IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 April 2025, accepted 20 April 2025, date of publication 24 April 2025, date of current version 5 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3564120

SURVEY

Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions

MAHA DRISS[1,2], (Senior Member, IEEE), LAMIA BERRICHE[3], SAFA BEN ATITALLAH[1,2], AND SIWAR REKIK[3]

[1]Robotics and Internet-of-Things Laboratory, Computer Science Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
[3]Computer Science Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

Corresponding author: Maha Driss (mdriss@psu.edu.sa)

ABSTRACT The Internet of Things (IoT) has raised significant security concerns, especially with regard to secure data transfer among resource-constrained devices. While effective, traditional encryption techniques are often computationally expensive and easily identifiable, making them unsuitable for many IoT applications. Steganography is an intriguing approach that allows hiding sensitive information within seemingly ordinary data, preventing unauthorized parties from detecting and accessing it. Existing studies on IoT security lack a comprehensive analysis of steganographic techniques tailored for IoT-specific constraints. This study bridges this gap by providing a comprehensive review of steganographic methods for IoT, exploring approaches across many domains such as spatial, frequency, and hybrid methods used in images, videos, audio, text, network traffic, hybrid approaches, and quantum-based methods. We evaluated and validated the techniques employed using key metrics such as imperceptibility, robustness, and embedding capacity while emphasizing the computational restrictions, real-time processing requirements of IoT devices, and the vital requirement for energy-efficient algorithms. This survey also investigates the integration of steganography and cryptographic approaches, as well as advances in Machine Learning (ML), Deep Learning (DL), and quantum techniques that could revolutionize the field. The study ends with future research directions that underscore the importance of innovative steganographic techniques that strike a compromise between security, efficiency, and scalability in IoT applications.

INDEX TERMS Internet of Things (IoT), steganography, covert communication, secure data transfer, resource-constrained devices.

I. INTRODUCTION

The Internet of Things (IoT) has transformed numerous industries, enabling seamless connectivity and automation in healthcare, smart cities, and industrial systems. With countless connected devices, the IoT allows real-time data collection, analytics, and decision-making, unlocking unprecedented opportunities [17], [55], [89]. However, this rapid growth has resulted in major security challenges, particularly for devices with limited resources operating under severe computational, memory, and energy constraints. Conventional encryption algorithms, while necessary to secure data, are often too resource-intensive for IoT devices [51]. Furthermore, while encrypted communications are secure, they can be easily identifiable, thereby bringing attention to sensitive information and affecting privacy.

Steganography is a covert communication method that hides data within apparently harmless cover objects, such as images, audio files, videos, and network protocols, to ensure that unauthorized parties are unaware of the presence of hidden information [77], [119]. In contrast to encryption, which safeguards content by rendering it unreadable while indicating its presence, steganography not only protects the information but also conceals its existence altogether. This

The associate editor coordinating the review of this manuscript and approving it for publication was Alexander Kocian.

major advantage makes it an effective method to maintain confidentiality, especially in frequently monitored settings such as IoT networks, where simply identifying encrypted communication might raise suspicion and invite possible cyberattacks [50].

In IoT ecosystems, steganography offers a novel security method by concealing sensitive information within trusted communication channels generated by IoT devices. In this way, IoT devices can share sensitive information seamlessly without disclosing hidden data, reducing the chances of intercepting or cyber threats. Consequently, by employing steganography, IoT systems can improve security and privacy without exposing sensitive information exchanges. Therefore, steganography reinforces data protection in high-risk and resource-constrained contexts like IoT applications by acting as a complementary security mechanism to encryption. For example, in intelligent healthcare solutions, medical IoT devices can send patient information hidden within ordinary physiological signals, preventing unauthorized individuals from accessing sensitive data. In a similar manner, industrial IoT systems may employ steganographic methods to securely convey authentication keys or control commands hidden within regular telemetry data, reducing the threat of cyber espionage or industrial sabotage.

Moreover, the decentralized and restrictive characteristics of IoT networks present unique challenges for steganography, such as restricted computational resources, the need for real-time processing, and the need for resilience against data compression and noise disruption [76]. Given that IoT environments produce large amounts of data, it is essential to develop lightweight, effective, and resilient steganographic techniques that seamlessly integrate into these networks. In contrast to conventional computing systems that can implement intricate steganographic algorithms with few limitations, IoT devices require customized methods that harmonize security, efficiency, and imperceptibility in real-time uses.

Ensuring scalability and detection avoidance is also an important challenge when developing efficient steganographic algorithms for IoT applications. IoT networks are made up of a huge number of diverse devices that operate in dynamic environments using different hardware and communication protocols. A scalable steganographic solution must work across multiple IoT platforms, from edge computing nodes to low-power embedded sensors, without substantially affecting network latency, performance or energy consumption [46]. However, since many recent steganalysis techniques can examine data patterns to uncover hidden information, avoiding adversary detection is crucial. Adaptive encoding mechanisms, in which embedding techniques dynamically adapt depending on the network environment, data type, and security risk level, are necessary to provide undetectability in steganographic communications. Furthermore, utilizing blockchain-based security mechanisms and Artificial Intelligence (AI)-driven steganography might improve detection resilience, offering decentralized, adaptive, and self-learning security solutions for large-scale IoT ecosystems.

In order to overcome these challenges, innovative approaches that take into account the diverse and dynamic characteristics of IoT environments are required. The ongoing development of IoT security threats demands the creation of intelligent self-adaptive steganographic models that can dynamically modify embedding capacity, cover selection, and embedding parameters in response to changing network conditions and security threats.

The main goal of this survey is to comprehensively investigate the role of steganography as a security mechanism in IoT environments. Existing surveys have largely overlooked the specific challenges posed by IoT settings, particularly the inherent resource constraints of IoT devices, including limited memory, processing power, and energy efficiency. Furthermore, these surveys often fail to address the real-time processing demands of IoT applications or the scalability issues arising from the large-scale interconnectivity of IoT devices. While some studies have explored hybrid models that combine cryptography and steganography, they did not adequately evaluate the effectiveness of these models in addressing the distinct challenges presented by IoT systems. This survey aims to fill these gaps by providing a comprehensive analysis of steganography's role and potential in securing IoT environments. This study provides an exhaustive review of steganographic approaches in spatial, frequency, and hybrid domains by investigating the specific challenges as well as prospects offered by IoT environments. These approaches are evaluated not only for their ability to hide information, but also for their adaptability in the resource-constrained, real-time, and heterogeneous environment of IoT devices. Furthermore, this survey highlights the transformational potential of combining steganography with sophisticated technologies like ML and DL models, which improve embedding techniques, and quantum computing, which provides exceptional security levels. This paper not only examines existing approaches but also identifies key deficiencies and challenges in the current literature, offering practical solutions to adapt steganography to meet IoT-specific requirements. This survey aims to promote the proposal and development of novel and practical steganographic solutions by describing future research directions. It considers steganography as a crucial addition to traditional security practices, proposing scalable, resilient, and effective steganographic techniques suited for the IoT environment, ensuring secure, discrete, and effective data transfer in highly complex, interconnected, and vulnerable systems.

The main contributions of this survey are:

- **Comprehensive Review**: Analyzes IoT-specific steganographic techniques, considering their applicability and effectiveness.
- **New Taxonomy**: Introduces a structured classification based on embedding domains, cover media, and IoT constraints.

- **Performance Evaluation**: Assesses key performance metrics such as imperceptibility, robustness, and embedding capacity in IoT environments.
- **Security and Scalability Analysis**: Examines challenges related to real-time processing, scalability, and resilience against attacks.
- **Integration of Advanced Technologies**: Explores the role of ML, DL, and quantum computing in improving steganographic solutions.
- **Tailored IoT Solutions**: Proposes optimized steganographic methods aligned with blockchain, quantum key distribution, and evolving IoT security needs.
- **Future Research Directions**: Identifies key areas for further exploration, including AI-driven steganography, adaptive embedding, and scalable security frameworks.

The remainder of this paper is structured as follows. Section II reviews related surveys, identifying research gaps in IoT steganography. Section III highlights the main contributions of this study. Section IV provides background information on the concepts of IoT and steganography. Section V presents a comprehensive review of the literature research, analyzing existing steganographic approaches. Section VI discusses current challenges and future research directions, focusing on advances in AI, quantum computing, and service computing. Finally, Section VII concludes the survey by summarizing key insights.

II. RELATED SURVEYS AND GAPS IN IoT STEGANOGRAPHY RESEARCH

This section investigates how existing surveys dealt with steganographic approaches in both general and specific contexts. It highlights the limitations of these surveys, particularly their focus on IoT-specific challenges such as resource restrictions, real-time requirements, and scalability. By examining these limitations, this section highlights the importance and novelty of the current study while laying the foundation for its thorough review and contributions.

Steganography approaches have been surveyed in several recent papers. We mention [118], which offered an overview of steganography methods, with a specific emphasis on image steganography. This work classified techniques into traditional methods, Convolutional Neural Network (CNN) approaches, and Generative Adversarial Network (GAN) techniques. Traditional techniques such as Least Significant Bit (LSB) substitution were commonly utilized but presented several constraints in terms of capacity and security. Methods that used CNNs showed improved results in embedding and extraction by employing encoder-decoder architectures. GAN-based techniques, especially CycleGAN, were noted for their impressive performance in image reconstruction and anti-forensics. The article also addressed challenges such as the absence of benchmark datasets, problems with scalability, and difficulties with implementing real-time solutions. This survey ended with the urge for further research in fields such as the use of new techniques such as quantum computing and hybrid methods, emphasizing the potential of DL to advance steganography. The main emphasis of the [118] survey is on improving image steganography methods; however, it does not address the use of steganography in IoT settings. The methods examined frequently do not consider the limited computational power, memory, and energy resources that IoT devices have. Steganography methods, particularly those that utilize DL methods such as CNN and GAN, often require substantial computational resources, which may not be feasible for small IoT devices. Furthermore, the survey shows that the scalability of IoT networks, which are made up of multiple interconnected devices, presents another obstacle, as DL-driven steganography techniques may face difficulty in scaling efficiently because of their heavy computational requirements. Moreover, real-time processing is vital in IoT settings, where real-time data transmission and processing are necessary for tasks such as remote monitoring and automated decision-making, underscoring the importance of steganography techniques that can function effectively under such strict limitations. All these aspects and issues were not deeply discussed in this survey.

In [96], the authors examined recent advances in quantum image steganography and highlighted a set of methods, including a turtle shell-based matrix and Least Significant Qubit (LSBq). Compared to traditional methods, these techniques improved image quality, security, and embedding capacity. However, the article had several limitations in addressing issues in the IoT environment. By considering more resilient environments, the survey ignored the specific constraints imposed by IoT devices, such as limited energy, memory, and processing capacity. Scalability was also a challenge, as IoT environments strained computational resources due to the large number of interconnected devices. The survey mainly focused on quantum steganography, which was relevant to secure data transmission, but not directly applicable to IoT environments. Although quantum steganography could increase security, the assessment failed to explore how these methods could be adapted to address vulnerabilities specific to IoT applications, such as data manipulation and unauthorized access in distributed networks.

Jan et al. in [63] offered an in-depth examination of dual-layer security systems that incorporate cryptography and steganography methods (crypto-stego). This survey emphasized the increasing need for security in digital communications, especially when transmitting multimedia data. Jan et al. examined different cryptographic techniques such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and chaos-based encryption, along with their combination with image steganography for creating robust security systems. Different techniques of steganography, such as spatial and frequency domain methods, were examined along with their strengths and weaknesses in terms of embedding capacity, imperceptibility, and resistance to attacks. The article assessed the advantages and disadvantages of these techniques and highlighted the importance

of maintaining a balance between security, embedding capacity, and image quality in crypto-steganography systems. It also covered assessment metrics like Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) to evaluate the effectiveness of these methods. Finally, the article proposed potential areas for future research in enhancing the effectiveness, scalability, and security of crypto-stego systems. This survey did not place a specific emphasis on the use of steganography for security concerns in IoT settings. Although the paper thoroughly discussed cryptography and steganography methods, its main focus was on the secure transfer of multimedia data and overall data protection. It presented different steganographic techniques combined with cryptography to improve data security, but did not delve into the specific issues encountered when using IoT devices, such as computational limitations, energy constraints, or real-time processing needs. The challenges related to scalability and resource constraints were not thoroughly explored when it comes to integrating steganography in IoT settings. Therefore, this survey did not specifically address the potential adjustments or enhancements needed for steganography to address IoT-related security issues.

All of these surveys fail to adequately consider the different issues encountered in IoT settings by ignoring the particular limitations of IoT devices, such as limited computational capability, memory, and energy resources. In addition, they ignore the challenges in scaling up interconnected device networks and do not take into account the critical requirement for real-time processing in IoT applications. Moreover, certain surveys focus on the combination of cryptography and steganography but fail to address how these hybrid systems can effectively address weaknesses and constraints in IoT settings.

Therefore, a focused research survey that collects, examines, and discusses steganographic solutions tailored to the unique requirements of IoT systems is urgently needed. The primary goal of this work is to bridge the gaps identified in previous surveys by highlighting the role of steganography in solving significant IoT challenges, including storage and power consumption. Given the constrained nature of IoT devices, optimizing data storage and minimizing energy usage is crucial to efficient operation. Steganographic techniques offer a compact and secure data embedding approach within existing IoT communication protocols. Using lightweight encoding and embedding methods, steganography minimizes redundancy, effectively reducing the volume of transmitted data and conserving storage space [42]. Moreover, traditional cryptographic methods require significant computational power, making them impractical for resource-limited IoT devices. In contrast, steganography provides a low-energy alternative for secure communication by embedding authentication directly within transmitted signals [32]. Therefore, integrating steganography into IoT security frameworks not only enhances data confidentiality but also ensures efficiency in large-scale real-time IoT deployments.

III. MAIN CONTRIBUTIONS OF THE CURRENT SURVEY

This survey offers multiple significant contributions to the area of IoT steganography by providing an in-depth analysis of existing related works, addressing the main challenges, and suggesting innovative solutions. It presents a new taxonomy for classifying related work studies, assessing the promise of emerging technologies, and comparing existing approaches. Moreover, it highlights future research directions and stresses practical uses in different IoT areas, with the goal of promoting scalable and efficient steganographic technologies. The main contributions of this survey are described in more detail in the following points.

1) **Comprehensive Review of Steganographic Solutions in IoT Environments**: This survey offers an in-depth analysis of steganographic methods designed for IoT applications that address a wide range of techniques, such as spatial, frequency, and hybrid strategies. It emphasizes how these methods are tailored to the distinctive data structures and communication protocols of IoT, providing a solid understanding of the present condition of the field.
2) **Proposal of a Taxonomy for Steganography in IoT**: A new classification for IoT steganography is presented, organizing methods according to important factors such as embedding domains, types of cover media (such as images, audio, and network traffic), and particular application needs. This classification offers an organized approach to understanding the domain of IoT steganography and acts as a useful resource for researchers and professionals. By categorizing methods based on their characteristics and applications, the taxonomy emphasizes the variety of strategies and aids in pinpointing appropriate techniques for particular IoT issues, such as resource limitations, real-time processing requirements, and resistance to detection.
3) **Assessment of Essential Performance Metrics**: The survey thoroughly assesses the steganographic methods according to essential performance criteria such as imperceptibility, robustness, and embedding capacity. It highlights how these metrics are affected by the limitations of IoT devices, including restricted computational capabilities and energy efficiency, providing insights into the performance of methods in practical situations.
4) **Investigation of the Incorporation of Cutting-Edge Technologies**: This study investigates the incorporation of advanced technologies such as ML, DL, and quantum computing into steganography. It explores how these technologies can improve embedding methods, increase detection resistance, and broaden the possible uses of steganography in IoT systems.
5) **Critical Analysis and Comparisons of Existing Approaches**: A comprehensive comparative analysis is presented that emphasizes the advantages,

disadvantages, and relevance of current steganography approaches proposed for IoT environments. This study helps researchers and professionals identify which approaches are most appropriate for particular applications and scenarios.

