganography with ECC-ChaCha20 for Secure Medical IoT Systems [32]	1. The wavelet-domain embedding needs careful synchronization during extraction and stays sensitive to geometric distortions, a weakness that shows up experimentally as a somewhat higher bit error rate whenever stego images are rotated or translated. 2. The ECDH key exchange used to derive the shared encryption secret is open to man-in-the-middle attacks unless an additional authentication layer is added on top of it. 3. Deploying the ECC component becomes more complex on constrained devices that lack dedicated ECC library support. 4. The ChaCha20 cipher carries extra overhead for managing its nonce values and offers only limited support for hardware acceleration.	1. Planned extensions include adding perceptual-aware modulation of the payload together with adaptive scheduling of the encryption keys. 2. The team also intends to explore deep learning based encoder-decoder architectures that would allow embedding within a learned feature domain instead of fixed wavelet coefficients. 3. Adopting authenticated encryption schemes such as AEAD constructions is being considered so that confidentiality and integrity can be guaranteed together. 4. Further plans involve investigating public-key steganographic primitives and testing real-time performance through hardware-in-the-loop simulation to broaden the framework's use across more operational settings.
A Novel Image Steganography Method for Industrial Internet of Things Security [35]	No limitations were explicitly stated in the paper.	1. Exploring other metaheuristic optimization algorithms is planned as a way to speed up the computation involved in mobile edge computing scenarios within the IoT. 2. Combining the integer wavelet transform with pixel value differencing schemes is being considered for future development of the method. 3. Extending the approach to work with color images rather than only grayscale is identified as another direction going forward.
Optimal Deep Learning Model Enabled Secure UAV Classification for Industry 4.0 [56]	No limitations were explicitly stated in the paper.	Improving the classification performance further by applying hybrid deep learning methodologies is identified as a direction for future work.

(Continued)

Table 5 (continued)

Steganography in IoT		
Literature Title	**Limitations/Gaps**	**Suggested Future Work**
Enhancing privacy in data transmission between IoT devices: A robust encryption and embedding framework for secure and meaningful image communication [57]	Converting the ciphertext image into a meaningful image causes the resulting image to grow in size, roughly doubling to 2X the size of the original plaintext image, so an M × N plaintext image ends up producing a 2M × 2N meaningful ciphertext image.	Considering an alternative approach that relies on bit-planes rather than DWT when embedding the encrypted information into another plaintext image, with the goal of preserving the size of the meaningful ciphertext image while still resolving the size-expansion issue.
IoTSLE: Securing IoT systems in low-light environments through finite automata, deep learning and DNA computing based image steganographic model [58]	No limitations were explicitly stated in the paper.	1. Adopting data compression techniques is planned so that larger secret message files can be embedded within the same payload, as long as overall efficiency is preserved. 2. Combining encryption together with the steganography process is being considered as a way to meaningfully strengthen security, particularly for IoT settings.
Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework [59]	1. Scalability is a concern because the study only tested 256 × 256 cover images, so its performance on higher resolution images still needs to be confirmed. 2. Running the optimization raises the embedding time as the embedding rate increases, which makes the approach impractical for real-time use despite the efficiency gains it provides. 3. The imperceptibility of the method is strong, but its resistance to steganalysis attacks specifically has not been thoroughly examined and needs closer scrutiny.	1. Designing an embedding mechanism that adapts to the complexity of the image is proposed as a way to improve both imperceptibility and security together. 2. Applying deep learning based detection models to identify vulnerabilities under steganalysis attacks, and then closing those security gaps, is suggested as a next step. 3. Extending the method with high resolution support and optimized algorithms is planned so it can be used in real-time steganographic applications.

(Continued)

Table 5 (continued)

Steganography in IoT		
Literature Title	**Limitations/Gaps**	**Suggested Future Work**
SmartSteganogaphy: Light-weight generative audio steganography model for smart embedding application [60]	1. The spectrogram results show that the model spreads the secret across the entire area of the figure, which may make the secret easier to be discovered. 2. Compared with traditional audio steganography methods, the SNR of the proposed method is relatively low, though it comes with an increase of almost 0.8 in embedding capacity. 3. Training the encoder to fool the steganalyzer during adversarial training does not guarantee the method can counter an independent steganalyzer, since the GAN training strategy limits how much the discriminator can influence this outcome. 4. Under a Gaussian noise attack, normal training causes secret recovery to weaken, while training with added noise restores secret recovery but reduces the fidelity of the steganographic audio itself.	1. Investigating some adaptive method as a further direction. 2. Exploring how to strike a better balance between the three losses that make up the encoder loss, namely the decoder loss and the steganalyzer loss, as a separate research direction.
RLL-SWE: A Robust Linked List Steganography Without Embedding for intelligence networks in smart environments [61]	1. The scheme is comparatively weak against rotation attacks, with accuracy stated by the authors to top out at 85% (though their reported data reaches 87.42%), noticeably lower than its resistance to noise, filtering, and compression attacks, attributed to the small 3×3 window size used relative to the overall image size. 2. Message restoration accuracy shows a prolonged decreasing trend as the segment length grows from 10 to 15 bits, and drops sharply once the length increases past 16 bits. 3. Using a larger step length together with heavier sampling shrinks the resulting feature map considerably, which causes the search algorithm's success rate to fall off sharply, so the step length has to be kept small to keep the search effective.	1. Further optimizing the technique's performance. 2. Exploring the method's application across a wider range of real-world scenarios to provide a more complete solution for security management in smart environments.

(Continued)

Table 5 (continued)

Steganography in IoT		
Literature Title	**Limitations/Gaps**	**Suggested Future Work**
A Shuffling-Steganography Algorithm to Protect Data of Drone Applications [62]	1. The amount of data that can be hidden within the text cover stays fairly small, so this needs to be factored into the choice of segmentation pattern, or a very long text with many punctuation marks needs to be used instead. 2. Hidden data within the image cover can be affected if the image undergoes modification or compression, since the approach is built on the spatial-domain LSB technique rather than a frequency-domain one. 3. The approach depends on both parties agreeing beforehand on three separate secrets, namely the encryption key and two patterns, one used for the text-hiding stage and the other for the image-embedding stage.	1. Combining the method with the KASHIDA technique to fit more data into the text cover without weakening the level of protection. 2. Designing an algorithm that derives the two patterns directly from the encryption key itself, so the sender and receiver no longer need to agree on them separately. 3. Looking into other ways of hiding data in text, such as adding dummy data or reordering the encrypted secret data. 4. Testing the automated pattern-generation algorithms in real agricultural drone deployments to confirm they hold up in practical conditions.
Encryption with Image Steganography Based Data Hiding Technique in IoT Environment [63]	No limitations were explicitly stated in the paper.	Future improvements to the EIS-DHT technique are expected to come from applying hybrid metaheuristic algorithms to the optimal pixel selection step.
Hiding information in encrypted images with (t, n) secret sharing for IoT and cloud services [64]	The scheme's larger embedding capacity comes with a cost of higher computational overhead, since its theoretical time complexity is not optimal compared to some other secret sharing methods.	Future work aims to explore the scalability of this secret sharing approach in multi-party computation cloud environments to further improve both security and efficiency across a wider range of practical applications.
A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography [65]	No limitations were explicitly stated in the paper.	Future plans include testing the proposed EAST method within an actual real-time IoV setting and benchmarking it against a wider range of encryption and decryption techniques across different text and multimedia formats, continuing toward more accurate, efficient, and secure IoV communication solutions.
Protecting health data in the cloud through steganography: A table-driven, blind method using neural networks and bit-shuffling algorithm [66]	No limitations were explicitly stated in the paper.	Future plans involve embedding additional biodata into media used by common smart devices such as smart cards and watches, and combining different media types like DNA sequences, ECG, and EEG signals to hide personal and medical secrets within hybrid media content.

(Continued)

Table 5 (continued)

Steganography in IoT		
Literature Title	**Limitations/Gaps**	**Suggested Future Work**
Novel Self-sufficient Coverless Video Steganography for Secured Internet of Things (IoT) Communication [67]	Matching accuracy in the hash-based mapping step can be affected by inherent video factors such as scene content, background, and animation characteristics, so a complete match for every secret information segment cannot be guaranteed without the added synthesis step to fill in missing sequences.	Further testing in an actual Internet of Things environment with constrained computing resources is still needed to properly evaluate the method's real-world performance.
Privacy-preserving in the Internet of Things based on steganography and chaotic functions [68]	The initial key for the chaos function is generated from the block center pixel values, so if even a single bit changes during data transmission the key itself changes, causing the hidden secret data to be lost rather than exposed, and this loss is treated as an acceptable trade-off since it is considered preferable to disclosure of the secret information.	No future work was explicitly stated in the paper.
SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT [69]	No limitations were explicitly stated in the paper.	No future work was explicitly stated in the paper.
Invertible generative speech hiding with normalizing flow for secure IoT voice [70]	1. During the extraction process a small amount of noise is introduced at high frequencies, causing minor differences between the original secret speech and the extracted secret speech, although this does not affect the perceived speech quality. 2. Choosing between the two available vocoders involves a trade-off, since the higher-quality vocoder comes with a considerably larger model size while the lightweight, resource-friendly vocoder option carries a slightly reduced level of speech quality.	Future work will incorporate common noise attacks into the training pipeline to improve the robustness of the hiding method.

A capacity-quality-detectability trade-off appears repeatedly among the surveyed entries. He et al. [31] note that increasing the embedding capacity of their DAS-GAN framework comes at the cost of reduced image quality and greater susceptibility to steganalysis, reflecting a tension the authors describe as persistent rather than fully resolved. Jiang et al. [60] report a related issue for their audio-based SmartSteganogaphy model, where the spectrogram of the stego signal spreads the secret across the entire time-frequency plane, potentially making it easier to detect, while the model's SNR remains lower than that of traditional audio steganography methods despite an accompanying gain in embedding capacity. Rajan and Ganesh [59] identify a comparable concern for their optimization-driven pixel shuffling scheme, whose strong imperceptibility has not yet been paired with a thorough evaluation against steganalysis attacks specifically. Ge et al. [70] report a milder version of this trade-off, noting that their two available vocoder options force a choice between a larger, higher-quality model and a lighter, resource-friendly one that sacrifices a small amount of speech quality, alongside minor high-frequency noise introduced during extraction that does not noticeably affect perceived quality.

Key management and protocol-level vulnerabilities form a second recurring concern. Sethi et al. [32] identify several such issues in their ECC-ChaCha20 framework, including susceptibility of the ECDH key exchange to man-in-the-middle attacks without an added authentication layer, added deployment complexity on devices lacking native ECC library support, and nonce management overhead in the ChaCha20 cipher that limits hardware acceleration. Alkodre et al. [62] report a different flavor of the same problem, since their shuffling steganography approach depends on both communicating parties pre-agreeing on three separate secrets, namely the encryption key and two segmentation patterns, before any secure exchange can take place. Rostam et al. [68] describe an intentional design trade-off rather than an oversight, where a single bit change during transmission alters the chaos function's derived key enough that the hidden data is lost rather than exposed, a failure mode the authors frame as preferable to disclosure even though it limits reliability under noisy channels.

Robustness against specific classes of attack also varies considerably across the surveyed methods, and several authors are transparent about where their techniques fall short. Zhao et al. [61] report that their RLL-SWE scheme is comparatively weak against rotation attacks. Although the authors textually state that accuracy tops out at 85%, their reported data shows a peak of 87.42%, which remains noticeably lower than its resistance to noise, filtering, or compression, a limitation they attribute to the small window size used relative to the overall image. The same authors also note that restoration accuracy declines steadily as the message segment length grows past 15 bits, and that increasing the step length or sampling rate to speed up processing causes the underlying search algorithm's success rate to fall sharply. Sethi et al. [32] similarly acknowledge that their wavelet-domain embedding remains sensitive to geometric distortion, showing a somewhat higher bit error rate under rotation and translation compared to other tested attacks. Alkodre et al. [62] add that because their image-embedding stage relies on spatial-domain LSB modification rather than a frequency-domain technique, the hidden data can be disrupted if the carrier image undergoes compression or other modification during transmission.

Scalability and real-time practicality represent a further gap identified across several entries. Rajan and Ganesh [59] report that their method was tested only on 256 by 256 cover images, leaving its behavior at higher resolutions unconfirmed, and that embedding time increases alongside the embedding rate to a degree that limits practical real-time use despite otherwise strong efficiency. Lin et al. [64] note that the larger embedding capacity achieved through their secret sharing scheme comes with higher computational overhead, since its theoretical time complexity does not match more optimized alternatives. Calo et al. [67] observe that the matching accuracy of their coverless video steganography approach can be affected by inherent video properties such as scene content and background complexity, meaning a complete hash match

for every secret segment cannot be guaranteed without the synthesis step that fills in missing sequences. Shafique et al. [57] report a more structural limitation, where converting an encrypted image into a visually meaningful one roughly doubles its dimensions relative to the original plaintext image, an expansion that carries direct implications for storage and transmission bandwidth on constrained IoT links.

A notable pattern in this body of work is how unevenly limitations are reported across the surveyed literature. Several works, including those by Hassaballah et al. [35], Alissa et al. [56], Mukherjee et al. [58], Ragab et al. [63], Rathore et al. [65], Nahar et al. [66], and Dhawan et al. [69], do not explicitly state any limitations, despite reporting strong quantitative results elsewhere in their respective papers. This asymmetry makes it difficult to judge how these methods might behave outside the specific conditions under which they were evaluated, and it stands in contrast to entries such as Sethi et al. [32], Jiang et al. [60], and Zhao et al. [61], which offer detailed, multi-point self-assessments covering both algorithmic and deployment concerns. A more consistent norm of transparent limitation reporting across the field would make it considerably easier to judge which methods are genuinely closer to real-world readiness.

Despite this unevenness in self-reported limitations, the suggested future work converges on a fairly consistent set of priorities. Several authors point toward hybrid or adaptive optimization as a next step, including Hassaballah et al. [35], who propose exploring additional metaheuristic algorithms for faster mobile edge computation, and Rajan and Ganesh [59], who suggest an embedding mechanism that adapts to image complexity to jointly improve imperceptibility and security. Others emphasize deeper integration of learning-based components, such as Sethi et al. [32], who plan to explore encoder-decoder architectures operating in a learned feature domain rather than fixed wavelet coefficients, and Mukherjee et al. [58], who intend to combine encryption more tightly with their steganographic pipeline. A third recurring theme is validation under realistic operating conditions, reflected in Alkodre et al.'s [62] plan to test their pattern-generation algorithms in real agricultural drone deployments, Calo et al.'s [67] call for further testing within an actual resource-constrained IoT environment, and Rathore et al.'s [65] intention to benchmark their EAST method within a live Internet of Vehicles setting. Ge et al. [70] contribute a related direction specific to the audio domain, planning to incorporate common noise attacks directly into the training pipeline to improve robustness rather than treating noise resilience as a purely post-hoc evaluation step. Two entries in the table, those by Rostam et al. [68] and Dhawan et al. [69], do not state any future work, leaving open questions about their respective key-loss trade-off and their untested robustness against steganalysis without a clearly articulated path forward.

Overall, these limitations and future directions suggest that IoT steganography research has matured considerably in demonstrating imperceptibility and basic security under controlled conditions, but that formal robustness guarantees, consistent self-reported limitations, and validation under realistic multi-device deployment remain the areas most in need of continued attention. Closing these gaps will likely depend on the field adopting more uniform reporting practices for limitations, alongside broader dataset standardization and hardware validation.

4.4 Comparative Performance across Operational Metrics

This subsection compares steganographic methods for IoT across several practical performance dimensions, including memory and storage, computational time, processing speed, energy consumption, data overhead, embedding capacity, image quality, and robustness. Metrics are grouped into a shared table only where the underlying unit and measurement are genuinely comparable across studies. Where a metric is reported by very few methods, uses inconsistent units, or measures conceptually different things despite a shared name, it is discussed directly in the text instead.