6) **Addressing IoT-Specific Challenges**: This survey enumerates and discusses the relevant challenges encountered when applying existing steganographic solutions in IoT environments, such as resource constraints, the dynamicity of IoT network topologies, and the requirement for real-time processing. It explores how these challenges impact the development and use of steganographic techniques and suggests possible ways to address them.
7) **Suggestions for Future Research Directions**: This survey highlights various prospective research directions, such as AI-based steganography, adaptable embedding techniques, and multi-layered security systems. In addition, it highlights the need for scalable solutions and robustness against advancing steganalysis methods to tackle the increasing complexity and dynamicity of IoT systems.
8) **Effective Solutions for IoT Requirements**: Novel solutions are suggested to tailor steganography to the specific requirements of IoT. These include resource-efficient algorithms for data embedding, flexible real-time systems, and alignment with broader security frameworks such as blockchain and quantum key distribution to guarantee secure and private data transfer in interconnected networks.

These contributions not only strengthen the existing state of research related to steganographic solutions in IoT settings but also propose a framework to progress the field, tackle essential challenges, and facilitate the development of innovative and practical solutions designed for the specific requirements of IoT environments.

IV. BACKGROUND

This section presents an overview of IoT including its architecture, main limitations, and security challenges. In addition, it presents the fundamentals of steganography techniques, their categories, and performance criteria. In addition, this section examines the role of steganography in improving IoT security and privacy, ending with a review of new trends and developments in steganographic techniques in IoT settings.

A. OVERVIEW OF IoT

IoT has been presented as a breakthrough technology that has fundamentally transformed various aspects of our lives, driving innovation and reshaping industries. In the following sections, we will provide a comprehensive definition of IoT, explore its layered architecture, and discuss the key limitations and challenges that hinder its full potential.

1) DEFINITION AND ARCHITECTURE

IoT refers to a network of interconnected devices that can communicate and exchange data seamlessly [20]. These devices can process data and perform intelligent actions. This capability enables them to operate autonomously and provide valuable insights in various applications, such as smart homes, healthcare monitoring, and traffic management.

The IoT architectures consist mainly of four layers, as depicted in Figure 1. This architecture includes:

1) **Perception Layer:**
This layer is responsible for collecting data through the use of physical devices and sensors. It can detect changes in the environment and convert them into digital signals for further processing.
2) **Network Layer:**
This layer is responsible for transferring data to the processing centers using different communication protocols such as Wi-Fi, Bluetooth, and 5G. In addition, it manages the routing and connectivity between devices, enabling seamless communication within the IoT ecosystem.
3) **Processing Layer:**
This layer includes computer systems located in the cloud or at the edge of the network to analyze and process the data collected. It plays an essential role in the transformation of raw data into meaningful insights using advanced analytics, ML, and data processing techniques.
4) **Application Layer:**
This is the top layer of the IoT architecture that communicates directly with users. It delivers actionable insights, facilitates decision making, and allows users to monitor and control IoT devices and systems. By transforming processed data into user-friendly formats, this layer ensures seamless interaction between IoT technologies and their end-users, enabling effective management and utilization of IoT applications.

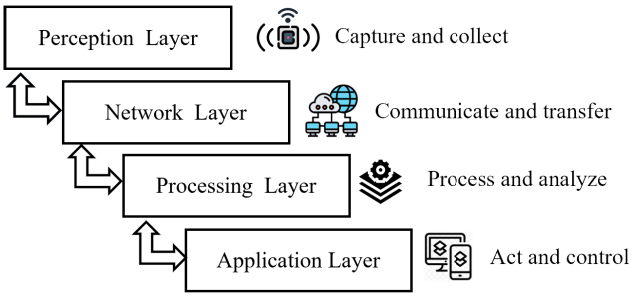

FIGURE 1. The internet of things architecture.

This layered design ensures the efficient functioning of IoT systems by integrating data collection, transmission, analysis, and application functions.

2) LIMITATIONS IN IoT SYSTEMS

IoT systems face several inherent limitations that reduce their efficiency and scalability.

1) **Resource Constraints:**
   One of the main IoT challenges is resource constraints. Many IoT devices have limited processing power, small storage space, and energy resources, which restrict their ability to perform complex computations.
2) **Network Bandwidth:**
   The network bandwidth poses another constraint. As the number of connected devices increases, the demand for data transmission can exceed available bandwidth, resulting in latency and degraded performance.
3) **Device Heterogeneity:**
   IoT ecosystems include a wide variety of devices with various capabilities, operating systems, and communication protocols. This heterogeneity introduces compatibility challenges, complicates device management, and requires custom solutions to achieve seamless integration.

3) SECURITY CHALLENGES IN IoT

IoT systems come with distinct characteristics and features, including distributed architecture, resource-constrained devices, and highly diverse operational environments. These unique attributes introduce a wide range of security challenges that must be addressed effectively to ensure the safe and efficient functioning of these systems. Key challenges include:

1) **Data Privacy and Integrity:**
   Ensuring the security and accuracy of sensitive data is a top priority in IoT systems [35], [50]. Unauthorized access or manipulation can result in data breaches, disinformation, or compromised operations, particularly when dealing with sensitive or mission-critical information [80], [121].
2) **Cyber-Attacks:**
   IoT systems are vulnerable to a variety of attacks, including DoS, Distributed Denial-of-Service (DDoS), and Man-In-The-Middle (MITM) [16], [25]. Such attacks could interrupt system functioning, compromise security, or lead to data theft.
3) **Limited Computational and Energy Resources:**
   Many IoT devices have limited processing power, memory, and battery life [104]. As a result, there is a growing need to develop and implement energy-efficient security solutions that can effectively protect IoT systems.
4) **Latency and Real-Time Security Requirements:**
   Real-time IoT applications, such as healthcare monitoring and autonomous systems, require minimal latency [27]. Security measures must be efficient and unobtrusive to ensure that they do not compromise the system's performance or timeliness.

B. FUNDAMENTALS OF STEGANOGRAPHY

In a steganographic system, secret data is embedded in a cover object in a way that prevents its detection. The cover object can take various forms, including images, audio, video, text, network traffic, or quantum form. The embedding process, also called encoding, consists of inserting the secret data - payload- into the cover object carrier. It involves making unnoticeable alterations to the cover object to produce the stego-object. This process may involve the utilization of a key, which is also used in the extraction or decoding process to retrieve the hidden data from the stego-object. The key ensures that only authorized users can successfully extract concealed messages [69].

Figure 2 illustrates the steganography process, where a secret message is embedded into a cover object, which may take different forms, to produce a stego object. The resulting stego object should appear similar to the original cover object to ensure that the hidden message remains imperceptible to unauthorized parties.

Based on the technology used, steganography can be categorized into classical steganography and quantum steganography. Classical steganography relies on conventional computing, whereas quantum steganography uses the principles of quantum mechanics. Based on the cover object, steganography is categorized into five types: image steganography, audio steganography, video steganography, linguistic steganography, and network steganography. Each type employs different techniques. The taxonomy of the steganography approaches is shown in Figure 3.

1) IMAGE STEGANOGRAPHY

Image steganography is a technique that is used to conceal secret data in an image. The original image that contains the embedded bits is the cover image. The embedded data are the payload, and the image with embedded data is called the stego image. Image steganography is classified into two main techniques based on the embedding domain; Spatial domain techniques and transform domain techniques.

1) **Spatial domain techniques:** Modify the pixel values of the cover image to hide secret data. An example is LSB substitution, which replaces the least significant bits of each pixel with the bits of secret data [15].
2) **Transform domain techniques:** This technique consists of transforming the cover image into the frequency domain and embedding the secret data in the transformed coefficients. Examples of frequency domain techniques include Discrete Cosine Transform (DCT), which is used in JPEG compression [133], and Discrete Wavelet Transform (DWT), which decomposes an image into high and low-frequency components for embedding data [54].
3) **Hybrid techniques:** Hybrid image steganography combines the strengths of spatial and frequency domain techniques to balance imperceptibility, robustness, and computational efficiency [128].

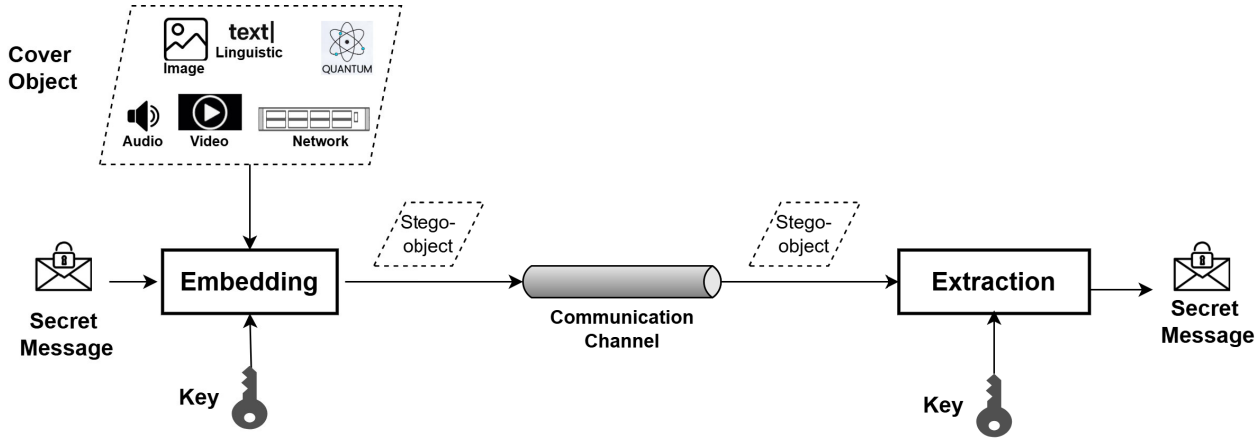

FIGURE 2. Steganography process in IoT.

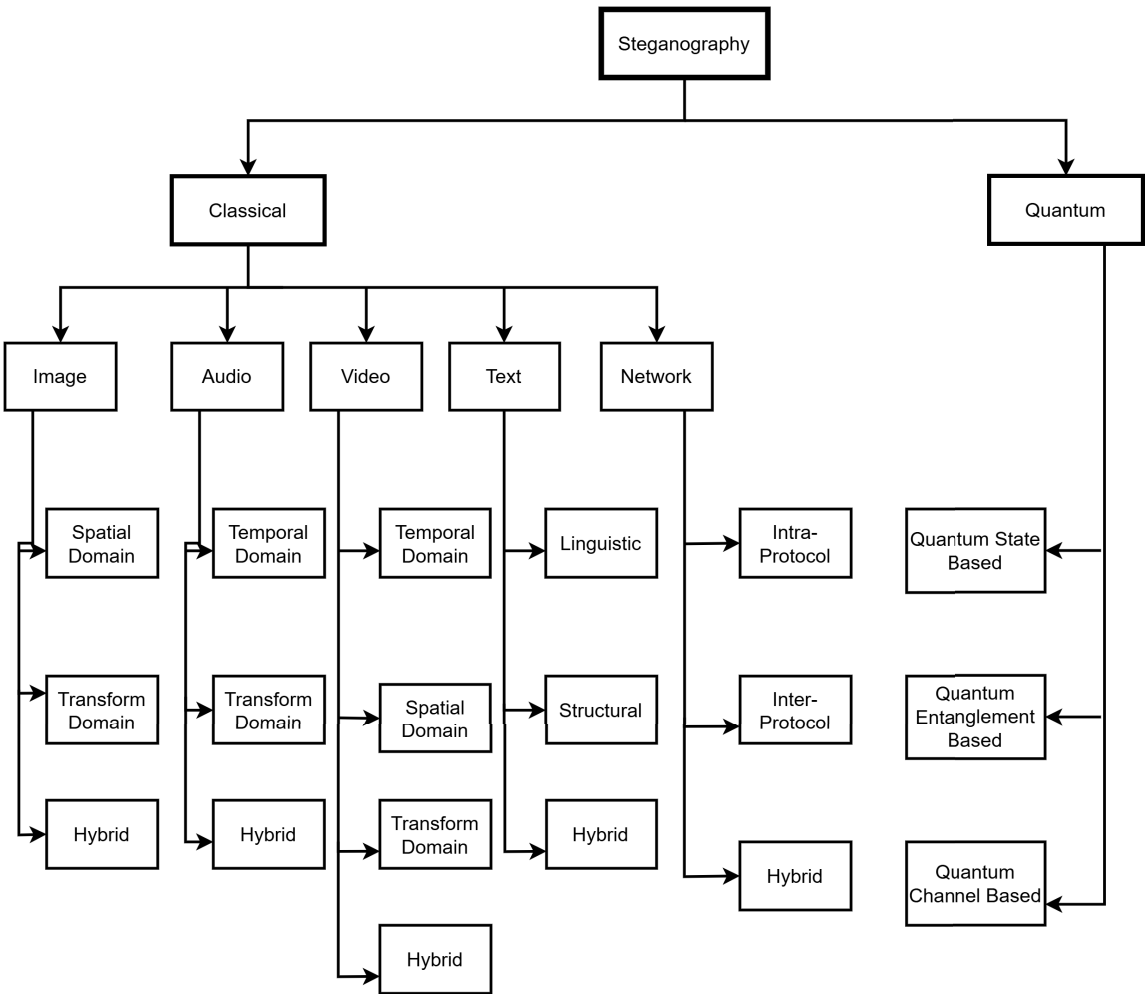

FIGURE 3. Taxonomy of steganography.

2) AUDIO STEGANOGRAPHY

Audio steganography is a technique used to conceal secret data in audio files. Audio steganography takes advantage of recent advances in speech compression and data hiding. Similarly to image steganography, audio steganography aims to maintain imperceptibility, robustness, and embedding capacity. The audio file used to carry hidden data is called cover audio, while the modified audio file containing

embedded data is called stego audio [47], [48]. Based on the embedding domain, audio steganography can be categorized into three main types:

1) **Temporal-based steganography:** Temporal domain steganography consists of hiding secret data in a coefficient of a time-domain representation of the signal, such as the amplitude or the phase.
   - **LSB substitution:** embeds secret bits into the least significant bits of audio samples, making small changes imperceptible to the human ear [5], [100].
   - **Phase coding:** modifies the phase components of the audio signal while preserving its magnitude, ensuring high imperceptibility since the human ear is less sensitive to phase changes compared to amplitude variations [14].
2) **Transform-based steganography:** This method conceals secret data within the frequency domain of an audio signal by applying mathematical transformations.
   - **Wavelet-based audio steganography:** uses DWT to decompose the signal into frequency subbands, embedding data in the wavelet coefficients for improved robustness against compression and noise [123].
   - **Discrete cosine-based audio steganography:** embeds secret data in DCT coefficients, offering greater computational efficiency compared to DWT [102].
3) **Hybrid audio steganography:** This method combines temporal and transform-based techniques to leverage the advantages of both domains. Hybrid methods enhance security, robustness, and embedding capacity by strategically embedding data across multiple domains.