Memory and storage are reported by only two methods, and the two figures describe different things. Sethi et al. [32] report runtime memory consumption of 38.00 to 49.14 MB, the RAM occupied while their ECC-ChaCha20 and wavelet-domain scheme executes, a range modest enough to run comfortably on most embedded Linux platforms with more than 64 MB of available RAM. Jiang et al. [60] instead report a stored model size under 5 MB for their SmartSteganogaphy network, a figure small enough to fit on flash-constrained microcontrollers where Sethi et al.'s runtime footprint would not necessarily apply, since the two numbers measure disk footprint and active execution memory respectively. Taken together, the two results suggest that both classical signal-processing pipelines and compact neural models can be made to fit within the memory budgets typical of mid-range IoT hardware, though the very small number of methods reporting either figure makes it difficult to say how representative these two cases are of the field as a whole.

Reported computational time spans several orders of magnitude, from Rathore et al.'s [65] sub-millisecond EAST encryption to embedding stages exceeding thirty seconds in Hassaballah et al. [35] and Ragab et al. [63], both dependent on iterative pixel search within a wavelet transform. Part of this spread reflects genuine algorithmic differences, but part is confounded by hardware, since Ge et al. [70] needed an RTX 4090 GPU to reach millisecond-scale latency, with the same method slowing to over two seconds on CPU alone, a nearly hundredfold difference driven entirely by hardware rather than the underlying algorithm. Four of the eight methods in Table 6, namely Hassaballah et al. [35], Alissa et al. [56], Alkodre et al. [62], and Ragab et al. [63], do not report the hardware used to obtain their timings, which is marked as unspecified rather than assumed. This leaves the thirty-second embedding times reported by Hassaballah et al. and Ragab et al. impossible to attribute confidently to algorithmic cost rather than modest test hardware, and it similarly leaves Alissa et al.'s sub-1.5 s result and Alkodre et al.'s sub-second result without a clear indication of whether they were achieved on desktop-class or genuinely constrained equipment.

Table 6: Computational time and reported hardware configuration across IoT steganography methods.

Method	Application Area	Computational Time	System/Hardware Used
HHO-IWT [35]	Industrial IoT	Embedding 34.14–35.35 s; Extraction 18.76–19.36 s	Unspecified
CSODL-SUAVC [56]	UAV/Industry 4.0	1.115–1.448 s	Unspecified
Visually meaningful encryption [57]	IoT image transmission	0.0018–0.0033 s	Intel i5 CPU (2.45 GHz), 16 GB RAM
HLSB + RC4 + Cheetah Optimizer [59]	General IoT data security	Embedding 0.0153–0.0390 s; Extraction 0.5329–0.6256 s	Intel Core i7-9700K CPU, 16 GB RAM, NVIDIA GTX 1660 Ti
SSA [62]	Drone applications	Execution 0.35–0.40 s	Unspecified
EIS-DHT [63]	Industrial IoT	Embedding 33.75–35.06 s; Extraction 17.82–18.85 s	Unspecified
EAST [65]	Internet of Vehicles	0.083–0.334 ms	Unspecified
SecFlow speech hiding [70]	Voice-controlled IoT	Embedding 0.017–0.035 s (GPU)/1.28–2.44 s (CPU)	NVIDIA RTX 4090 GPU, Intel i9-14900K CPU

A further five methods report their test hardware without pairing it to any computational time figure, leaving the specification effectively orphaned from a performance number. He et al. [31] state their DAS-GAN model was deployed on a Raspberry Pi 4B with a 1.5 GHz quad-core ARM Cortex-A72 processor and 4 GB of RAM, confirming feasibility on constrained hardware without reporting a corresponding latency

figure that would show how quickly the model actually runs on that device. Lin et al. [64] report an AMD Ryzen 7 5800H system, Nahar et al. [66] report a 3 GHz desktop with 16 GB of RAM, and Rostam et al. [68] report an older Intel Core 2 Duo laptop with 4 GB of RAM, all of which are considerably more capable than typical IoT edge nodes yet none of which is accompanied by a stated processing time to indicate how that capability translates into actual speed. Dhawan et al. [69] similarly mention only an 8 GB RAM environment without further detail.

Processing speed, distinct from raw embedding or extraction time, is reported by only two methods using incompatible units. Calo et al. [67] report 0.00007 s per byte for coverless video steganography, measured on an Intel Core i7 system with a GTX 1050 GPU, a rate that would allow a one-megabyte payload to be processed in roughly 70 milliseconds. Ge et al. [70] instead report a real-time factor of 0.572 to 0.577, comparing processing time to audio playback duration rather than data volume, meaning their SqueezeWave configuration generates stego speech in just over half the time it takes to play back, which is fast enough to support streaming voice communication without a perceptible buffering delay. Both results indicate that their respective methods are fast enough for near real-time IoT communication, though the video-oriented per-byte rate and the audio-oriented real-time factor answer different practical questions and cannot be converted into one another.

Energy consumption is reported by only one method, Sethi et al. [32], at 78.20 to 104.28 mW for their ECC-ChaCha20 and DWT configuration as message size increases from 32 to 8192 bytes. This range sits well within the power budget of many battery-operated microcontroller platforms, which commonly draw tens to a few hundred milliwatts during active operation, suggesting the method itself would not be the dominant drain on a typical IoT sensor's battery life. No other surveyed method reports a comparable power draw figure, so it is not possible to say whether this result is representative of steganographic methods generally or specific to the lightweight cipher and wavelet combination Sethi et al. selected.

Data overhead is mentioned by three methods but in forms that describe different relationships between input and output size. Nahar et al. [66] report a maximum expansion rate of 50% for their DNA sequence relative to the original message, meaning a fully expanded encoding could nearly double the space needed to store or transmit the hidden data. Rathore et al. [65] report that their EAST cover must be roughly 1.9 times the size of the secret file, a similar near-doubling but measured as a cover-to-secret ratio rather than a message expansion rate, evaluated across secret file sizes of 10, 20, and 40 kilobits. Shafique et al. [57] report the largest overhead of the three, since their visually meaningful ciphertext image doubles in both width and height relative to the plaintext, producing a fourfold increase in pixel count for an $M \times N$ image mapped to $2M \times 2N$. All three figures point toward the same practical concern for bandwidth-limited IoT links, namely that stronger visual concealment or biological encoding tends to come with a substantial increase in transmitted data volume.

Four methods report embedding capacity in bits per pixel, allowing direct comparison in Table 7, where Lin et al. [64] report the highest average capacity at 4 bpp and He et al. [31] report the widest range, from 0.9453 up to 3.3704 bpp as embedding rate increases across their four tested payload levels. Mukherjee et al. [58] and Rostam et al. [68] report fixed capacities of 2.67 and 1.5 bpp respectively, both comfortably within the range spanned by the other two methods, indicating that low-light image steganography and chaos-based blocking are not systematically more or less capacity-limited than the reversible and secret-sharing approaches at either end of the table. Several other methods report capacity in units that do not translate cleanly into bits per pixel. Hassaballah et al. [35] and Ragab et al. [63] report capacity as a percentage of image resolution, reaching up to 50% and 17.37% respectively, Zhao et al. [61] report 10 to 14 bits per message segment independent of a fixed bpp rate, and Nahar et al. [66] report 1 bit per DNA nucleotide, a

unit specific to their biological encoding scheme and considerably lower than the image-based figures once the difference in medium is taken into account.

Table 7: Embedding capacity reported in bits per pixel across IoT steganography methods.

Method	Application Area	Capacity (bpp)
DAS-GAN [31]	Medical IoMT	0.9453–3.3704
IoTSLE [58]	Low-light IoT	2.67
(t, n) secret sharing RDHEI [64]	IoT/cloud sharing	4.0 (average)
Chaos-based image blocking [68]	General IoT privacy	1.5

Table 8 lists methods where PSNR compares a stego image to its original cover, so a higher value indicates better imperceptibility. Sethi et al. [32] report the strongest result at up to 75.32 dB, followed by Alkodre et al. [62] near 79 dB and Rajan and Ganesh [59] at up to 61.68 dB, all three well above the 30 to 40 dB range typically considered visually indistinguishable from an unmodified cover. Mukherjee et al. [58] sit at the lower end of the table with a narrow 38.52 to 38.57 dB range, still within an acceptable imperceptibility band but noticeably less headroom above the visual detectability threshold than the top-performing methods, which may reflect the added difficulty of embedding into already low-light, lower-contrast source images. Rathore et al.'s [65] reported figure of 64.31% to 71.58% is preserved exactly as it appears in the source study, carrying a percentage symbol rather than a decibel unit. He et al. [31] and Rostam et al. [68] both show PSNR declining as embedding capacity increases, from 44.32 down to 35.12 dB and from roughly 56 down toward 46 dB respectively, illustrating the same capacity-quality tradeoff across two otherwise very different steganographic designs, one built on a generative adversarial network and the other on chaotic pixel blocking.