3) VIDEO STEGANOGRAPHY

Video steganography is an extension of image and audio steganography that hides secret data within video files. Video, as a sequence of images combined with audio, provides a rich medium for data embedding due to its large size, temporal redundancy, and multiple components. The video file used to carry hidden data is called the cover video, while the resulting file with embedded information is called the stego video [79]. Small alterations to video frames or audio components are more difficult to detect in dynamic video sequences, making video steganography highly effective. It incorporates techniques from both image and audio steganography, including the temporal domain, spatial domain, transform domain, and hybrid methods [87].

4) TEXT STEGANOGRAPHY

Text steganography is a method to conceal secret information within natural language text [90]. Text steganography involves three main techniques.

1) **Linguistic steganography:** This technique involves altering or generating text in such a way that it remains non-suspicious. It includes:
   - **Lexical steganography:** encodes information by replacing selected words with synonyms, a technique effectively applied using CNNs [129].
   - **Syntactic steganography:** embeds secret data by altering the structure of sentences [130].
   - **Semantic steganography:** hides information within the meaning of the text [22].
   - **Text generation:** generates entire text blocks based on statistical features [12], [101], or Large Language Models (LLMs) [132].
2) **Structural steganography:** In this technique, the secret message is hidden by changing the physical format of a text. For example, in [105], hidden information is encoded by manipulating whitespaces by adding spaces, tabs, or line breaks.
3) **Hybrid text steganography:** This method combines linguistic and structural techniques to enhance security, embedding capacity, and robustness. Hybrid methods utilize both text modifications and format alterations to create steganographic messages that are more resistant to detection.

Text steganography is used in applications that involve the use of text data.

5) NETWORK STEGANOGRAPHY

In network steganography, secret data are hidden within network traffic taking advantage of network protocols or their behavior [88]. Network steganography is often defined as a covert channel or covert communication [24], [93]. Depending on the number of protocols involved, network steganography can be categorized as follows.

1) **Intra-protocol steganography:** A single network protocol is involved in the embedding process [28]. This type has been investigated more thoroughly, revealing three main techniques:
   - **Protocol Data Unit (PDU) embedding:** this method hides data in header fields, unused or reserved fields, padding bits, or the payload. For example, the IPv4 overflow field of the timestamp option was used for covert communication in [24].
   - **Inter-PDU time embedding:** this technique modifies the timing relationships between PDUs to encode hidden information. It takes advantage of the temporal aspects of network traffic to create a covert channel for secret communication by intentionally introducing delays between packets [126], [131].
   - **Hybrid intra-protocol steganography:** Combines both PDU content modification and timing-based techniques, maximizing covert capacity and robustness against detection.

2) **Inter-protocol steganography:** Multiple protocols are involved in the embedding process [65]. This technique allows for the embedding of more secret data across multiple protocols. Lehner et al. [82] investigate inter-protocol steganography for real-time services and propose a traffic coloring approach to detect covert channels.
3) **Hybrid network steganography:** Integrates both intra-protocol and inter-protocol techniques for greater flexibility, improved security, and higher embedding capacity. Using multiple hiding mechanisms across various network layers, hybrid methods enhance resilience against detection and adaptability to different network environments.

6) QUANTUM STEGANOGRAPHY

A quantum system is a physical system that behaves according to the rules of quantum mechanics [116]. The energy levels of quantum systems are discrete. The qubit is the fundamental unit of information in quantum computing. Quantum systems have two main properties: Superposition and entanglement [33]. The superposition principle states that a qubit can be in a superposition of both 0 and 1 at the same time, as written in Eq.1.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

α and β are complex numbers representing the probability amplitudes for the states $|0\rangle$ and $|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. The principle of entanglement states that the states of two or more particles can become correlated in a way that the state of one particle cannot be defined without considering the others, even when they are far apart. The entangled state of two qubits is represented as a Bell state as in Eq. 2.

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2}$$

A quantum channel is a communication channel that is used to transmit quantum information. It may include photons or other quantum particles used to carry quantum states across distances [108].

Quantum steganography techniques use the principles of quantum mechanics to hide secret information within quantum states [7]. The main techniques of quantum steganography include:

1) **Quantum state-based steganography**: The secret information is encoded into the quantum state using qubits or quantum registers. In superposition encoding, the hidden data are encoded in a superposition of quantum states. In this method, the information is hidden in the coefficients of the states of the qubit. In quantum amplitude modulation, the information is hidden in the amplitudes of quantum states.
2) **Quantum entanglement-based steganography**: This technique encodes the hidden information in the quantum entanglement between particles. The no-cloning theorem, stating that any observation of the system will disturb the entangled state, applies to this technique [94].
3) **Quantum channel-based steganography**: It utilizes quantum communication channels, such as optical fibers or free-space links, to transmit hidden information. Quantum noise-based encoding hides information in the fluctuation of the inherent quantum noise of a system. In phase encoding, the secret information is encoded in the phase of quantum particles, such as photons [70].

With the advent of quantum computing, various forms of data, such as images and audio, have been represented within the quantum realm. The quantum image, in which qubits represent the values of pixels, was investigated for applications in steganography. Quantum image steganography techniques such as Least Significant Qubit (LSQ) [66], Turtle Shell based Matrix [36], and quantum image scrambling [59] and many others were presented in [96].

7) PERFORMANCE EVALUATION METRICS

All steganography techniques aim to embed the maximum amount of secret data in a cover object, guaranteeing that the changes are imperceptible. The goal is for the stego object to reach its destination without any noticeable distortion and to be protected against various types of attacks. Consequently, the main criteria for assessing the performance of the steganography technique include imperceptibility, embedding capacity, robustness, and security. These criteria are evaluated using various metrics to measure their effectiveness in hiding data while ensuring the quality and security of the cover object. Furthermore, the importance of specific evaluation metrics may vary depending on the steganographic category.

a: IMPERCEPTIBILITY

Imperceptibility refers to how well the hidden data are blended into the cover object, ensuring that the stego object remains visually or perceptually indistinguishable from the original. This is important to avoid detection through human observation or statistical analysis. Common metrics to assess imperceptibility are listed in Table. 1. In image, audio and video the PSNR is used to evaluate the imperceptibility. The PSNR estimates the difference in the pixel values of a stego image and its original image as shown in Eq. 3.

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{3}$$

where MAX is the maximum signal/pixel value and MSE is the mean square error which is an important parameter used to evaluate the performance of a steganographic system. This parameter consists of comparing the original cover audio signal with the obtained stego audio signal (the signal after embedding hidden data). The MSE measures the average squared difference between these two signals, providing insight into the level of distortion introduced by the steganography process. The MSE between the cover audio

signal and the stego-audio signal is calculated using the Eq. 4 [83]:

$$\text{MSE} = \frac{1}{n}\sum_{i}(C(i) - S(i))^2 \tag{4}$$

$C(i)$ is the signal/pixel value in the cover object and $S(i)$ is the signal/pixel value in the stego-object. A high PSNR indicates that the distortion introduced by the embedding is minimal. Even though the PSNR is frequently used for its simplicity and effectiveness, it does not relate to human perception as the Normalized Cross-Correlation (NCC) metric. The NCC quantifies how well the overall structure of the cover object is preserved while hiding the secret information. Imperceptibility increases as the NCC approaches 1. NCC formula is given by Eq. 5:

$$NCC = \frac{\sum_i \text{C}(i)\text{S}(i)}{\sum_i [\text{C}(i)]^2} \tag{5}$$

Specifically, in image steganography, the Structural Similarity Index Metric (SSIM) is a metric assessing the structural similarity between the cover and the stego image. As shown in Eq. 6, SSIM includes information about luminance, contrast, and structural information in an image which aligns with human visual perception.

$$\begin{aligned}\text{SSIM}(C,S) &= \ell(C,S)\cdot\zeta(C,S)\cdot\delta(C,S)\\ \ell(C,S) &= \frac{2\mu_C\mu_S + b_1}{\mu_C^2 + \mu_S^2 + b_1}; \quad \zeta(C,S) = \frac{2\sigma_C\sigma_S + b_2}{\sigma_C^2 + \sigma_S^2 + b_2}\\ \delta(C,S) &= \frac{\sigma_{CS} + b_3}{\sigma_C\sigma_S + b_3}\end{aligned} \tag{6}$$

where $l(C,S)$ is the luminance function for measuring the proximity between mean luminance (μ_C, μ_S) of cover and stego images, $\zeta(C,S)$ is the contrast function for measuring the proximity between the contrast of the two images. σ_C and σ_s are the standard deviation of the cover image and the stego image respectively. $\delta(C,S)$ is a structural function for measuring the correlation coefficient between cover and stego images. b_1, b_2 and b_3 are positive constants.

In audio, the Segmental Signal-to-Noise Ratio (SegSNR) evaluates the SNR on a segment-by-segment basis. SegSNR measures the average SNR for multiple segments; this metric is used for a more detailed analysis of audio quality and variations in noise in different parts of the signal. The SegSNR is given in Eq. 7.

$$\text{segSNR} = \frac{1}{N}\sum_{m=1}^{N} 10\cdot\log_{10}\left(\frac{\sum_{n=1}^{L} s_m^2(n)}{\sum_{n=1}^{L}(s_m(n) - \hat{s}_m(n))^2}\right) \tag{7}$$

where N is the number of segments and L is the length of each segment. $s_m(n)$ is the original signal in segment m and $\hat{s}_m(n)$ is a reconstructed or noisy signal in segment m. The SegSNR is just an indicative performance measure. The Perceptual Evaluation of Speech Quality (PESQ) is a more reliable method to assess the performance of any speech steganography technique. This technique is used to assess speech quality in telecommunication systems, such as VoIP or mobile networks. The PESQ measurement provides an objective and automated technique for evaluating speech quality. The degradation of the speech sample can be predicted using the PESQ algorithm with a subjective opinion score. In general, the PESQ returns a score from 0.5 to 4.5, with higher scores signifying better quality [61], [62]. The PESQ method can be used to evaluate the stego speech. The reference signal refers to an original (cover) signal and the degraded signal refers to the stego signal with the hidden secret message.

b: EMBEDDING CAPACITY

The embedding capacity refers to the size of secret data (payload) that are hidden within a cover object. It measures the data-hiding potential of a specific steganographic method. More formally, embedding capacity is defined as in Eq. 8:

$$EC = \frac{\text{Size of Secret Data}}{\text{Size of cover object}} \tag{8}$$

In image steganography, the embedding capacity evaluates the number of bits embedded in an image pixel and is measured in bit per pixel (bpp). In audio steganography, it is related to the number of secret bits embedded in one audio signal sample or in one frame. In video steganography, it is evaluated in bits per frame. The embedding capacity in text steganography is generally measured in bits per character, word, or sentence, while in network steganography it is measured in bits per PDU.

c: ROBUSTNESS

The robustness of a steganography technique refers to the ability to maintain the integrity of hidden information against various attacks and distortions that may occur during transmission or processing. Robustness against statistical attacks includes immunity against statistical steganalysis, the practice of detecting hidden information by leveraging statistical information. Robustness against image manipulation includes robustness against cropping, rotation, compression, and noise addition. Robustness performance metrics are listed in Table. 1.

The most commonly used metric to evaluate robustness against noise, compression, and error in image, audio, and video steganography is the Bit Error Rate, shown in Eq. 9.

$$\text{BER} = \frac{\text{number of incorrect bits}}{\text{size of cover image}} \tag{9}$$

d: SECURITY

Security is about ensuring that hidden information remains undetected and unrecoverable by unauthorized parties. Security in steganography includes resistance to detection and steganalysis. Security performance metrics are listed in Table. 1. The resistance of steganalysis in image steganography can be evaluated using metrics such as the Chi-Square

TABLE 1. Steganography performance indicators and metrics.

Performance Indicator	Metric	Image	Audio	Video	Text	Network
Capacity	Capacity	✓	✓	✓	✓	✓
Imperceptibility	MSE (Mean Squared Error)	✓	✓	✓	✓	✓
	PSNR (Peak Signal-to-Noise Ratio)	✓	✓	✓	✗	✗
	SSIM (Structural Similarity)	✓	✗	✓	✗	✗
	NCC (Normalized Cross Correlation)	✓	✓	✓	✓	✓
	K-L Divergence	✓	✓	✓	✓	✓
	Distortion Metrics	✗	✓	✗	✗	✗
Robustness	BER (Bit Error Rate)	✓	✓	✓	✗	✓
	SNR (Signal-to-Noise Ratio)	✗	✓	✗	✗	✗
	Frame Stability	✗	✗	✓	✗	✗
	Temporal Distortion	✗	✗	✓	✗	✗
Security	Entropy	✓	✓	✓	✓	✓
	Chi-Square Test	✓	✓	✓	✓	✓
	Payload Detection Rate	✓	✓	✓	✓	✓
	Randomness/Statistical Tests	✓	✓	✓	✓	✓
	Resistance to Statistical Steganalysis	✓	✓	✓	✓	✓
	Traffic Pattern Analysis	✗	✗	✗	✗	✓

Test, Histogram Analysis, Correlation Test, and Fourier Transform Analysis. Additionally, ensuring that the entropy of the stego object closely matches that of the cover object is crucial to minimizing the risk of detection.

Although spatial domain methods offer simplicity and high embedding capacity, frequency domain techniques provide robustness against image manipulation. Hybrid methods present promising solutions that take advantage of the strengths of both domains.

C. ENHANCING IoT SECURITY AND PRIVACY THROUGH STEGANOGRAPHY: USE CASES AND APPLICATIONS

The widespread adoption of IoT systems in various domains has brought unique challenges related to data security, privacy, and resource efficiency. IoT devices, often equipped with limited computational power, storage, and energy resources, require lightweight and effective methods to protect sensitive information during transmission and storage. Steganography has emerged as a significant solution for enhancing IoT security by enabling covert data communication without drawing attention to the presence of hidden data. In the following, we highlight the importance of steganography in different IoT use cases:

1) **Healthcare IoT:** Security and confidentiality of patient information are critical in healthcare IoT systems. Medical photos, audio files, or video streams can leverage CNNs or GANs to securely embed diagnostic data during transmission.
2) **Industrial IoT (IIoT):** Industrial IoT networks produce critical operational data (for example, machine status and performance records) that, if intercepted, could interrupt operations or cause data breaches. Steganography could hide control instructions and operational data inside network packets or video streams.
3) **Smart Homes:** Smart homes depend on continuous data exchange between interconnected devices, making them vulnerable to cyber-attacks. Steganography can embed control signals or encryption keys in multimedia streams, such as voice commands or video feeds.
4) **Smart Cities:** In smart cities, surveillance cameras, traffic sensors, and monitoring systems collect and transmit large volumes of data. Steganography can ensure that critical information remains hidden within multimedia streams.
5) **Financial IoT Systems:** IoT-enabled financial devices, such as ATMs and POS systems, require secure transmission of sensitive information, such as PINs and transaction logs. Steganography can hide this information in system logs or multimedia outputs.

Steganography in IoT serves as a critical solution to address security and privacy challenges in resource-constrained environments. The integration of ML and DL techniques enables covert data transmission across resource-constrained environments and ensures that sensitive information remains hidden, imperceptible, and secure. The adaptability of steganographic techniques to various multimedia formats, such as images, audio, and video, makes them highly suitable for improving security in IoT systems. In the next section, we will provide a comprehensive review of the literature on the use of steganography in the IoT.

V. COMPREHENSIVE LITERATURE REVIEW

In this comprehensive survey, we selected articles published after 2020, from academic databases such as IEEE Xplore, ACM Digital Library, Springer, Elsevier, and Google Scholar. We categorized the literature based on the embedding medium, including image, audio, video, text, network, and quantum. To evaluate the techniques, we compared their imperceptibility, capacity, security, robustness, and computational efficiency within IoT scenarios. This section examines steganographic approaches designed for IoT contexts, categorizing them according to the embedding medium. The following subsections discuss IoT image steganography, IoT video steganography, IoT audio steganography, and IoT hybrid steganography, highlighting their approaches,

strengths, and limitations. A comparative analysis is also provided to assess and compare the methodologies studied.

A. STEGANOGRAPHIC TECHNIQUES IN IoT

1) IoT IMAGE STEGANOGRAPHY

Image steganography is categorized as the most widely used steganographic method in IoT systems because of the widespread use of image data in various IoT applications. In IoT environments, devices such as surveillance cameras, smart medical imaging devices, and smart home systems generate, transmit, and store image data. These devices require lightweight and secure techniques for data protection. IoT image steganography achieves these requirements by incorporating sensitive data within image pixels.

The methods used in image steganography are classified into three categories: spatial domain techniques, frequency domain techniques, and hybrid approaches. However, since hybrid approaches are not commonly used in IoT contexts, only techniques in the spatial and frequency domains will be considered. The following subsections explore these two categories, highlighting their methodologies, discussing their relevance to IoT applications, and identifying their limitations. Table. 2 shows a comparison of the discussed IoT image steganography techniques.

a: IOT SPATIAL IMAGE STEGANOGRAPHY

Spatial domain steganography directly modifies pixel values to embed data. This approach is simple and computationally efficient, which makes it suited for resource-constrained IoT devices. For example, Khari et al. in [75] discussed security issues in IoT environments, highlighting weaknesses in data transfer due to inadequate emphasis on security protocols. The authors employed Elliptic Curve Cryptography (ECC) to ensure confidentiality, integrity, non-repudiation, and authentication of data exchanged between IoT devices. In addition, they applied matrix XOR steganography, a spatial domain technique that altered the pixel values of image blocks to hide encrypted messages. This method was further improved with the Adaptive Firefly algorithm, which was utilized to optimally select the embedding pixels. Combining ECC and matrix XOR steganography provided an effective approach for protecting sensitive information, particularly medical information, but introduced potential computational overhead.

In [26], an IoT-assisted cloud environment for the urban transportation system has been utilized to facilitate safe data sharing by applying the hybridized cryptographic-integrated steganography (HCIS) algorithm with auxiliary data input. LSB-based image steganography aids in the transmission of secret data to prevent information from being discovered, and cryptography transforms the data into a safe structure that can only be read by an authorized user. The upload and download times were optimized and surpassed the performance of the state-of-the-art methods. The simulations were conducted with 50 source nodes, 50 destination nodes, and 10 routers using the NS-simulator. However, no results were reported for the steganography performances. In addition, scalability for an environment with a large volume of data, a larger number of nodes, and real-time requirements need to be explored.

Ding et al. [45] proposed an image steganography method based on evolutionary multi-objective optimization (EMOsteg) with a focus on imperceptibility. EMOsteg utilized artificial immune theory to locate perturbation locations that were used for secret data embedding. First, multiple directional and non-directional high-pass filters were used to preprocess the cover image, and filter residuals were aggregated to form the candidate locations of the perturbation. EMOsteg formalized multi-objective optimization by minimizing perceptibility and optimizing security while using embedded capacity as a constraint condition. EMOsteg leveraged artificial immune theory to solve the multi-objective optimization problem. The optimization problem was represented as an antigen, and the perturbation locations were considered antibodies. The perturbation was then obtained by selecting the most advantageous antibodies from the population, and EMOsteg iteratively searched for antibodies to eliminate the antigen using feature extraction and adaptive evolution operators. To evaluate EMOsteg, experiments were conducted in the standard image database BOSSbase [68]. The authors selected 100 images as the cover and injected the same secret into each cover image. The embedding capacity was below 0.1 bpp. They reached an MSE of 0.000308, 82.75 PSNR, and a unit SSIM. The optimization algorithm was implemented on the IoT edge server with high computing power. One advantage of EMOsteg was that it balanced imperceptibility, security, and embedding capacity by using evolutionary multi-objective optimization and artificial immune theory. Its implementation on IoT edge servers ensured suitability for real-time applications in resource-intensive environments. While the technique was successfully implemented on IoT edge servers, its ability to scale for larger networks or meet strict real-time constraints remains untested.

The study in [2] explored the use of a classical quantum-inspired rendition of the Controlled Alternate Quantum Walks (CAQWs) model to develop a robust image steganography protocol for cloud- and IoT-based e-healthcare platforms. The authors used the CAQWs algorithm to select two LSB pixel locations in the carrier image to embed the secret bits. They tested their method on two sets of medical images from the MedPix dataset in [1]. The first set consisted of five 256×256 and five 128×128 color images, while the second set contained two sets of five greyscale medical images of the same dimensions. For a 2bpp capacity, they achieved a PSNR greater than 44dB and an SSIM of 0.9499. The authors also performed data loss analysis and demonstrated that their steganography technique could withstand clipping and noise addition attacks. Additionally, since their steganographic algorithm used a key related to the quantum state, they showed that their technique was robust against brute-force attacks. Finally, the use of CAQW

balanced imperceptibility and embedding capacity, but added computational complexity.

Dhawan et al. [43] proposed a technique that utilized the Salp Swarm Optimization Algorithm (SSOA) and a hybrid fuzzy neural network for data embedding and enhancement of the stego image quality. First, the secret image was encrypted using binary bit-plane decomposition based on piecewise-linear chaotic maps. The secret image data were embedded in both the smooth and edge regions. The SSOA algorithm was applied to differentiate between smooth and edge blocks in the stego image. Then, a neural backpropagation method was employed to enhance quality. In their experiments, they used the USC-SIPI image database [115]. The cover images included 8-bit 225 × 225 grey-level images such as Lena, Bell Pepper, and Baboon. Secret images comprised 8-bit grey-level images such as Cameraman (64 × 64), Airplane images (128 × 128), and Barbara (192 × 192), with file sizes of 5kB, 10kB, and 15kB. They evaluated the performance of their approach using PSNR, K-L divergence, and IF. Their results showed a PSNR greater than 52 dB for 2.5 bpp, K-L divergence below 0.065 for 0.7 to 2.3 bpp, and an IF greater than 0.999, indicating high imperceptibility. The achievement of high imperceptibility through SSOA and neural backpropagation for optimized embedding in both smooth and edge regions across diverse datasets demonstrated the robustness of the approach. The main limitation of [43] was its high computational requirements. However, the authors did not validate their technique using healthcare image datasets.

Khan et al. [74] proposed a system that utilized the achromatic component (Y-Plane) of the YCbCr color space and integrated a Maximum Likelihood Estimation Algorithm (MLEA) for secure data embedding. The process began with rotating the input image 90 degrees and transforming it into the YCbCr color space. The secret data were divided into blocks, encrypted using MLEA, and then embedded in the Y-Plane of the image. The authors conducted their experiments using a dataset from the COREL database. The method achieved high imperceptibility with a PSNR greater than 66 dB. Embedding data in the Y-Plane of the YCbCr color space preserved color fidelity, making the technique suitable for IoT devices exchanging color images. However, computational complexity, robustness testing, and reliance on the COREL dataset raised concerns about its security and applicability in diverse or adversarial scenarios.

Jan et al. [64] introduced a hybrid edge detector named CLoG, which combined the strengths of the Laplacian of Gaussian (LoG) and Canny edge detectors. To evaluate the technique, they tested it on 512×512 color images from the USC SIPI-Database. Each cover image was divided into three color channels: red, green, and blue. The green and blue channels were used to embed the data, while the red channel recorded the edge status of the pixels in the green and blue channels. The proposed method achieved an average PSNR of 48.12 dB with a payload of 2 bpp. Although the authors leveraged the channels of the color images to embed secret data with high imperceptibility, they did not elaborate on the robustness tests or computational complexity.

Chen et al. [38] proposed an image steganography-based secret sharing scheme for IoT security using GANs and image morphing techniques. Progressive Growing GAN (PGGAN) uses random noise vectors to generate high-resolution synthetic face images, called shadow images. These shadow images were used to embed the secret shares using participant-specific keys and were then morphed with participants' images. The use of GANs to generate high-resolution synthetic images ensured high performance while preserving privacy. The authors tested their technique in the high-Qversion of the CelebA high-resolution face image dataset (CelebA-HQ) [72]. One main limitation of this approach was the computational resource requirements for training GANs and extractors, which limited real-time scalability.

The work presented in [10] proposed a steganography approach, named IoTSteg, in the spatial domain, using the pixel attributes of the cover images to protect data in IoT networks. The IoTSteg approach divided pixels into Highly Smooth (HS) and Less Smooth (LS) regions, hiding confidential information in the HS region. In contrast to traditional techniques that utilized all pixels, IoTSteg selectively embedded data to improve efficiency. Using PSNR, Capacity-Distortion Trade-Off (CDTO), and SSIM, the technique achieved a PSNR of 66.61 and an SSIM of 0.9998, maintaining high imperceptibility. Compared to conventional approaches, IoTSteg performed well at embedding rates of 0.1 and 0.2 bits per pixel. However, the paper overlooked steganalysis attacks and discussions of computational overhead, which are essential for IoT applications.

Rostam et al. [111] proposed a method that utilized chaotic functions to generate initial keys for the embedding process. First, they divided the cover image into 3×3 pixel blocks. Then, they selected the secret data bits and replaced them with the least significant bits of block pixels that they randomly selected. Chaotic functions were used to ensure randomness. They evaluated their method on the UCID-Image Database images and the Harvard Whole-Brain Atlas (Dataset-75). Their technique achieved high imperceptibility with PSNR values above 45 and SSIM values above 0.98 at 1.5 bpp with the UCID dataset. Furthermore, they attained PSNR values above 55 dB with Dataset-75 when they hid 1000 characters in 256×256 images. The method leveraged chaotic functions to enhance security while ensuring high imperceptibility but did not discuss computational overhead and scalability capability.

Namasudra [99] proposed a scheme in which IoT devices collect data and send it to the data owner through the gateway. Afterwards, the data owner encrypts the data using a randomly generated secret key, followed by hiding the encrypted data in an image. Both cryptography

and steganography were based on data representation as Deoxyribonucleic Acid (DNA) sequences. Three 512×512 images were considered to evaluate the performance of the proposed cryptosystem. The method demonstrated a good imperceptibility performance with 53 dB PSNR, 0.41 MSE, and 0.99915 SSIM. Although the scope of the evaluation was limited, the combination of cryptography with steganography and DNA sequence-based data representation improved security by increasing randomness and robustness against attacks. However, the approach introduced high computational complexity due to the DNA encoding and encryption process, making it less suitable for real-time or resource-constrained IoT environments.

In [122], the authors suggested a GAN-based steganographic technique to embed text into images in wireless sensor networks. Secret information was converted into a noise vector and encoded into a stego image using a generator network. A discriminator network validated whether the image contained hidden information. A key ensured that only authorized users could decode secret information through a denoising process at the receiver. The authors validated their method with experiments using the Div2K [8], Common Objects in Context (COCO) [85], and Pascal Visual Object Classes (VOC) [49] datasets. The method demonstrated high perceptual quality with an average PSNR of 38.96 dB, an SSIM of 0.98, and a high retrieval accuracy of 99.92% while resisting attacks such as random key guesses. However, their approach increased computational requirements, making it inappropriate for resource-constrained Wireless Sensor Network (WSN) devices.

Mobi-Sense, designed and developed to improve data security and reliability in mission-critical IoT applications, was introduced by Mukherjee et al. in [98]. Using steganography techniques and network coding, the authors proposed a mobility-aware sensor fog paradigm that supports various types of data, including audio, video, and images. Data transmission security was improved through the use of steganographic techniques deployed in the spatial domain for image data. However, the approach introduced significant computational overhead, making it unsuitable for real-time applications on resource-constrained Wireless Sensor Network (WSN) devices. Furthermore, the method lacked robustness analysis against adversarial attacks, which could compromise the security of embedded data in highly dynamic network environments.

Prabhu et al. [106] introduced a steganographic approach enhanced with CNNs. Secret messages were encrypted, compressed, converted into binary and then embedded in images using an adaptive CNN-based approach. CNNs extracted features from images to enhance their accuracy and robustness. Their technique, tested on the COCO dataset, showed high detection resistance to SFNET and RSNET, with an average score of 98.1%. The average processing time was 0.01 ms per operation, making it suitable for real-time IoT applications. The image fidelity was maintained with negligible distortion, achieving a PSNR of 30 dB. However, the method lacked a comprehensive analysis of its scalability when applied to large-scale IoT networks and did not evaluate its robustness against noise and compression attacks, which are common in real-world communication channels.

Kaur et al. [73] presented EGCrypto, a low-complexity cryptographic architecture intended to improve secure data transfer in IoT-based applications. This architecture is appropriate for IoT devices with constrained processing capacity, as it uses elliptic Galois cryptography to provide strong encryption with low computing requirements. Their method offered a foundational layer of security that could be used together with additional techniques, such as steganography, to improve confidentiality, but it was mostly concerned with secure data transmission rather than steganography. To ensure that sensitive data were safely incorporated into non-sensitive data without compromising transmission efficiency, this study used steganographic techniques for images functioning in the spatial domain. In this work, effective low-complexity encryption was proved, which is highly recommended to ensure scalability and security in IoT-based applications. However, the study lacked a detailed performance evaluation of its resilience to modern cryptographic attacks and did not assess its adaptability to dynamic IoT environments with varying data loads and security requirements.