Table 8: Embedding and stego image quality (PSNR) across IoT steganography methods.

Method	Application Area	PSNR (Higher = Better Imperceptibility)
DAS-GAN [31]	Medical IoMT	44.32–35.12 dB
ECC-ChaCha20 + DWT [32]	Medical IoT	75.32–61.08 dB
HHO-IWT [35]	Industrial IoT	35.66–52.47 dB
CSODL-SUAVC [56]	UAV/Industry 4.0	57.30–62.45 dB
IoTSLE [58]	Low-light IoT	38.52–38.57 dB
HLSB + RC4 + Cheetah Optimizer [59]	General IoT data security	51.65–61.68 dB
SSA [62]	Drone applications	~67–79 dB
EIS-DHT [63]	Industrial IoT	55.70–56.76 dB
EAST [65]	Internet of Vehicles	64.31–71.58 (reported as %, not dB)
Chaos-based image blocking [68]	General IoT privacy	45.88; ~46–56
SSII [69]	Industrial IoT	~55.91–60.82 dB

Table 9 separates the two methods that report PSNR in the opposite sense, confirming dissimilarity between an encrypted image and its plaintext rather than measuring embedding quality. Shafique et al. [57] and Lin et al. [64] both report values between roughly 6 and 10 dB, with Lin et al.'s range starting slightly

lower at 6.31 dB, indicating marginally stronger dissimilarity between their encrypted shares and the original plaintext than Shafique et al. achieve with their chaotic map and confusion-diffusion approach. Both results sit far below the 30 dB range considered visually acceptable for embedding-oriented steganography, which is the intended outcome for an encryption stage rather than a shortcoming, since the goal in both cases is to make the encrypted output as statistically unlike the original as possible.

Table 9: Encryption dissimilarity (PSNR) across IoT steganography methods.

Method	Application Area	PSNR (lower = stronger encryption)
Visually meaningful encryption [57]	IoT image transmission	6.76–9.56 dB
(t, n) secret sharing RDHEI [64]	IoT/cloud sharing	~6.31–8.74 dB

SSIM values largely parallel the PSNR results already discussed, since the two metrics are reported by the same methods and follow the same relative ordering. Rajan and Ganesh [59] and Dhawan et al. [69] report the highest SSIM values, both exceeding 0.999, consistent with their strong PSNR results above and indicating near-perfect structural preservation between cover and stego image even at higher payloads. He et al. [31] and Hassaballah et al. [35] show SSIM declining alongside PSNR as embedding capacity increases, from 0.9902 down to 0.9433 on ADNI and from 0.9095 up to 0.9988 depending on the number of embedded bits respectively, reinforcing the same capacity-quality tradeoff observed in the PSNR results. Mukherjee et al. [58] report a comparatively tight SSIM range of 0.9884 to 0.9990, again mirroring their narrow PSNR band and suggesting that their low-light embedding method behaves consistently across the tested payload sizes rather than degrading sharply at higher capacities.

Only one method, Lin et al. [64], reports SSIM in the encryption-dissimilarity sense, with an average value between 0.0046 and 0.0100 across their encrypted shares on BOSSbase, BOW-2, and Osirix. This near-zero result is consistent with the same authors' correspondingly low PSNR values reported in Table 9, together confirming that their encrypted output bears almost no structural resemblance to the original plaintext image, which is the desired property for a secret-sharing scheme intended to withstand direct visual or statistical comparison against the source.

Four methods report robustness under simulated attacks, summarized in Table 10. Sethi et al. [32] report the tightest bit error rate range at 0.012 to 0.027 across six distinct attack types, with JPEG compression at quality 50 producing the lowest error and 10 degree rotation producing the highest, suggesting their wavelet-domain embedding is somewhat more resilient to compression than to geometric distortion. Zhao et al. [61] report a comparable pattern using a different metric, restoration accuracy, which stays above 98% under Gaussian noise, salt and pepper noise, and JPEG compression but falls to 87.42% at 5 degrees of rotation and further down to 66.40% at 30 degrees, again showing geometric distortion as the harder case relative to pixel-level noise. Hassaballah et al. [35] and Ragab et al. [63] apply an overlapping attack set spanning erosion, dilation, and three types of noise, and both recover normalized cross-correlation values above 0.95 alongside PSNR figures in the low-to-mid 20s and low 30s decibel range, indicating that some visible degradation remains after these attacks even though the underlying secret data proves recoverable. Because Sethi et al. and Zhao et al. use different rotation severities and different reporting metrics, and because Hassaballah et al. and Ragab et al. report structural and correlation-based results rather than accuracy or bit error rate, the four methods cannot be ranked against one another on a single robustness scale, even though each individually demonstrates measurable resistance to the specific attacks it was tested against.

Table 10: Reported robustness under signal attacks across IoT steganography methods.

Method	Attacks Tested	Reported Result Range
ECC-ChaCha20 + DWT [32]	Gaussian noise, salt & pepper, rotation, translation, blurring, JPEG compression	BER 0.012–0.027
HHO-IWT [35]	Erosion, dilation, Gaussian/salt & pepper/speckle/Poisson noise, motion blur, JPEG compression	NCC 0.9514–1.0000; PSNR 22.68–30.80 dB
RLL-SWE [61]	Gaussian/salt & pepper noise, mean/median filtering, rotation, JPEG compression	Restoration accuracy 66.40%–99.99%
EIS-DHT [63]	Erosion, dilation, Gaussian/salt & pepper/speckle/Poisson noise	NCC 0.9614–1.0000; PSNR ~23.19–31.41 dB

Across all metrics considered, no single method performs best on every dimension. Methods with the strongest imperceptibility, such as Sethi et al. [32] and Alkodre et al. [62], are not the fastest in Table 6, and the fastest methods, such as Rathore et al. [65], report their strongest results elsewhere. Memory, energy, processing speed, and data overhead remain the least consistently reported dimensions despite being the most directly tied to constrained IoT hardware, and computational time figures are frequently missing the hardware context needed to interpret them. Addressing these gaps through standardized hardware reporting, a shared definition of data overhead, and a common attack protocol for robustness testing would substantially improve the comparability of future work in this area.

5 Inferential Take-Away Messages: Key Insights for IoT Steganography Research

The comprehensive analysis of steganographic data hiding approaches for IoT presented in Section 4 reveals several critical insights that shape the future of this field. These take-away messages synthesize the patterns, gaps, and opportunities identified across the eighteen evaluated studies. Fig. 4 outlines a conceptual adaptive security framework that motivates several of the directions discussed below, illustrating how an IoT device might select among robust, hybrid, or lightweight steganography based on device resources, network conditions, and data sensitivity, then continue monitoring the transmitted data through AI-driven steganalysis so that the security policy can be adapted if a threat is later detected.