In [113], the authors proposed an image steganography algorithm that minimized image distortion. The proposed approach transformed secret data into a simplified format and arranged the binary representations of secret bits in ascending order. The experimental results showed that this method achieved a PSNR of 67.42 dB and an average SSIM of 0.99. However, the study did not evaluate the robustness of the algorithm against steganalysis attacks, leaving its security in adversarial environments uncertain. Furthermore, its adaptability to different types of cover media beyond images was not explored, limiting its potential applications.

b: IOT TRANSFORM DOMAIN IMAGE STEGANOGRAPHY

In contrast to spatial methods, frequency domain techniques embed data within transformed image components. This approach provides greater imperceptibility and robustness against compression and noise. For example, Kumar et al. [78] proposed a DL-based approach for text extraction based on steganography and encryption for IoT-based applications. First, the image was converted from spatial to DCT. The secret text was encrypted using homomorphic encryption based on equilibrium. Afterwards, the Extended Wavelet Convolutional Transient Search (EWCTS) optimized with Quotient Multi-Pixel Value Differencing (QMPVD) was developed to embed the secret text. A CNN was applied before the optimization to extract the features. They used the USC-SIPI image dataset for cover images and the medical records dataset i2b2 [117] for the secret text. The technique demonstrated high imperceptibility with good embedding capacity, achieving 69.76 PSNR, 0.01 MSE, 0.01 RMSE, and an SSIM of 0.999 when embedding 5KB of patient data in

256×256 images, nearly 0.07 bpp. However, the technique introduced computational complexity, which could limit its suitability for resource-constrained IoT environments. Furthermore, its robustness against steganalysis and noise-based attacks was not thoroughly evaluated, raising concerns about its security under adversarial conditions.

In [13], Alkhliwi proposed image steganography and encryption using the Manta Ray Foraging Optimization Technique (EIS-SDT). Before embedding, the secret image was encrypted using the Digital Logistic Chaotic Map (DLCM) technique. The cover image (RGB) was decomposed into different frequency bands (LL, LH, HL, HH) using a multilevel DWT. The Manta Ray Foraging Optimization (MRFO) algorithm was applied to select the optimal pixels from the decomposed image, to minimize MSE and maximize PSNR. The author compared their results with the Whale Optimization Algorithm (WOA) and Grey Wolf Optimization (GWO). They evaluated the performance of their technique on two datasets: the COVID-19 Radiography dataset [39] and the NIH Chest X-ray dataset [125]. EIS-SDT achieved lower MSE values (0.0098 to 0.0156) and higher PSNR values (66.20 to 68.22 dB). Under attack conditions, EIS-SDT maintained a lower MSE (1.652) compared to 2.847, and a PSNR of 43.59. However, while the technique demonstrated strong imperceptibility and resilience under attacks, it introduced computational overhead due to DWT decomposition and MRFO-based pixel selection, which could impact its real-time applicability in resource-constrained IoT environments. Furthermore, the study lacked an evaluation of resistance to steganalysis, raising concerns about its robustness against advanced detection techniques.

Hassaballah et al. [58] proposed the Harris Hawks Optimization-Integer Wavelet Transform (HHO-IWT) method for digital image steganography in the IoT environment. The metaheuristic optimization algorithm HHO was applied to select image pixels to embed secret data within integer wavelet transforms. They used the USC-SIPI dataset for both cover and secret images. The method demonstrated high imperceptibility, achieving a PSNR greater than 35 dB while maintaining robustness against image processing attacks such as erosion, dilation, salt and pepper noise, Gaussian noise, local variance, speckle noise, motion blur, JPEG compression, and Poisson noise. The PSNR values varied from 18 dB for the local variance attack to 30 dB for the Gaussian attack. Furthermore, the NCC value was close to 1, while the RMSE values remained low. The main advantage of this technique was the use of lightweight IWTs, which makes it suitable for IoT environments. However, despite its effectiveness, the study did not investigate robustness against adaptive steganalysis attacks, leaving its security in adversarial scenarios uncertain. Furthermore, while IWT-based steganography reduced computational complexity, the optimization process with HHO introduced additional overhead, which could affect efficiency in real-time IoT applications.

Ragab et al. [110] proposed an encryption-based image steganography technique, named EIS-DHT, to enable secure data transfer within the IIoT environment. They used color images for both cover and secret data. The process involved several stages, including channel extraction, decomposition, QBWO-based optimal pixel selection, encryption, and embedding. The Quantum Black Widow Optimization (QBWO) algorithm was applied in the EIS-DHT approach to effectively select pixel values to embed important information within the cover image. Additionally, data transformation was accomplished using a multi-level DWT. The R, G, and B bands, which comprised the secret image, were separately encrypted using the Blowfish, Twofish, and Lorenz Hyperchaotic Systems. The steganographic image was then created by embedding these encrypted images into the optimal pixel positions of the cover image. The authors evaluated their method using the USC-SIPI benchmark image dataset. Their results outperformed [43], achieving 56.76 PSNR with an embedding capacity of 17.37%, 0.9992 SSIM, and 0.1372 MSE. The technique was tested against different types of attacks, including erosion, Gaussian noise, and salt-and-pepper noise. Under attack conditions, the PSNR dropped to less than 32 dB, indicating some vulnerability to image distortions. Furthermore, while the method demonstrated strong security and imperceptibility, its high computational complexity could limit its practicality for real-time IIoT applications, particularly in resource-constrained environments.

Aleisa et al. [11] used color and greyscale cover images with Integer Wavelet Transform (IWT) embedding. Before embedding, the secret picture was compressed using a sophisticated wavelet-based algorithm and encrypted using simple bit operations such as AND and OR. First, IWT was applied to the cover image. The secret image bits were then embedded into the LSB of the cover IWT coefficient image. Finally, inverse IWT was applied to obtain the stego image. Afterwards, a Hybrid Fuzzy Neural Network with backpropagation learning was employed to improve the stego image quality. They obtained an MSE of less than 0.15 and a PSNR of 55 dB for color images. In addition, they achieved a unit NCC for both greyscale and color images. Although the technique used lightweight encryption, the incorporation of neural networks introduced additional computational complexity, potentially limiting its feasibility for real-time or resource-constrained applications.

In [91], a new steganographic method, known as Image Authentication using Boustrophedon Transformation (IABT), was introduced to improve the security of digital media when transmitted over a network. This study used ten 512×512 benchmark images to fully evaluate the performance of the proposed method. In this method, each cover image was initially broken down into spatial components arranged in 1×3 blocks. The spatial components were converted to frequency components using the Boustrophedon transformation. Bitstream formats were used to

TABLE 2. Summary of IoT image steganography techniques.

Work	Domain	IoT use case	Dataset	Strengths	Limitations
Khari et al. [75]	Spatial + ECC	Healthcare IoT	Medical data and image dataset	Enhanced security with ECC, adaptive firefly optimization	High computational complexity
Bi et al. [26]	Spatial + Cryptography	Smart Cities/ Transportation	Cloud-based data sharing scenarios	Secure hybrid method for data sharing	No performance metrics reported
Ding et al. [45]	Spatial/ Optimization	General IoT	BOSSbase	High imperceptibility, robust with EMOsteg optimization	Requires high computing power, limited embedding capacity (0.1 bpp)
Abd et al. [2]	Spatial (Quantum LSB)	Healthcare IoT	MedPix	Robust to noise, clipping, and brute force attacks	Limited to medical images, tested on specific datasets
Dhawan et al. [43]	Spatial + Optimization	Healthcare IoT	USC-SIPI	High PSNR (52 dB), quality enhancement with SSOA	High computational requirements
Khan et al. [74]	Spatial (YCbCr)	Smart Cities, Autonomous Vehicles, Smart Drones	COREL	High PSNR (66 dB), robust against salt-and-pepper noise	Limited embedding capacity (0.007 bpp), tested on limited datasets
Jan et al. [64]	Spatial (Edge-Based)	Smart Cities/ Transportation	USC-SIPI	High PSNR (48.12 dB), hybrid edge detection	Limited embedding capacity (2 bpp), moderate imperceptibility
Chen et al. [38]	Spatial	General IoT	CelebA-HQ	High capacity, GAN based	High computational requirements
Alarood et al. [10]	Spatial	General IoT	4 cover images	High imperceptibility (PSNR: 65 dB, SSIM: 0.9998)	Not suitable for noisy images or real-time applications
Rostam et al. [111]	Spatial	General IoT	UCIDImage Database, Harvard Whole Brain Atlas (Dataset-75)	Randomized embedding using chaotic functions, robust	Limited to small cover images, computationally expensive
Namasudra [99]	Spatial	General IoT	Private IoT data and image dataset	Secure encryption using DNA sequences, high PSNR	Limited to standard images, high complexity for real-time IoT
Veerashetty et al. [122]	Spatial	WSN	Div2K, COCO, Pascal VOC	GAN based, High perceptual quality, resistance to random key guess attack	High computational requirements
Mukherjee et al. [98]	Spatial	Mobile IoT	Sensor data transmitted within images	Focus on dynamic IoT environments with mobile sensors, effective for critical latency scenarios.	Computational requirements
Prabhu et al. [106]	Spatial	General IoT	COCO	High detection resistance, Low processing time, High image fidelity	Scalability
Kaur et al. [73]	Spatial	General IoT	IoT data embedded within 5 images.	Low complexity, suitable for resource-constrained IoT devices.	No robustness test
Septinaputri et al. [113]	Spatial	General IoT	Digital images	Low image distorsion	No robustness test
Kumar et al. [78]	Transform (DCT)	Healthcare IoT	USC-SIPI	High PSNR (69.76), low error rates, robust encryption	Computationally intensive, limited to 5KB embedding
Alkhliwi et al. [13]	Transform (DWT)	Healthcare IoT	COVID-19 Radiography database, NIH Chest X-ray dataset	Robust against attacks, Low MSE, High PSNR	Computational complexity
Hassaballah et al. [58]	Transform (IWT)	General IoT	USC-SIPI	Robust against image processing attacks, low RMSE	Moderate PSNR values for certain attacks (18-30 dB)
Ragab et al. [110]	Transform (DWT)	Industrial IoT	USC-SIPI	High imperceptibility, Tested against noise and erosion attacks	High complexity
Aleisa et al. [11]	Spatial (LSB)	Healthcare IoT	Medical image dataset (private)	Enhances patient data confidentiality	High complexity because of NN
Mandal et al. [91]	Frequency (IABT)	Smart city	Benchmark image dataset (10 images, 512×512 resolution)	High performance metrics: PSNR, IF, embedding capacity	Requires transformations, limited real-time feasibility

embed confidential data in transformed coefficients. These transformed coefficients were then converted back to pixel components using the inverse Boustrophedon transformation. This procedure was repeated until all the hidden data were merged into the host image, creating a steganographic image. The IABT method was assessed using metrics such as PSNR, MSE, IF, and embedding capacity, showing improved performance compared to existing steganographic methods. However, while the method demonstrated strong security and imperceptibility, its suitability for real-time applications remained uncertain due to the potential computational overhead introduced by the transformation process. Furthermore, the study did not assess the robustness of the approach against advanced steganalysis techniques, which could expose vulnerabilities in adversarial scenarios.

2) IoT AUDIO STEGANOGRAPHY

Technological developments have led to the widespread application of audio steganography in many domains, such as digital watermarking, copyright protection, and secure

data transfer. These developments have expanded their uses to include data integrity checking, covert surveillance, and authentication. As methods evolve, audio steganography becomes more important in maintaining confidentiality, privacy, and intellectual property protection. Compared to image steganography, less work has been devoted to audio steganography. This is mostly because audio signals are more complicated and sensitive to changes, necessitating careful consideration like perceptibility and sound quality. Audio steganography has had difficulty in striking a balance between embedding capacity, robustness, and audio quality. The design of an audio steganography system primarily involves optimizing the impact on cover speech quality. The goal is to produce a stego signal that remains perceptually indistinguishable from the original cover signal. Hidden data should not degrade audio clarity or introduce detectable artifacts. Table. 3 shows a comparison of the audio steganography techniques implemented for IoT environments and discussed in this subsection.

Jiang et al. developed a new smart steganography technique [67], which was automatically generated from adversarial training. The embedding model was considered lightweight and could be used as an ML tool in smart devices. The proposed methods were based on machine learning (ML), whereas the existing methods relied on manual crafting. The hiding model was built on three neural networks: an encoder that embedded the secret message in the carrier, a decoder that extracted the message, and a discriminator that identified carriers containing hidden messages. The system was trained in various configurations on two datasets, the TIMIT Acoustic-Phonetic Continuous Speech Corpus [53] and LibriSpeech [103], demonstrating its flexibility and potential for automation in steganography. However, despite its advantages, the study did not evaluate the resilience of the method against steganalysis attacks, which are crucial to ensure security in real-world applications. Furthermore, reliance on ML-based models introduced computational overhead, which could limit their feasibility for resource-constrained smart devices.

The work in [112] proposed an advanced audio steganography technique designed for IoT environments. The method used an Optimized Audio Embedding Technique (OAET), which utilized an elevated bit-range LSB technique to embed secret messages deeper within audio streams. Compared to typical LSB approaches, this method reduced distortion while improving the resilience and overall quality of the embedded audio. The experimental results demonstrated that this method provided excellent security, especially for applications such as IoT smart speakers. However, despite its effectiveness, the study did not evaluate the impact of compression and real-time transmission on embedded audio, which could affect its robustness in low-bandwidth IoT networks. Additionally, increasing the embedding depth may introduce computational overhead, potentially limiting its applicability to resource-constrained IoT devices.

3) IoT VIDEO STEGANOGRAPHY

Video steganography is an emerging field in IoT security due to the increasing use of video data in applications such as surveillance, smart homes, and industrial monitoring [79]. Videos provide an extensive medium for data embedding and offer ample storage capacity and multi-dimensional hiding opportunities across spatial and temporal domains. The dynamic nature of video content also makes it challenging for attackers to detect hidden information. Table. 4 shows a comparison of the discussed IoT video steganography techniques.

Koptyra and Ogiela introduced a notable approach in [77]. They proposed a steganography system designed for IoT settings, which combined spatial and frequency domain methods for improved security. This study used MP4 files due to their ample storage space and popularity in IoT systems equipped with digital cameras. The proposed system encoded hidden data using two different algorithms: video stego and metastego. Videostego operated within the spatial domain, inserting data directly into the pixel values of video frames. In contrast, metastego worked in the frequency domain, embedding data into the frequency components of video files using transformations such as DCT, making hidden information less apparent during regular processing. Sensors were used to covertly input data, enabling efficient operation in IoT environments with limited resources. This combination of spatial and frequency domain methods enabled the embedding of a large amount of data while also ensuring a balance between imperceptibility, resilience, and security. The proposed method addressed major weaknesses in IoT, such as unsecured data transfer and storage, by introducing an additional level of hidden communication and protection for confidential data. However, despite its strengths, the study did not evaluate the resilience of the method against real-time processing constraints and its vulnerability to advanced steganalysis attacks, which could compromise its security in practical IoT deployments.

Calo et al. [31] proposed a novel self-sufficient coverless video steganography method to address security and privacy challenges in IoT communication. The proposed method combined mapping and synthesis approaches to maximize carrier video capacity while reducing computational costs and time. The approach utilized sub-band features of the DWT to create a hash table and independently generate missing hash sequences, ensuring a highly efficient embedding process. To validate their work, Calo et al. used the UCF101 dataset. This dataset is a widely used video set that contains 13,320 videos in 101 human action classes, sourced from YouTube. It features diverse backgrounds, camera motions, and complex movements. Experimental results demonstrated a 100% covert data rate in any carrier video, superior time efficiency, and robustness against external attacks. However, while the method achieved impressive performance metrics, its practical scalability in real-time IoT applications and its resilience against evolving steganalysis techniques were not

TABLE 3. Comparative analysis of IoT audio steganography techniques.

Work	Domain	IoT use case	Dataset	Strengths	Limitations
Jiang et al. [67]	Temporal Domain	Audio Signals	TIMIT Acoustic-Phonetic Continuous Speech Corpus, LibriSpeech	Lightweight model suitable for smart devices. Automated embedding using adversarial training. Flexible, adaptive, and robust against detection.	Computationally intensive during training. Limited testing datasets for real-world applications. No evaluation of resilience against steganalysis attacks.
Anguraj et al. [112]	Spatial domain	IoT Smart Speakers	Audio Data Samples < 100	High security for data communication using elevated bit-range LSB. Reduced distortion and improved audio quality. Enhanced resilience for IoT smart speakers.	Effectiveness in diverse IoT environments not explored. Impact of compression and real-time transmission not evaluated. Increased embedding depth may introduce computational overhead.

TABLE 4. Summary of IoT video steganography techniques.

Work	Domain	IoT Use Case	Dataset	Strengths	Limitations
Koptyra and Ogiela [77]	Spatial and Frequency	IoT settings with digital cameras (e.g., surveillance, monitoring)	MP4 files	Combines spatial and frequency domain methods for improved security. Efficient for resource-constrained IoT environments. Balances imperceptibility, resilience, and security.	No evaluation of resilience against real-time processing constraints. Vulnerability to advanced steganalysis attacks not tested.
Calo et al. [31]	Transform (DWT)	Secured IoT Communication	UCF101 dataset	High covert data rate (100%). Superior time efficiency and robustness against external attacks. Reduces computational costs and time.	Practical scalability in real-time IoT applications not evaluated. Resilience against evolving steganalysis techniques not thoroughly tested.

thoroughly evaluated, raising concerns about its deployment in large-scale and adversarial environments.

4) IoT TEXT STEGANOGRAPHY

IoT text steganography leverages textual communication as a medium for embedding secret data. This approach presents a discrete and efficient solution for secure data transmission in IoT environments. Table. 5 shows a comparison of the text steganography techniques implemented for IoT settings and discussed in the following paragraphs.

In [52], the authors proposed a novel approach to secure data transmission in the IoT environment using linguistic steganography. This involved embedding secret data in textual communication by relying on ambiguous token selection. The approach began by identifying the most ambiguous word in a sentence for substitution, minimizing semantic distortion while embedding the data. The secret data were encrypted and split into multiple ''shares'' using (k, n)-threshold secret sharing over a Galois field. The secret data were embedded in the GPT-4 generated cover text, while RoBERTa was used to predict and embed tokens. The proposed method achieved an accuracy of approximately 50%. The results showed that the text maintained its meaning and coherence, with a high BERT score of 0.948 ensuring semantic integrity. Furthermore, a BERT score of 0.984 indicated that the text remained natural and easy to understand, preserving its original fluency. However, while the approach ensured semantic integrity, it was constrained by a limited embedding capacity, as only a small number of ambiguous tokens could be substituted per sentence. Furthermore, reliance on RoBERTa and GPT-4 introduced significant computational overhead, potentially restricting its feasibility for real-time or resource-constrained IoT applications.

In the context of symbolic steganography, where data are hidden within structured symbols or behaviors, [32] aligns with linguistic steganography in its use of symbolic systems to transmit information secretly. In [32], the authors used generative behavior steganography to embed secret data within the Gomoku game moves, where the moves in the game served as the steganographic carrier. The integration with blockchain and IPFS for data storage addressed the challenges of storage limitations, making it suitable for transmitting larger data files. The method also combined stream cipher encryption with the game model to secure data transmission. This approach offered high-security and covert transmission capabilities, demonstrating its robustness against common attacks such as noise and filtering. Although the method achieved better imperceptibility compared to traditional steganography due to its carrier-less nature, the challenge of key generation and sharing remained,

TABLE 5. Comparative analysis of IoT text steganography techniques.

Approach	Technique	Type of Data	Dataset	Strengths	Limitations
Gao et al. [52]	Linguistic	General IoT	GPT-4 generated text	High semantic integrity (BERT score: 0.984). Maintains text coherence and naturalness. Ensures semantic integrity with minimal distortion.	Limited embedding capacity due to few ambiguous tokens per sentence. High computational overhead from RoBERTa and GPT-4. Not suitable for real-time or resource-constrained IoT applications.
Cao et al. [32]	Behavioral (Symbolic)	General IoT	Synthetically generated data	High imperceptibility due to carrier-less nature. Robust against noise and filtering attacks. Low storage resource demands with blockchain and IPFS integration. Secure transmission using stream cipher encryption.	Challenges in key generation and sharing. Dependence on behavioral patterns (Gomoku game moves). Computational complexity may limit real-world deployment.

potentially affecting its practical deployment in real-world applications.

5) IoT NETWORK STEGANOGRAPHY

Network steganography is an innovative solution for secure communication in IoT environments. This approach leverages network protocols and traffic patterns as carriers for covert data transmission. Unlike conventional steganography, which focuses on multimedia data, network steganography embeds hidden information within network protocol fields or manipulates packet structures and behaviors. It is particularly suited for IoT scenarios where data often flow continuously across constrained and heterogeneous networks. Table. 6 shows a comparison of the discussed IoT network steganography techniques.

Recent advances have explored a variety of techniques for implementing network steganography. For example, Cabaj et al. [30] proposed Distributed Network Covert Channels (DNCCs) in IoT environments, using simulated IoT traffic as a carrier for covert data transmission. The method employed three primary covert channels: TTL Modulation, which modified the Time-To-Live field in IPv4 headers; HTTP Header Reorder, which altered the order of HTTP headers; and TCP Options Reorder, which changed the order of TCP header options to embed secret data. The authors evaluated the technique using bandwidth, undetectability, and robustness in their custom-simulated IoT traffic dataset. They utilized a Software-Defined Networking (SDN)-based testbed and achieved a maximum covert data rate of approximately 20 bits per second (bps). By integrating changes across different covert channels, DNCC decreased detectability by improving stealth. In addition, the authors provided a network traffic dataset. However, the study relied on simulated IoT traffic, which may not have fully represented real-world IoT deployments. Furthermore, several detection approaches were not tested on the generated traffic, leaving uncertainty regarding the resilience of the method against advanced network analysis techniques.

Mileva et al. [95] evaluated MQTT v5.0's susceptibility to network covert channels. They analyzed 18 direct covert channels (DCCs) and 5 indirect covert channels. Direct covert channels were based on modifying static protocol fields or appending data to fields in control packets, while the indirect covert channel manipulated the behavior of the protocol. New hiding patterns, such as PT15, were proposed. Detailed evaluation results were provided for their synthetically generated MQTT 5.0 traffic. Direct covert channels achieved up to 1,572,840 bps. The bandwidth of the indirect covert channels depended on the pattern used and the network configuration. Robustness against packet delays and losses was demonstrated, except for PT15. The covert channel was exclusive to MQTT, but statistical monitoring and behavioral analysis of MQTT properties could expose the covert channels. Furthermore, high-bandwidth channels were more susceptible to detection, potentially limiting their stealth in real-world applications.

The authors in [23] presented an approach to secure data transmission in underwater IoT environments. The proposed method focused on achieving both stealth and security. It supported a variety of underwater applications, including monitoring, climate observation, oceanographic data collection, and pollution detection. However, while the approach demonstrated its effectiveness in ensuring secure transmission, it lacked an in-depth evaluation of latency and energy consumption, which are critical factors in resource-constrained underwater networks.

Lazzaro et al. [81] proposed an approach in which secret messages were split into multiple parts and then encoded using modular arithmetic and XOR operations. Finally, they were hidden in the MQTT message headers. To maintain imperceptibility, dummy payloads were added to match the encoded lengths. The proposed technique was robust against standard IoT network operations, but could be sensitive to modifications of protocol fields by brokers or middleware. The embedding capacity depended on the frequency of the MQTT messages.

In [9], the authors altered interpacket delays in existing network traffic to embed secret data. The paper presented several steganography techniques for creating covert timing channels. They proposed an L-Bits to N-Packets covert channel, which correlated covert information with specific delays. Additionally, they introduced a covert time replay channel, which utilized a matrix of possible delays and a random number generator. The authors investigated the inter-arrival time behavior of covert timing channels using statistical metrics. They also conducted experiments to identify the packet delaying threshold value. Their findings showed that when the packet delaying threshold was approximately equal to or greater than double the mean of legitimate inter-arrival times, the covert timing channels became detectable as strong anomalies. Although the study showed a successful method for secret communication, it did not assess how it would affect Quality of Service (QoS) in real-time networks, where excessive packet delays could cause substantial latency and compromise critical IoT applications. Moreover, modern traffic-shaping strategies, which actively normalize network delays, may outperform the reliance on inter-packet delays, thus making the hidden channels useless.

Severino et al. [114] studied the feasibility and performance of Timing Covert Channels (TCCs) within the IEEE 802.15.4 protocol, specifically its Deterministic and Synchronous Multichannel Extension (DSME). TCCs operate by encoding secret data through manipulations of inter-packet delays (IPDs) in DSME's Guaranteed Timeslot (GTS) mechanism. They analyzed three methods: the On/Off method, the L-Bits to N-Packets method, and the Time Replay method. They used the openDSME simulation model integrated into the OMNeT++ framework to assess the Covert Channel Capacity and Efficiency under different configurations, such as varying superframe orders, traffic generation rates, and packet sizes. They reached a capacity of 1 byte per second (B/s) for the simple On/Off encoding and 6 B/s for the L-Bits to N-Packets and Time Replay. In addition, they noticed that higher SO values increased capacity but led to longer delays between slots, whereas lower TGR reduced capacity. However, the study was restricted to single-hop communication and specific to DSME under IEEE 802.15.4.

Hou et al. [60] introduced a covert channel, called CloakLoRa, utilizing the physical layer of LoRa (PHY). LoRa used the chirp spread spectrum modulation technique, in which the starting frequency of each chirp was applied to encode messages as LoRa symbols. The amplitude modulation served to embed the information in the LoRa chirps. In a real-world setting, the proposed approach achieved 99.47% accuracy for covert messages over a distance of 250 meters. The proposed technique was undetectable by regular LoRa receivers. However, its implementation required hardware or firmware modifications. Increasing the modulation depths improved covert communication efficiency and also increased detectability. The best results were obtained within 250 meters only.

The physical layer of LoRa gained attention in [92], where amplitude modulation was also used to embed secret information. Their BER reached 20% for a distance of 600 meters between the sender and the receiver, with a PSNR of 6 dB. Although CloakLoRa showed great hidden communication capabilities, its dependence on modulation of amplitudes can make it more vulnerable to environmental noise and signal interference, which could compromise its dependability in high-interference or urban IoT networks.

6) IoT QUANTUM STEGANOGRAPHY

Quantum steganography introduces a revolutionary approach to secure communication in IoT environments. Using quantum principles [116], it can embed and transmit sensitive information. Techniques include quantum state-based steganography, which encodes data in qubit superpositions or amplitudes, entanglement-based methods that exploit the no-cloning theorem to prevent unauthorized access, and channel-based approaches hiding data in quantum noise or photon phases across optical or free-space links. Quantum image steganography, such as LSQ and Turtle Shell-based Matrix, embeds data in quantum pixel representations, while quantum audio and network steganography adapt these for IoT data streams. These methods ensure high imperceptibility, resistance to classical steganalysis, and energy efficiency, making them suitable for real-time IoT applications such as healthcare and industrial systems, although integration with quantum hardware poses challenges for low-power devices [96].

Table. 7 shows a comparison of the discussed IoT quantum steganography techniques.

Chen et al. introduced two quantum audio steganography (QAS) protocols in [37]. These methods altered the LSQ of the host quantum audio signal, which was represented using a Flexible Quantum Audio (FRQA) format. The first protocol involved swapping qubits that encoded the quantum audio message with the LSQ of the amplitude information of the host audio signal. The second protocol embedded the quantum audio message directly into the Most Significant Qubit (MSQb) of the host signal, leveraging the inherent constraints of the MSQb. Although the suggested protocols showed innovative quantum-based steganographic methods, their real-world applicability may be limited because they did not assess real-world implementation issues like error rates in quantum computing environments and the feasibility of embedding messages in noisy quantum channels.

Abd El-Latif et al. [3] proposed a framework for secure communication in fog-cloud-based IoT environments using quantum steganography. Their protocol consisted of quantum entangled states, XOR operations, grey codes, and hash functions to embed and authenticate secure data. The sender encoded sensitive information using unitary transformations and quantum entangled particles before uploading the data to the fog cloud. The receiver extracted and authenticated the information using agreed-upon hash functions and

TABLE 6. Comparative analysis of IoT network steganography techniques.

Approach	Technique	IoT Use Case	Dataset	Strengths	Limitations
Cabaj et al. [30]	PDU Embedding	General IoT	Custom-simulated IoT traffic dataset	Utilized three covert channels: TTL Modulation, HTTP Header Reorder, and TCP Options Reorder. Achieved a covert data rate of 20 bps. Decreased detectability via integration across multiple channels.	Relies on simulated IoT traffic, which may not fully represent real-world deployments. Several detection approaches were not tested.
Mileva et al. [95]	PDU Embedding	General IoT	Synthetically generated MQTT 5.0 traffic	Evaluated 18 direct and 5 indirect covert channels in MQTT v5.0. Introduced PT15 hiding pattern and demonstrated robustness against packet delays and losses.	High-bandwidth channels (up to 1,572,840 bps) increase detectability. Limited to MQTT-based IoT communication.
Baker et al. [23]	PDU Embedding	Internet-of-Underwater-Things	Underwater network traffic dataset	Focused on achieving both stealth and security. Supported various underwater applications, including pollution detection and climate observation.	Lacked an in-depth evaluation of latency and energy consumption. Specific to underwater IoT environments.
Lazzaro et al. [81]	PDU Embedding	Privacy Protection in IoT	MQTT message traffic dataset	Split secret messages, encoded with modular arithmetic and XOR, then embedded in MQTT headers. Maintains imperceptibility with dummy payloads.	Sensitive to modifications of MQTT protocol fields by brokers or middleware. Embedding capacity depends on MQTT message frequency.
Al Eidi et al. [9]	Inter-PDU Time Embedding	General IoT	Network traffic data	Developed L-Bits to N-Packets and covert time replay channels. Investigated inter-arrival time behavior using statistical metrics.	Covert timing channels become detectable with strong anomalies when excessive packet delays occur. Did not assess QoS impacts in real-time IoT networks.
Severino et al. [114]	Inter-PDU Time Embedding	IoT Cybersecurity	Experimental network traffic data	Investigated TCCs within IEEE 802.15.4 DSME. Used OMNeT++ openDSME simulation model. - Achieved a covert capacity of 1 B/s for On/Off encoding and 6 B/s for L-Bits to N-Packets and Time Replay.	Study restricted to single-hop communication under IEEE 802.15.4. Higher SO increased capacity but introduced delays.
Hou et al. [60]	Physical Layer	General IoT	Experimental LoRa communication dataset	Introduced CloakLoRa, embedding covert data in LoRa PHY layer chirps via amplitude modulation. Achieved 99.47% covert message accuracy over 250 meters. Undetectable by standard LoRa receivers.	Requires hardware or firmware modifications. Limited covert range; best results obtained within 250 meters. Vulnerable to environmental noise and signal interference.
Maurya et al. [92]	Physical Layer	General IoT	Experimental LoRa communication dataset	Applied amplitude modulation for embedding secret data. Evaluated steganographic performance of LoRa PHY layer.	BER reached 20% for 600-meter distance with PSNR of 6 dB. Increased detectability at higher modulation depths.

initial states. The protocol leveraged quantum principles like no-cloning and uncertainty to enhance imperceptibility and prevent eavesdropping. Furthermore, any alteration of the entangled states was detected during hash verification, further improving the robustness of the protocol. By maximizing embedding capacity through the use of Bell states, the approach facilitated scalable communication for large IoT networks. The authors demonstrated the security of the proposed protocol against multiple types of attacks, including man-in-the-middle attacks and message attacks. Although the protocol had excellent security features, it depended on the availability of quantum infrastructure, which is still in its early stages and not yet widely accessible. Furthermore, quantum state manipulation's feasible processing complexity and resource requirements may make it impractical for real-time IoT applications.