5.1 Balancing Imperceptibility, Robustness, and Resource Constraints

A central tension in IoT steganography lies between achieving strong imperceptibility or robustness and operating within the severe resource limitations of IoT devices. Optimization-driven methods such as the Harris Hawks [35] and Quantum Black Widow [63] based approaches reviewed in Section 4 achieve high PSNR and reliable recovery under attack, but require embedding times exceeding thirty seconds, a cost whose relationship to the underlying hardware cannot be fully assessed since neither method discloses the platform used for testing. Flow-based generative approaches such as SecFlow [70] similarly depend on GPU acceleration to reach millisecond-scale latency, with the same method slowing by up to roughly 140 times when run on CPU alone rather than GPU. On the other hand, lightweight designs such as the sub-5 MB SmartSteganogaphy model [60] and the low-power ECC-ChaCha20 configuration [32] are explicitly built to minimize model size and power draw, and their robustness evaluation is not uniform even between the two: Jiang et al. [60] uniquely report explicit steganalysis detection accuracy against SRM and CNN classifiers, while Sethi et al. [32] instead cover a broader range of six distinct attack types without testing detector

accuracy directly, so neither lightweight method combines both forms of evidence. Reversible medical image steganography has separately demonstrated feasibility on genuinely constrained hardware through a Raspberry Pi deployment [31], though this method is not itself designed to minimize model size or power draw in the way the two lightweight methods above are, so hardware feasibility and lightweight design remain two distinct properties that do not always co-occur in the surveyed literature. To resolve the underlying resource tension, future embedding architectures should adaptively scale computational cost according to available device resources and payload sensitivity, reserving higher-cost optimization for critical data while defaulting to lightweight embedding elsewhere, in the spirit of the context-driven policy selection illustrated in Fig. 4. The performance variation documented in Section 4.4 confirms that deployment feasibility is not a binary property but a continuum shaped by the interaction between algorithm design, target hardware, and operational environment.

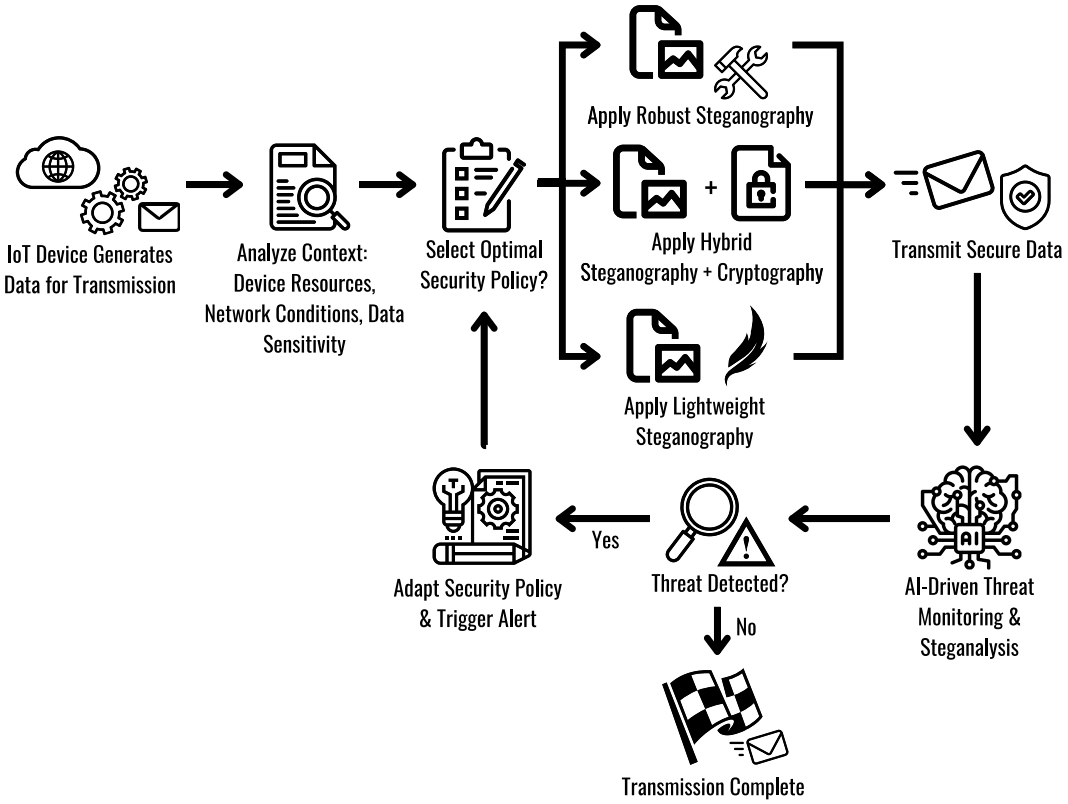

Figure 4: A future adaptive security framework for IoT.

5.2 Addressing the Reproducibility Gap in IoT Steganography Research

The lack of reproducibility across the surveyed literature poses a significant barrier to meaningful comparison. A substantial share of the eighteen reviewed methods rely on unspecified or self-selected datasets rather than named public benchmarks, a pattern already documented in Section 4.2, and several report performance figures without disclosing the CPU, GPU, or embedded platform used to obtain them. USC-SIPI recurs across four of the surveyed studies as a shared public benchmark, while other named datasets such as BOSSbase appear in only a single study, so public benchmark reuse remains the exception rather than a broadly established norm across the field. Most methods instead evaluate on individually chosen test images, generated files, or proprietary data whose scale and diversity are difficult to assess from the reported figures alone. This gap is compounded by inconsistent pairing of performance figures with

hardware context, since Section 4.4 found several methods reporting computational time without stating their test platform, and several others reporting detailed hardware specifications without a corresponding timing figure. Advancing the field will require wider adoption of shared, publicly available datasets, consistent disclosure of the hardware and software environment behind every timing, memory, or energy measurement, and sufficient methodological detail to support independent replication.

5.3 Evolving toward Domain-Specific Embedding Strategies

Application-specific constraints increasingly shape steganographic design choices across the surveyed literature, echoing the deployment heterogeneity discussed in Section 4.1. Medical IoT applications favor wavelet-domain embedding evaluated across increasing payloads on radiograph and neuroimaging data [31,32], though both reported implementations show PSNR declining as payload increases, a capacity-quality tradeoff also noted in Section 4.3 rather than a fully resolved property of the medical domain; He et al. [31] additionally design their framework to be fully reversible so that the original image can be perfectly recovered alongside the embedded data. Industrial IoT communication instead prioritizes robust protection against steganalysis despite the heavier computational cost that optimization-based pixel selection introduces [35], with one design explicitly targeting near real-time secrecy as a stated goal even though its own reported embedding time runs into the tens of seconds [63]. Unmanned aerial and vehicular applications operate under constraints that vary by their specific source: Rathore et al. [65] target the low-latency, high-throughput communication demands of the Internet of Vehicles directly, while Alkodre et al. [62] are instead motivated primarily by the interception risk on the drone-to-station link, and Alissa et al. [56] are motivated by the limited onboard computational capacity of drones to run deep classification models rather than by link bandwidth itself. The surveyed literature demonstrates that a single, domain-blind embedding strategy is unlikely to serve all of these contexts equally well, since a wavelet-domain approach tuned for medical image fidelity does not necessarily meet the timing constraints required for drone or vehicular communication. Future efforts should instead tailor embedding domain, cover medium, and optimization strategy to each application's specific data type, hardware limitations, and latency tolerance. The performance figures collected in Section 4.4 reinforce this point directly, since methods evaluated under medical, industrial, aerial, and vehicular conditions show substantially different trade-offs between imperceptibility, capacity, and speed, precluding the use of one generic steganographic design across all of these domains.

5.4 Toward Intelligent, Adaptive, and Steganalysis-Aware Frameworks

A critical limitation across the reviewed literature is the predominance of static embedding strategies that operate with fixed parameters regardless of the operational context in which they are deployed. While optimization-driven and generative approaches have begun to appear in IoT steganographic systems, their use has largely remained confined to the design stage rather than becoming architecturally central to how the system behaves once deployed. Intelligent pixel selection aimed at minimizing distortion [35,56,63], security-motivated pixel shuffling [59], adaptive payload allocation [69], and adversarial training [31,60] have each measurably improved imperceptibility, capacity, or resistance to attack in individual studies, yet none of the surveyed frameworks adjusts its embedding behavior in response to real-time variables such as fluctuating device resources, network conditions, or evolving steganalysis capability. This gap is visible directly in Section 4.3, where strong imperceptibility results are not always paired with a corresponding evaluation against steganalysis [59], and where scalability to larger images or higher resolutions frequently remains unconfirmed beyond the specific conditions tested. Metaheuristic optimization algorithms have proven effective at locating embedding positions that minimize distortion in several of the surveyed

studies [35,56,63], while the invertible generative framework reviewed for voice-controlled IoT [70] has demonstrated, through distribution-matching rather than adversarial training, the ability to produce stego media whose statistical distribution closely resembles that of unmodified cover data, yet few of the surveyed studies combine optimization-based and learning-based approaches within a single pipeline. What is needed is a shift toward steganographic systems that treat embedding strategy as a dynamic variable rather than a static design choice, in which optimization-based embedding selection is guided by a learned steganalysis-resistance objective rather than imperceptibility alone, echoing the monitor-and-adapt loop shown in Fig. 4. Future frameworks should incorporate lightweight decision layers, trainable on constrained hardware, and should be evaluated not only on peak imperceptibility metrics but on their behavioral consistency and resilience under dynamic, realistic IoT deployment conditions as steganalysis techniques themselves continue to advance.