Chaharlang et al. in [34] proposed a method for a quantum audio steganography system. The steganography technique utilized quantum circuits to perform the embedding process. This process consisted of three primary components: the quantum host audio (the carrier medium), the secret quantum data (hidden information), and the quantum embedding key (used to securely integrate the data into the host audio). The result was quantum stego audio, which replaced the original quantum host audio for transmission. The embedding process hid the data in the LSB by substituting the last significant bit of the host media. The stego media obtained by the LSB algorithm closely resembled the host media and was visually indistinguishable. In quantum audio representation, each quantum audio signal was a sequence of qubits, which captured the quantum signal samples. The least significant qubit (LSQ) in each sequence represented quantum audio information. Experiments on music and speech audio used

TABLE 7. Comparative analysis of IoT quantum steganography techniques.

Approach	Technique	Type of Data	Dataset	Strengths	Limitations
Chen et al. [37]	Quantum Domain	Secure Quantum Audio Communication	Synthetic quantum audio signals	Efficient embedding via LSQ or MSQb protocols	Dependence on quantum infrastructure and feasibility in noisy quantum channels.
Abd El-Latif et al. [3]	Entangled Embedding	Fog-cloud-based IoT	Simulated scenarios for Quantum-encrypted data and fog cloud IoT traffic dataset	Enhanced imperceptibility by no-cloning theorem.	Quantum infrastructure is still in its infancy.
				Maximized capacity through Bell states. High scalability and proven security.	High processing complexity may limit real-time applications.
Javad et al. [34]	Quantum Domain	Music and Speech (Quantum Audio)	Custom generated quantum audio dataset	High imperceptibility using LSB substitution.	Requires quantum computing infrastructure.
				Utilizes LSQ for quantum signals.	Limited practical implementation for current IoT.
				Achieved SNR of 30.214 (4 qubits) and 49.326 (8 qubits).	Did not evaluate quantum noise and decoherence effects.
Qu et al. [109]	State Embedding	6G-Quantum Internet of Vehicles	Quantum point cloud data and IoV network traffic dataset	High capacity and secure reversible information hiding.	Practical deployment is constrained by quantum networking limitations.
				Utilized Grover's algorithm for faster quantum data processing.	Did not evaluate resilience against quantum-specific attacks.
Biswas et al. [29]	Quantum Channel	Smart city IoT	Quantum data streams and encrypted IoT traffic dataset	High imperceptibility in quantum streams.	Requires quantum hardware.
				Robust against steganalysis techniques.	Sensitive to quantum noise and decoherence.

1024 samples, with fractional qubits alternating between 4 and 8, resulting in SNRs of 30.214 and 49.326, respectively. The proposed technique did not evaluate the effects of quantum noise and decoherence, which are significant challenges in real-world quantum computing systems, despite showing excellent imperceptibility and security. Furthermore, its applicability in real quantum communication systems is limited by its untested scalability to large quantum audio datasets.

In [109], the authors proposed a Quantum Efficient Privacy Protection Protocol (QEPP) in the 6G Quantum Internet of Vehicles. As 6G-enabled vehicular networks expanded, this protocol leveraged quantum mechanics to protect sensitive data against multiple threats. It employed reversible information hiding techniques in quantum point-to-point communication channels to securely transmit sensitive data. The embedding process began with the preparation of quantum states, which served as a cover for sensitive information and were shared between edge devices and cloud servers. Sensitive information was then encoded in these quantum states. The protocol implemented the quantum Grover algorithm to accelerate the processing speed of quantum data in the cloud. Furthermore, the protocol included a quantum error correction code. However, while QEPP demonstrated strong security and processing efficiency, its practical deployment remained constrained by the current limitations of the quantum networking infrastructure.

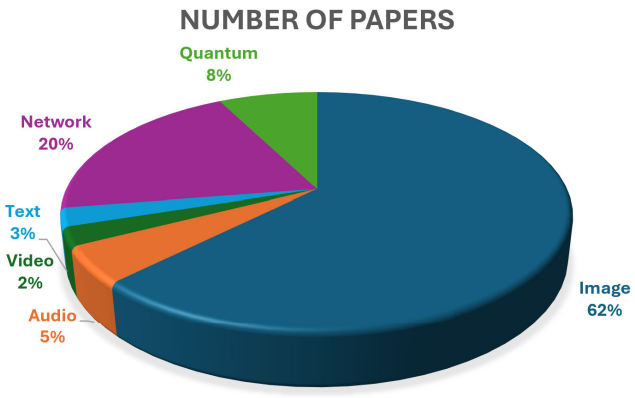

FIGURE 4. Distribution of steganography techniques utilized in IoT systems.

Furthermore, the protocol did not evaluate quantum-specific attacks, such as quantum side-channel attacks, which could compromise data integrity in real-world implementations.

Reference [29] combined quantum cryptography and quantum steganography for a smart city IoT system. Steganography was applied to the quantum stream. Although this approach improved security and covert communication, it did not account for the effects of quantum noise and decoherence, which may compromise the dependability of hidden data in real-world quantum IoT settings. Furthermore,

since quantum resources are often limited in large-scale smart city structures, the study failed to evaluate scalability.

B. EVALUATION OF EXISTING TECHNIQUES

In this section, we provide a comparative analysis of various steganographic techniques applied in IoT systems, focusing on the type of data used to embed secret information and identifying the most commonly used methods in different studies.

Steganography techniques in the IoT employ diverse types of media as carriers to hide sensitive information. Figure 4 illustrates the proportion of research papers focused on various steganographic techniques in IoT systems. The distribution highlights the dominance of image-based steganography, which accounts for 62% of the reviewed studies due to its simplicity, high embedding capacity, and widespread applications in IoT. Network-based steganography follows with 20%, emphasizing its emerging role as a lightweight solution for secure IoT communication. Quantum steganography, with 8%, reflects its potential for future applications despite the limitations of the current infrastructure. Text, video, and audio steganography occupy smaller proportions, at 3%, 2%, and 5%, respectively, indicating limited but specialized use cases in IoT environments. The figure underscores the diverse adoption of steganographic techniques tailored to specific IoT scenarios.

The primary types of media used for embedding secret information in IoT steganography include:

- **Images:** Widely used due to their large embedding capacity and simplicity in pixel-based manipulation. Spatial domain techniques, such as least LSB substitution, are the most common for image steganography, while frequency domain approaches like DCT and DWT enhance robustness.
- **Video:** Video files are an extension of image steganography, offering a higher embedding capacity due to temporal redundancy. Hybrid methods that combine spatial domain (pixel-based) and frequency domain (DCT) approaches are widely adopted to balance capacity and robustness.
- **Audio:** Audio files provide imperceptible embedding options, utilizing the properties of human auditory perception. Techniques like LSB substitution and ML-based methods, such as adversarial training, are popular for embedding in audio steganography.
- **Hybrid:** Combining multiple media (e.g., image, video, and audio) improves data security and reliability, particularly in dynamic IoT environments such as smart cities and mission-critical systems.
- **Text:** Text steganography is characterized by its minimal storage requirements and the ease of embedding within linguistic structures.
- **Network Traffic:** Steganography in network packets is emerging as a lightweight option for secure communication in IoT. It offers significant advantages in covert data transmission without significant computational overhead.
- **Quantum:** Quantum steganography stands out for its theoretical robustness, using principles such as the no-cloning theorem and quantum uncertainty. It holds promise for future IoT systems in 6G networks and beyond.

Our analysis of IoT steganography techniques reveals immanent trade-offs between performance metrics as well as IoT constraints. In image steganography, spatial domain techniques (e.g., Khari et al. [75], IoTSteg [10]) dominate in imperceptibility (e.g., 65 dB PSNR) but suffer from low robustness to noise. Transform domain methods (e.g. Kumar et al. [78], Alkhliwi et al. [13]) prioritize robustness and high image quality (69 dB PSNR), but are resource-demanding, making them unfit for edge devices. For audio steganography, although Jiang et al. [67] propose a lightweight temporal domain audio steganography method tailored for IoT smart devices, their embedding phase remains computationally intensive. In video steganography, spatial-frequency hybrids (e.g., Koptyra and Ogiela [77]) balance efficiency and resource constraints, but introduce latency. In text steganography techniques, Gao et al. [52] linguistic approach preserves semantic integrity but requires high computational power. For network steganography, protocol-aware methods (e.g., Cabaj et al. [30]) prioritize stealth (20 bps) at the cost of throughput, while high-bandwidth approaches (e.g., Mileva et al. [95], 1.57 Mbps) are more exposed to detectability.

Based on the reviewed works, the spatial domain techniques, particularly LSB substitution, are the most widely used because of their simplicity, low computational requirements, and high embedding capacity, making them ideal for resource-constrained IoT devices. However, these techniques lack robustness against attacks and compression. For enhanced security and resilience, hybrid methods that combine spatial and frequency domains, as well as techniques integrating ML, are gaining popularity. These approaches improve imperceptibility, robustness, and capacity, addressing the limitations of simpler methods like LSB. However, the performance metrics used in the reviewed studies (e.g., PSNR, SSIM, capacity) fail to account for IoT-specific performance indicators such as energy consumption, computational overhead, or real-time processing capabilities.

The performance of hybrid methods against advanced steganalysis techniques and adversarial scenarios remains underexplored, posing risks in real-world applications. Techniques such as GAN-based and quantum steganography frequently involve high computational latency, making them unsuitable for real-time IoT applications where rapid data processing is critical. Moreover, certain methods, such as quantum steganography and CloakLoRa, require specialized hardware or infrastructure for implementation, which restricts their immediate adoption and scalability across

diverse IoT environments. Addressing these limitations is essential to improve the practicality and adoption of steganographic techniques in IoT systems.

Given these performance trade-offs, datasets play an essential role in evaluating steganographic techniques in IoT environments. The choice of dataset significantly impacts the reliability and comparability of different methods. The datasets commonly used in this domain vary depending on the medium in which the IoT data is embedded. Image datasets such as USC-SIPI and BOSSbase are widely used for image steganography. However, medical imaging datasets, such as COVID-19 chest radiographs, are used for secure healthcare IoT applications. Audio datasets, including TIMIT and LibriSpeech, are frequently used for audio steganography, particularly in smart speaker-based IoT security. Video datasets, such as the UCSD Traffic Dataset, are used in steganographic techniques designed for smart city surveillance and traffic monitoring. In addition, network traffic datasets, including custom MQTT traffic logs, are used to evaluate covert communication methods in IoT networks. However, many recent studies are based on private or experimental datasets collected from real-world IoT deployments. To improve reproducibility and comparability in IoT steganography research, there is a growing need for open dataset sharing, the use of standardized benchmark datasets, and clear documentation of dataset characteristics.

VI. CURRENT CHALLENGES AND EXPLORATORY RESEARCH AVENUES FOR ADVANCING IOT STEGANOGRAPHY

This section discusses the major challenges faced in implementing steganography in IoT environments and proposes potential solutions and emerging research avenues to address these challenges and guarantee scalability, efficiency, and robustness in IoT steganographic systems.

A. CURRENT CHALLENGES AND POTENTIAL FUTURE RESEARCH SOLUTIONS

The challenges discussed in this subsection are fundamentally tied to the distinctive characteristics of IoT settings, including resource limitations, dynamic IoT network structures, and the need for real-time data processing. By solving these challenges with innovative approaches such as lightweight algorithms, adaptive embedding, and hardware acceleration, steganography can become a practical and efficient security approach for IoT applications. The suggested solutions are based on the literature examined in previous sections, thereby ensuring a solid link between theoretical advances and practical applications in real-world IoT contexts. However, there are still many challenges to overcome in this area, such as the balance between robustness and computational efficiency, the requirement for high embedding capacity, and the scalability of steganographic methods in large-scale IoT settings. Future studies should focus on developing scalable, energy-efficient and resilient steganographic methods that can meet the changing requirements of IoT systems. By addressing these unresolved issues, steganography can significantly contribute to improving the security and privacy of IoT applications.

1) RESOURCE CONSTRAINTS

IoT devices typically face limitations in computational capabilities, memory, and energy resources, which restrict the execution of sophisticated steganographic algorithms. Methods such as GAN-based steganography [38] and quantum steganography [3] require significant computational resources and may not be practical for low-power IoT devices. Techniques in the spatial domain, such as LSB substitution [15], are lightweight but not very robust, while frequency domain approaches like DWT and DCT [78] provide enhanced security, but require more resources. To overcome these limitations, lightweight algorithms that ensure security while maintaining computational efficiency need to be proposed and implemented. Using hardware acceleration with GPUs or FPGAs [6] can relieve demanding tasks, while energy-efficient methods such as sleep mode capabilities and batch processing [98] can reduce power consumption. However, this challenge persists in developing algorithms that are both efficient and robust, as current approaches often compromise one for the other. Future studies should focus on co-designing hardware and software, adopting energy-efficient computing models, and integrating ML to improve resource allocation and embedding methods [41], ensuring that steganographic techniques remain lightweight and resilient for IoT settings. Unresolved issues include hardware dependency, energy usage, and the need for adaptable algorithms that can operate efficiently in resource-constrained settings. Solving these issues will allow the development of scalable and secure steganographic solutions tailored to the specific requirements of IoT environments.

2) LOW EMBEDDING CAPACITY

The transmission of sensitive data from IoT devices, such as those used in healthcare [2] and industrial IoT [110], poses a challenge as their limited bandwidth and storage capabilities restrict the embedding capacity of steganographic techniques. Although LSB substitution [15] provides high capacity, its vulnerability to steganalysis remains a challenge. Spatial frequency hybrid techniques [77] are more balanced in terms of capacity and robustness, but also more complex. To improve embedding capacity, the embedding rate can be adjusted based on network conditions and cover media properties with adaptive embedding techniques [40]. Data compression [124] and multilevel embedding techniques [107] can improve capacity by increasing hidden information or adding multiple levels or data domains. The integration of Generative Adversarial Networks (GANs) and self-learning AI models can dynamically optimize embedding strategies, enhancing imperceptibility and resilience against steganalysis [86]. All of these enhancements come with the challenge of achieving

high embedding capacity while still being imperceptible and robust, which remains a significant challenge. Future research directions might consider new embedding techniques that utilize temporal redundancy in video or audio files, consider hybrid techniques that blend different types of media, or optimize using ML for process automation of embedding. Moreover, decentralized embedding using other devices, improved compression methods, and novel techniques based on quantum theory could further increase the capacity. Certain IoT applications, especially those in the healthcare field, may benefit from context embedding, which could reduce capacity while maintaining sufficient robustness. The development of robust approaches for high-capacity steganography, which are required in resource-constrained contexts such as IoT environments, requires striking a balance between capacity and robustness, the amount of resources required for computational tasks, and real-time adaptability.