5.5 Sustaining Robustness across Deployment Lifecycles

Several of the surveyed methods depend on design choices that behave predictably under the specific conditions tested but that could plausibly degrade under channel conditions those tests did not cover. Key derivation schemes that regenerate a chaotic seed directly from cover-image pixels lose the hidden message entirely if even a single bit changes during transmission [68], a failure mode its authors present as an acceptable tradeoff against disclosure but one that nonetheless limits reliability on noisy channels. Cryptographic key-exchange protocols embedded within other frameworks remain vulnerable to interception without an additional authentication layer [32], and the same wavelet-domain embedding method shows a measurably higher error rate under rotation than under any of the other five attack types it was tested against [32]. None of the surveyed studies directly tested behavior over an extended deployment period, so it remains an open and untested question, rather than an established finding, whether these single-condition vulnerabilities compound as channel noise, geometric misalignment, and the sophistication of interception attempts evolve over a device's operational life. Future work should incorporate embedding schemes that degrade gracefully rather than failing completely under transmission errors, authentication layers added alongside existing key-exchange protocols, and periodic re-evaluation against newly published attacks rather than a single benchmark performed once at design time.

5.6 Strategic Priorities for Future Research

Based on these observations, several strategic directions emerge for advancing IoT steganography research. Standardized hardware and software reporting should become a baseline expectation for every timing, energy, or memory measurement, so that genuine algorithmic gains can be distinguished from differences in test infrastructure. Steganographic methods must evolve to defend against active, adaptive steganalysis rather than static detectors, extending the adversarial training strategies already demonstrated in two of the surveyed works [31,60] and the distribution-matching objectives demonstrated through invertible generative modeling [70] to a broader share of the field. A shared, common attack protocol covering geometric distortion alongside the more commonly tested noise and compression attacks would allow robustness claims to be compared directly across methods rather than read in isolation, as would a consistent unit convention for embedding capacity across image, audio, video, and biological media. Moving evaluation beyond desktop or single-board simulation toward validation on genuine multi-device IoT testbeds, following the direction already taken by the one surveyed study validated on constrained embedded hardware [31], is essential to confirm that the strong imperceptibility and robustness figures reported throughout this survey continue to hold under real deployment conditions. Proactively designed, resource-aware steganographic frameworks, evaluated consistently across these dimensions, are essential to ensure the safe and efficient use of covert communication in future IoT systems.

6 Conclusion

This survey has comprehensively analyzed the current landscape of steganographic data hiding for IoT, examining eighteen recent methods spanning medical imaging, industrial and Industrial IoT communication, unmanned aerial vehicles, voice-controlled devices, vehicular networks, and cloud-based health data. Notable advancements have been achieved in imperceptibility, embedding capacity, and resistance to common signal distortions, with several surveyed methods reporting PSNR values reaching above 60 dB [59,69] and SSIM values remaining above 0.99 even at nontrivial embedding payloads [59,63,69]. Despite this progress, critical challenges remain. A significant portion of the reviewed studies suffer from reproducibility issues, arising from undisclosed or self-selected datasets and inconsistent reporting of the hardware or software environment used for evaluation. Furthermore, several of the most capacity-efficient methods depend on iterative optimization or GPU-accelerated generative synthesis that exceeds the computational budget of genuinely constrained IoT devices, limiting their practical deployment without dedicated hardware acceleration. This survey addressed deployment feasibility directly by evaluating the surveyed methods against concrete operational metrics in Section 4.4, including memory and storage requirements, computational time, processing speed, energy consumption, and data overhead, providing a basis for assessing practical viability across heterogeneous IoT hardware. The heterogeneity of IoT application domains presents a further challenge, since medical, industrial, aerial, and vehicular deployments each impose different combinations of latency, payload, and fidelity requirements that no single steganographic design satisfies equally well. While emerging techniques such as coverless steganography [67] and invertible generative embedding [70] show clear promise, they require further testing on constrained hardware and evaluation against a broader and more consistent set of adversarial attacks before they can be considered viable at scale. Sustaining robustness across long deployment lifetimes, particularly against key-loss failure modes [68], unauthenticated key exchange [32], and evolving steganalysis capability, also remains insufficiently explored across the surveyed literature, since none of the eighteen studies reviewed here tested behavior under sustained, extended-duration deployment conditions.

To address these challenges, future research must prioritize several key directions. First, standardized benchmarks and public datasets tailored for IoT steganography are essential for meaningful comparison and reproducibility, alongside consistent reporting of the hardware platform behind every performance figure. Second, lightweight and adaptive embedding frameworks, of the kind conceptually outlined in Fig. 4, must be designed to balance imperceptibility against computational efficiency across heterogeneous devices, rather than optimizing for imperceptibility alone at the cost of deployability. Third, domain-specific optimization is essential, since solutions tailored to medical imaging fidelity, industrial latency budgets, and aerial or vehicular bandwidth constraints will outperform generic designs applied uniformly across these contexts. Fourth, closer integration of optimization-driven pixel selection with steganalysis-aware learning objectives, evaluated under a shared set of geometric, noise, and compression attacks, will strengthen robustness claims that currently cannot be compared directly across studies. Lastly, sustaining embedding and key-derivation robustness across long-lived deployments, rather than validating only against a single design-time benchmark, should be treated as a core design requirement rather than an afterthought. By aligning research with these priorities, the IoT steganography community can move toward more comparable, deployable, and resilient covert communication solutions.

Acknowledgement: The authors thank all members of the Cyber Security Research Group, Net-Centric Computing Laboratory, Department of Informatics, ITS, for their support and discussion. The authors declare that AI is used to check grammar and spelling.

Funding Statement: This research is funded by the Indonesian Endowment Fund for Education (LPDP) on behalf of the Indonesian Ministry of Higher Education, Science and Technology and managed under the EQUITY Program (Contract No 4299/B3/DT.03.08/2025 & No 3029/PKS/ITS/2025).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Rafif Aydin Ahmad, Ntivuguruzwa Jean De La Croix, Tohari Ahmad, Kambombo Mtonga, and Mungwarakarama Irenee; methodology, Rafif Aydin Ahmad, Ntivuguruzwa Jean De La Croix, Tohari Ahmad, Kambombo Mtonga, and Mungwarakarama Irenee; formal analysis, Rafif Aydin Ahmad, Ntivuguruzwa Jean De La Croix; investigation, Rafif Aydin Ahmad, Ntivuguruzwa Jean De La Croix; writing—original draft preparation, Rafif Aydin Ahmad; writing—review and editing, Ntivuguruzwa Jean De La Croix, Reynandriel Pramas Thandya, Tohari Ahmad, Kambombo Mtonga, and Mungwarakarama Irenee; visualization, Reynandriel Pramas Thandya; supervision, Tohari Ahmad; project administration, Tohari Ahmad; funding acquisition, Tohari Ahmad. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Vagas M, Majercak O. Usage of IoT devices as progressive technology in the era of digitization: case study. IFAC-PapersOnLine. 2024;58(9):79–84. doi:10.1016/J.IFACOL.2024.07.375.
2. Driss M, Berriche L, Atitallah SB, Rekik S. Steganography in IoT: a comprehensive survey on approaches, challenges, and future directions. IEEE Access. 2025;13(3):74844–75. doi:10.1109/ACCESS.2025.3564120.
3. Manjunath K, Ramaiah GNK, GiriPrasad MN. Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies. Digit Signal Process. 2022;122(25):103335. doi:10.1016/J.DSP.2021.103335.
4. Abood EW, Abdullah AM, Sibahee MAA, Abduljabbar ZA, Nyangaresi VO, Kalafy SAA, et al. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bull Electr Eng Inform. 2022;11(1):185–94. doi:10.11591/eei.v11i1.3279.
5. Kar DC, Mulkey CJ. A multi-threshold based audio steganography scheme. J Inf Secur Appl. 2015;23(3–4):54–67. doi:10.1016/J.JISA.2015.02.001.
6. Wu J, Chen B, Luo W, Fang Y. Audio steganography based on iterative adversarial attacks against convolutional neural networks. IEEE Trans Inf Forensics Secur. 2020;15:2282–94. doi:10.1109/TIFS.2019.2963764.
7. Lee CF, Chan KC. A novel dual image reversible data hiding scheme based on vector coordinate with triangular order coding. IEEE Access. 2024;12:90794–814. doi:10.1109/ACCESS.2024.3421545.
8. Shastri S, Thanikaiselvan V. Interpolation based dual image reversible data hiding using trinary encoding. Multimed Tools Appl. 2024;83(1):349–66. doi:10.1007/s11042-023-15574-9.
9. Yao H, Qin C, Tang Z, Tian Y. Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. Signal Process. 2017;135(8):26–35. doi:10.1016/J.SIGPRO.2016.12.029.
10. Lu TC, Lu YC, Vo TN. Dual-image based high image quality reversible hiding scheme with multiple folding zones. Multimed Tools Appl. 2019;78(24):34397–435. doi:10.1007/S11042-019-07904-7.
11. Lee CF, Chan KC. Improved dual-image quality with reversible data hiding using translocation and switching strategy. Comput Syst Sci Eng. 2022;44(2):1551–66. doi:10.32604/CSSE.2023.026294.
12. Zhang X, Han S, Huang W, Fu D. A generative image steganography based on disentangled attribute feature transformation and invertible mapping rule. Comput Mater Contin. 2025;83(1):1149–71. doi:10.32604/cmc.2025.060876.

13. Yi X, Yang K, Zhao X, Wang Y, Yu H. AHCM: adaptive Huffman code mapping for audio steganography based on psychoacoustic model. IEEE Trans Inf Forensics Secur. 2019;14(8):2217–31. doi:10.1109/TIFS.2019.2895200.
14. Ali AH, George LE, Zaidan AA, Mokhtar MR. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimed Tools Appl. 2018;77(23):31487–516. doi:10.1007/S11042-018-6213-0.
15. Chaharlang J, Mosleh M, Heikalabad SR. A novel quantum audio steganography–steganalysis approach using LSFQ-based embedding and QKNN-based classifier. Circuits Syst Signal Process. 2020;39(8):3925–57. doi:10.1007/S00034-020-01345-6.
16. Srinivasan K, Gowthaman T, Kanakaraj J. A novel copyright marking approach using steganography and robust RSA asymmetric-key cryptographic technique in audio files. J Discret Math Sci Cryptogr. 2017;20(8):1563–71. doi:10.1080/09720529.2017.1402575.
17. Kwak M, Cho Y. A novel video steganography-based botnet communication model in telegram SNS messenger. Symmetry. 2021;13(1):84. doi:10.3390/sym13010084.
18. Al-Mallah RN, Al-Jammas MH. Adaptive steganography based on motion vectors for H.264/AVC. Cyber Secur Appl. 2025;3(2):100109. doi:10.1016/J.CSA.2025.100109.
19. Mashkour MM, Jawad LM, Sulong G. A secure data hiding for H.264 video based on chaotic map methods and RC4 algorithm. Iraqi J Inf Commun Technol. 2023;6(3):50–64. doi:10.31987/IJICT.6.3.250.
20. Kumar N, Lakhani V, Singh K, Bhardwaj M, Raj S. Development of LSB based steganography method for video and image hiding. In: Proceedings of the 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2024; 2024 Mar 14–15; Noida, India. doi:10.1109/ICRITO61523.2024.10522364.
21. Zhang Z, Li Z, Liu J, Yan H, Yu L. Steganography algorithm based on modified EMD-coded PU partition modes for HEVC videos. Eurasip J Image Video Process. 2021;2021(1):1–20. doi:10.1186/S13640-021-00547-5.
22. Abdul-rahman N, Shakir S. Arabic text steganography: literature survey. Al-Furat J Innov Electron Comput Eng. 2024;3(2):1–18. doi:10.46649/fjiece.v3.2.1a.10.5.2024.
23. Majeed MA, Sulaiman R, Shukur Z, Hasan MK. A review on text steganography techniques. Mathematics. 2021;9(21):2829. doi:10.3390/math9212829.
24. Veerashetty S. Secure communication over wireless sensor network using image steganography with generative adversarial networks. Meas Sens. 2022;24(1):100452. doi:10.1016/J.MEASEN.2022.100452.
25. Zaid MA, Hassan S. Survey on modern cryptography. J Kufa Math Comput. 2021;7(1):1–8. doi:10.31642/jokmc/2018/070101.
26. Wu L, Wang XA, Liu J, Su Y, Tu Z, Liu W, et al. Homomorphic encryption for machine learning applications with CKKS algorithms: a survey of developments and applications. Comput Mater Contin. 2025;85(1):89–119. doi:10.32604/cmc.2025.064346.
27. Maity A, Dhara BC. An audio encryption scheme based on empirical mode decomposition and 2D cosine logistic map. IEEE Lat Am Trans. 2024;22(4):267–75. doi:10.1109/TLA.2024.10472959.
28. Eltoukhy MM, Alsubaei FS, Elnabawy YM, Hosny KM. Multiple image encryption techniques: strategies, challenges, and potential future directions. Alex Eng J. 2025;125(2):367–87. doi:10.1016/j.aej.2025.04.006.
29. Prasad S, Singh AK. Survey on medical image encryption: from classical to deep learning-based approaches. Comput Electr Eng. 2025;123(3):110011. doi:10.1016/j.compeleceng.2024.110011.
30. Duan H, Zhang S, Li D. Searchable attribute-based encryption with multi-keyword fuzzy matching for cloud-based IoT. Comput Mater Contin. 2025;86(2):1–25. doi:10.32604/cmc.2025.069628.
31. He P, Su X, Cui Y, Wu D, Wang R, Meng S. Dual-adversarial generative networks for reversible steganography in medical image security of Internet of Medical Things. Biomed Signal Process Control. 2026;116(11):109577. doi:10.1016/j.bspc.2026.109577.
32. Sethi K, Sahoo B, Shrishti, Kumar BNP, Dhal K, Cho W, et al. Lightweight DWT steganography with ECC-ChaCha20 for secure medical IoT systems. IEEE Access. 2025;13(2):142948–60. doi:10.1109/ACCESS.2025.3598099.

33. Venugopala PS, Raghavendra S, Ashwini B. CrypticCare: a strategic approach to telemedicine security using LSB and DCT steganography for enhancing the patient data protection. IEEE Access. 2024;12(3):101166–83. doi:10.1109/ACCESS.2024.3430546.
34. Saranya BS, Nalini M, Silambarasi P. Revolutionizing industrial Internet of Things security with an innovative image steganography technique. In: Proceedings of the 4th IEEE International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2023; 2023 Dec 8–9; Bengaluru, India. doi:10.1109/ICSTCEE60504.2023.10585078.
35. Hassaballah M, Hameed MA, Awad AI, Muhammad K. A novel image steganography method for industrial Internet of Things security. IEEE Trans Ind Inform. 2021;17(11):7743–51. doi:10.1109/TII.2021.3053595.
36. Croix NJDL, Ahmad T. A scheme based on convolutional neural network and fuzzy logic to identify the location of possible secret data in a digital image. Int J Eng Appl. 2024;12(1):1–14. doi:10.15866/irea.v12i1.23475.
37. Yang W, Liu Y, Chen Y, Cui Y, Guo C, Shen G, et al. HSMNet: a multi-resolution grayscale image steganalysis method based on hybrid dilated convolution and self-attention multi-channel network. Inf Sci. 2026;728(1):122824. doi:10.1016/j.ins.2025.122824.
38. He Z, Wu R, Wang X. Image steganalysis based on an adaptive attention mechanism and lightweight DenseNet. Comput Mater Contin. 2025;85(1):1631–51. doi:10.32604/cmc.2025.067252.
39. Chanda D'Layla AW, De La Croix NJ, Ahmad T, Han F. EHR-protect: a steganographic framework based on data-transformation to protect electronic health records. Intell Syst Appl. 2025;26(15):200493. doi:10.1016/j.iswa.2025.200493.
40. Li D, Kar P. B-Spot: blockchain and steganography based robust and secure photo transmission mechanism. J Mob Multimed. 2022;18:1677–708. doi:10.13052/JMM1550-4646.18610.
41. Cao Y, Li J, Chao K, Xiao J, Lei G. Blockchain meets generative behavior steganography: a novel covert communication framework for secure IoT edge computing. Chin J Electron. 2024;33(4):886–98. doi:10.23919/CJE.2023.00.382.
42. Xi J, Xu G, Zou S, Lu Y, Li G, Xu J, et al. A blockchain dynamic sharding scheme based on hidden Markov model in collaborative IoT. IEEE Internet Things J. 2023;10(16):14896–907. doi:10.1109/JIOT.2023.3294234.
43. Dargaoui S, Azrour M, Allaoui AE, Guezzaz A, Alabdulatif A, Alnajim A. Internet of Things authentication protocols: comparative study. Comput Mater Contin. 2024;79(1):65–91. doi:10.32604/cmc.2024.047625.
44. Najmi KY, Alzain MA, Masud M, Jhanjhi NZ, Al-Amri J, Baz M. A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability. Mater Today Proc. 2023;81(4):377–82. doi:10.1016/J.MATPR.2021.03.417.
45. Song B, Wei P, Wu S, Lin Y, Zhou W. A survey on deep-learning-based image steganography. Expert Syst Appl. 2024;254(7):124390. doi:10.1016/J.ESWA.2024.124390.
46. Setiadi DRIM, Rustad S, Andono PN, Shidik GF. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Process. 2023;206(3):108908. doi:10.1016/J.SIGPRO.2022.108908.
47. Qin J, Luo Y, Xiang X, Tan Y, Huang H. Coverless image steganography: a survey. IEEE Access. 2019;7:171372–94. doi:10.1109/ACCESS.2019.2955452.
48. Elsayed SH, Abdelsalam R, Shoman MAI, Alotaibi R, Reyad O. Lightweight multi-layered encryption and steganography model for protecting secret messages in MPEG video frames. Comput Mater Contin. 2025;85(3):4995–5013. doi:10.32604/cmc.2025.068429.
49. Shah D, Shah T, Naseer Y, Jamal SS, Hussain S. Cryptographically strong S-P boxes and their application in steganography. J Inf Secur Appl. 2022;67(3):103174. doi:10.1016/J.JISA.2022.103174.
50. Abdelwahab OF, Hussein AI, Hamed HFA, Kelash HM, Khalaf AAM. Efficient combination of RSA cryptography, lossy, and lossless compression steganography techniques to hide data. Procedia Comput Sci. 2021;182(5):5–12. doi:10.1016/J.PROCS.2021.02.002.
51. D'Layla AWC, Ahmad T, Ijtihadie RM, De La Croix NJ. A comprehensive survey on steganography of medical images. Comput Sci Rev. 2026;61(5):100973. doi:10.1016/j.cosrev.2026.100973.

52. Tang Y, Zhang M, Lai P, Yue Y, Di F. Fixed neural network image steganography based on secure diffusion models. Comput Mater Contin. 2025;84(3):5733–50. doi:10.32604/cmc.2025.064901.
53. Zhang Y, Chen Y, Dou H, Meng Y, Zhu H. AMF-VSN: adaptive multi-process fusion video steganography based on invertible neural networks. Inf Fusion. 2025;121(3):103130. doi:10.1016/J.INFFUS.2025.103130.
54. Zhang Z, Fu G, Ni R, Liu J, Yang X. A generative method for steganography by cover synthesis with auxiliary semantics. Tsinghua Sci Technol. 2020;25(4):516–27. doi:10.26599/TST.2019.9010027.
55. Li Q, Wang X, Wang X, Ma B, Wang C, Shi Y. An encrypted coverless information hiding method based on generative models. Inf Sci. 2021;553(3):19–30. doi:10.1016/J.INS.2020.12.002.
56. Alissa KA, Maray M, Malibari AA, Sana Alazwariand Hamed Alqahtani MKN, Obbaya M, Shamseldin MA, et al. Optimal deep learning model enabled secure UAV classification for industry 4.0. Comput Mater Contin. 2023;74(3):5349–67. doi:10.32604/cmc.2023.033532.
57. Shafique A, Mehmood A, Alawida M, Khan AN. Enhancing privacy in data transmission between IoT devices: a robust encryption and embedding framework for secure and meaningful image communication. J Inf Secur Appl. 2025;93(1):104112. doi:10.1016/j.jisa.2025.104112.
58. Mukherjee S, Mukhopadhyay S, Sarkar S. IoTSLE: securing IoT systems in low-light environments through finite automata, deep learning and DNA computing based image steganographic model. Internet Things. 2024;28(1):101358. doi:10.1016/J.IOT.2024.101358.
59. Rajan JG, Ganesh RS. Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: a robust data security framework. Expert Syst Appl. 2025;279(5):127403. doi:10.1016/J.ESWA.2025.127403.
60. Jiang S, Ye D, Huang J, Shang Y, Zheng Z. SmartSteganogaphy: light-weight generative audio steganography model for smart embedding application. J Netw Comput Appl. 2020;165(7):102689. doi:10.1016/j.jnca.2020.102689.
61. Zhao P, Zhou Y, Ijaz S, Khan F, Chen J, Alshawi B, et al. RLL-SWE: a robust linked list steganography without embedding for intelligence networks in smart environments. J Netw Comput Appl. 2025;234(5):104053. doi:10.1016/j.jnca.2024.104053.
62. Alkodre AB, Bahbouh NM, Sendra S, Sen AAA, Alsaawy Y, Alqahtany SS, et al. A shuffling-steganography algorithm to protect data of drone applications. Comput Mater Contin. 2024;81(2):2727–51. doi:10.32604/cmc.2024.053706.
63. Ragab M, Alshehri S, Alhadrami HA, Kateb F, Ashary EB, Abdel-Khalek S. Encryption with image steganography based data hiding technique in IIoT environment. Comput Mater Contin. 2022;72(1):1323–38. doi:10.32604/CMC.2022.024775.
64. Lin Y, Lin CC, Chang CC, Chang C. Hiding information in encrypted images with (t, n) secret sharing for IoT and cloud services. J Inf Secur Appl. 2025;93(8):104137. doi:10.1016/j.jisa.2025.104137.
65. Rathore MS, Poongodi M, Saurabh P, Lilhore UK, Bourouis S, Alhakami W, et al. A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Comput Electr Eng. 2022;102(1):108205. doi:10.1016/j.compeleceng.2022.108205.
66. Nahar M, Kamal AHM, Hossain G. Protecting health data in the cloud through steganography: a table-driven, blind method using neural networks and bit-shuffling algorithm. J Netw Comput Appl. 2023;217(6):103689. doi:10.1016/j.jnca.2023.103689.
67. Calo AMVM, Calanda FB, Medina RP. Novel self-sufficient coverless video steganography for secured Internet of Things (IoT) communication. In: Proceedings of the 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data, ICEIB 2024; 2024 Apr 19–21; New Taipei City, Taiwan. p. 133–8. doi:10.1109/ICEIB61477.2024.10602649.
68. Rostam HE, Motameni H, Enayatifar R. Privacy-preserving in the Internet of Things based on steganography and chaotic functions. Optik. 2022;258(4–6):168864. doi:10.1016/j.ijleo.2022.168864.
69. Dhawan S, Chakraborty C, Frnda J, Gupta R, Rana AK, Pani SK. SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. IEEE Access. 2021;9:87563–78. doi:10.1109/ACCESS.2021.3089357.
70. Ge X, Zhang X, Sun M, SongGong K, Zou X. Invertible generative speech hiding with normalizing flow for secure IoT voice. Internet Things. 2025;32(28):101606. doi:10.1016/j.iot.2025.101606.