3) REAL-TIME PROCESSING REQUIREMENTS

Steganographic algorithms with low latency are necessary for real-time IoT applications like autonomous systems [74] and healthcare monitoring [2] to guarantee secure and rapid data transfer. Methods like audio steganography [67] and video steganography [76] frequently require complex processing, including frame-by-frame analysis or frequency domain changes, which can cause noticeable delays. Extraction and embedding processes can be improved with the use of GPUs or FPGAs [6] in embedded systems, helping to meet real-time processing requirements. Supporting edge computing systems [45] can also help reduce processing and transmission delays by analyzing data closer to its source using predictive embedding algorithms [120]. However, the challenge here is to ensure that these solutions can work efficiently in real time without sacrificing the quality of the embedded data or the IoT devices' performance. Preserving resilience and imperceptibility while embedding data in real-time remains a critical problem, particularly in scenarios where device capabilities and network conditions can change. The development of adaptive real-time steganographic algorithms that can dynamically adapt to changing network conditions, including changes in bandwidth or device resource availability, should be the main goal of future research. Research should focus on real-time AI-driven steganographic adaptation to IoT environments [32]. Real-time embedding process optimization could be achieved with methods like reinforcement learning, guaranteeing low latency and high efficiency. Furthermore, the versatility of steganographic techniques in real-time applications can be improved by including lightweight ML models designed for edge devices.

4) DYNAMIC IOT ENVIRONMENTS

Ensuring reliable and secure steganographic communication channels is challenging in IoT networks because devices frequently join and exit the network. Changes in dynamic network topology in smart cities [26] and industrial IoT [110] require flexible steganographic solutions. To deal with these changes, network steganography techniques such as HTTP header reordering and TTL modulation [30] need to be adaptable. Although decentralized designs such as blockchain [71], can guarantee secure key distribution and data integrity in dynamic contexts thanks to decentralized verification mechanisms for tamper-proof steganographic embedding, adaptive protocols [97] can adapt to changes in device availability and network configuration. In these cases, research should explore smart contract-based stego-data verification and blockchain-assisted covert communication protocols. In addition, real-time network conditions, such as latency and bandwidth, can be used to customize the steganographic process using context-sensitive embedding approaches [44]. Even with these improvements, it is still difficult to guarantee the scalability and resilience of steganographic methods in extremely dynamic IoT scenarios. Context-aware embedding techniques should be improved as future research avenues to optimize performance under a range of loads by dynamically adjusting the steganographic process based on real-time network aspects, such as latency fluctuations and bandwidth availability. In order to ensure seamless data hiding in heterogeneous environments, multi-protocol steganographic approaches [65] could enhance adaptability by allowing covert communication across various IoT protocols and networks. It is also crucial to increase resistance to network-based threats such as traffic analysis and man-in-the-middle attacks. Steganographic communication could become more secure by reducing detection risks through the use of techniques such as traffic normalization and randomized embedding patterns. Furthermore, self-healing steganographic methods that use ML to detect and recover from network disruptions could improve adaptability and guarantee continuous secret communication even in situations of device malfunctions or connectivity breakdowns. In order to facilitate secure key synchronization between devices and adjust to changes in network architecture, dynamic key management solutions such as the quantum key distribution [4] should also be investigated.

5) SCALABILITY IN DIVERSE IoT ENVIRONMENTS

Scalability poses a significant challenge in IoT steganography due to the exponential increase in connected devices, necessitating methods that can manage large-scale deployments without sacrificing performance or security. The distributed network covert channels [30] provide a scalable approach by embedding information into several devices or packets, minimizing detection risk and improving resilience. Despite their effectiveness in large-scale, diverse IoT settings are still not fully examined, especially in scenarios with differing network conditions and device functionalities. Quantum steganography [4] appears promising for scalability due to

its ability to utilize quantum concepts such as superposition and entanglement, yet its dependence on quantum infrastructure restricts its current use. To address scalability-related issues, distributed embedding methods [57] can be improved to leverage the combined resources of various IoT devices, facilitating shared hidden information throughout a network while reducing computational load on single devices. Moreover, a microservice architecture [20] improves scalability and modularity by deconstructing steganographic processes into smaller autonomous services that can be deployed across distributed IoT networks. AI-driven optimization [41] improves scalability by dynamically allocating resources and improving the embedding processes according to real-time network conditions, guaranteeing effective performance in large-scale deployments. Despite this, developing steganographic methods that are scalable in a diverse and complex IoT environment remains a major challenge, since different devices may have dynamic computational capabilities, communication protocols, or energy constraints. To increase scalability and lower latency, future research should focus on hierarchical embedding frameworks that divide the embedding process between several layers of the IoT network, including the edge, fog, and cloud layers. Training steganographic models across distributed IoT devices through federated learning for steganography could enable scalable and adaptable embedding methods without the need for centralized data processing. Furthermore, decentralized ledgers could be used by blockchain-based steganography to guarantee safe and scalable data embedding across large-scale IoT networks. In addition, to ensure effective and scalable steganographic methods, dynamic resource allocation algorithms should be proposed and implemented to adapt to the fluctuating computing and energy capabilities of IoT devices. Focusing on energy efficiency is necessary, with an emphasis on energy-efficient scalability that reduces power consumption and supports large-scale IoT networks, guaranteeing sustainability in settings with limited resources. Finally, resilience to network dynamics can be improved by developing algorithms that can manage dynamic events such as device failures, intermittent connectivity, and fluctuating traffic loads. In order to create scalable steganographic frameworks that can satisfy the requirements of extensive IoT networks, it will be crucial to address these unsolved problems and investigate the suggested future research directions. This will make it easier for steganography to be widely used in critical applications where security and scalability are crucial, such as smart cities, industrial IoT, and healthcare.

6) PRACTICAL IMPLEMENTATION IN REAL-WORLD IoT SCENARIOS

Although numerous steganographic methods have been suggested, their practical implementation in real-world IoT situations continues to pose considerable difficulties. Sophisticated techniques such as GAN-based steganography [37] and quantum steganography [3] provide significant enhancements in security and imperceptibility, but frequently require specialized hardware, substantial computational resources, or exclusive quantum systems, rendering their immediate use impractical for IoT settings with limited resources. In addition, current IoT networks function with diverse devices, each of which has varying processing power, operating systems, and communication protocols, making the seamless integration of steganographic methods more complex. To overcome this gap, edge computing integration [44] can improve the feasibility of steganographic IoT applications by offloading highly computational embedding and extraction tasks to edge nodes, reducing latency, and improving real-time performance. Moreover, hardware-software co-design approaches [6] can improve steganographic algorithms for efficient operation in particular hardware architectures of the IoT, guaranteeing that security improvements do not compromise power usage or processing speed. Standardized protocols and frameworks can enhance interoperability between various IoT ecosystems, ensuring that steganographic solutions are flexible and scalable, thus increasing their accessibility for practical implementation. However, ensuring that these approaches can be easily integrated into current IoT systems without major changes remains a significant challenge. Many IoT setups depend on legacy systems that might not allow sophisticated data embedding techniques or computationally demanding security procedures. In addition, IoT devices typically operate in unpredictable environments where aspects such as network congestion, packet loss, and intermittent connectivity might compromise steganographic communication channels, thus decreasing efficiency and reliability. Lightweight and adaptable steganographic solutions that integrate with IoT systems and maintain security and efficiency should be the main focus of future studies. Although hybrid cryptographic-steganographic models improve security with minimal computational overhead, dynamic embedding strategies may improve performance according to real-time network conditions. IoT-specific benchmarks are required to assess real-world sustainability, and cross-layer steganography could increase resilience against detection. Edge-AI integration can also allow for scalable and real-time steganographic processing. Promoting these areas will make steganography an effective and widely accepted security tool for industrial automation, smart cities, and healthcare.

B. EXPLORATORY RESEARCH AVENUES FOR ADVANCING IOT STEGANOGRAPHY

This section suggests improving IoT steganography through the integration of artificial intelligence and quantum computing, transparent, explainable AI, and microservices to ensure scalability and robustness. It emphasizes the potential of using adaptive embedding, real-time adaptability, and multitenant approaches employing Mamba models to enhance security, capacity, and resilience in dynamic IoT settings.

1) AI INTEGRATION IN QUANTUM STEGANOGRAPHY

The integration of AI with quantum steganography presents exciting opportunities to enhance the security and efficiency of information-hiding techniques in the quantum realm. Future research work in this area could focus on several key directions. Upcoming studies in this field may focus on various innovative research directions. GANs are revolutionizing steganographic techniques by generating highly realistic carriers such as images, audio, or videos, allowing hidden data to seamlessly blend with authentic content to escape detection by even the most advanced systems [86]. Reinforcement learning adds a novel aspect to steganography by enabling dynamic, context-sensitive adjustments of techniques to different IoT settings [120]. These algorithms constantly learn and modify their strategies based on network conditions, device capabilities, and possible threats, guaranteeing optimal performance while saving resources. Upcoming studies in this field may focus on various innovative research directions. For example, AI-augmented quantum embedding methods [127] can utilize ML algorithms to enhance quantum embedding, for instance, by deploying adaptive models to flexibly modify CAQWs protocols or by investigating AI-based quantum image expansion strategies to increase embedding potential. Quantum-classical hybrid methods also present encouraging solutions by merging classical AI with quantum strategies, incorporating transfer learning to connect conventional and quantum steganography or multi-task learning models to address both domains at once. To improve security, AI for quantum steganalysis resistance might use adversarial training to protect against AI-driven detection techniques or leverage quantum-inspired generative models to produce remarkably realistic cover objects. Quantum-enhanced security frameworks can combine quantum steganography with strong protocols such as QKD for layered security or use blockchain for secure and decentralized data management in IoT settings [29]. Several other quantum advances could shape future-proof steganography, including quantum entanglement-based embedding, post-quantum cryptographic integration, and quantum-resistant cover selection to counter quantum-enabled steganalysis attacks [96]. Real-world implementation issues can also be addressed through performance optimization strategies. AI algorithms can reduce quantum noise, enhancing the dependability of steganographic protocols, whereas optimization strategies can guarantee resource efficiency, allowing quantum steganography to operate effectively on near-term quantum systems. By exploring these promising research directions, AI-enhanced quantum steganography has the potential to revolutionize the field by introducing highly effective, scalable, and secure techniques for hiding data in the quantum era.

2) MICROSERVICES-BASED STEGANOGRAPHY FOR IoT

The use of microservices architecture within IoT settings [19], [20] offers numerous possibilities to improve steganographic methods by improving scalability, modularity, and resilience in dynamic and distributed frameworks. First, microservice-based frameworks can facilitate dynamic embedding methods, with different services managing functions [18] such as cover selection, embedding, and transmission, adapting in real-time to IoT requirements for improved efficiency. Future studies should explore edge-based lightweight steganographic models that operate efficiently on low-power IoT nodes [45]. Fog-assisted steganography can distribute computational tasks across intermediate network layers, reducing energy consumption and enhancing security. In addition, the idea of Steganography as a Service (StaaS), which is similar to existing approaches such as Blockchain-as-a-Service [56], provides tailored, on-demand steganographic features that organizations can easily embed into their systems without the need for extensive knowledge. Moreover, implementing steganographic algorithms in containerized environments like Docker or Kubernetes facilitates portability and quick scaling across IoT devices and networks. Lastly, multi-tenant IoT systems, in which several stakeholders utilize the same infrastructure, need steganographic methods that guarantee confidentiality for each tenant and prevent interference. Microservices can isolate steganographic tasks for each tenant, allowing secure, personalized data hiding suited to specific requirements. All of these innovative research directions take advantage of the inherent flexibility of microservices to improve steganography in IoT by improving security, efficiency, and adaptability while dealing with complex and decentralized circumstances.

3) MAMBA-ENHANCED STEGANOGRAPHY FOR IoT

Mamba [21], an advanced computational model, performs exceptionally well in identifying directional dependencies and propagating features, making it remarkably versatile for intricate data processing. Future research directions on Mamba-enhanced steganography in IoT emphasize its ability to improve data security through enhanced adaptability and resilience. Using Mamba's capabilities to extract directional dependencies, adaptive embedding techniques can effectively determine the best locations for hiding data in IoT streams. In addition, algorithms that employ Mamba's selective state-space methods may facilitate real-time adaptations, guaranteeing invisibility and resilience in highly dynamic IoT environments [84]. Furthermore, Mamba's sophisticated features can be utilized for steganalysis resistance, generating embedding patterns via adaptive skip connections that are naturally resilient against AI-based detection. In addition, Mamba-inspired deceptive embedding patterns could imitate regular IoT traffic, making detection significantly difficult. Finally, incorporating Mamba into multilayered steganography creates new opportunities, allowing data embedding in spatial, frequency, and network domains simultaneously, increasing both capacity and robustness [84]. All these methods could also be combined with existing layered security

frameworks, involving Mamba's adaptive embedding and steganographic techniques to enhance the overall protection of data streams exchanged in IoT environments.

VII. CONCLUSION

The rapid proliferation of the IoT has transformed various sectors by enabling seamless communication and data exchange between interconnected devices. However, this evolution has also introduced significant security and privacy challenges, particularly the protection of sensitive information. Steganography, with its ability to hide data within seemingly innocuous media, has emerged as a promising solution to improve IoT security. This survey provides a comprehensive review of steganographic techniques for IoT applications, categorizing them into spatial, frequency, hybrid, and emerging quantum domains. By evaluating these techniques against key metrics, we highlight their strengths and limitations in addressing IoT-specific challenges.

Despite advances, the implementation of steganography in IoT environments presents several challenges. The typical resource limitations of IoT devices, including limited computational power, memory, and energy, require that steganographic techniques be lightweight and efficient. Furthermore, the dynamic and diverse characteristics of IoT networks require scalable and adaptable steganographic solutions that can function efficiently in different scenarios. A further major challenge is to guarantee the resilience of steganographic techniques to detection by using sophisticated steganalysis methods.

Future research directions in steganography for IoT should focus on enhancing conventional steganographic methods by incorporating AI and quantum computing while maintaining transparency and clarity with explainable AI. Furthermore, using microservices will improve scalability and resilience. Important directions of improvements also include adaptive embedding methods, real-time flexibility, and multi-tenant strategies utilizing Mamba models to enhance security, capacity, and resilience in fluctuating IoT settings. All of these proposed research directions seek to establish more secure, efficient, and scalable steganography techniques designed to address the changing challenges of IoT systems.

The resolution of these challenges and the exploration of these research directions will allow steganography to enhance the security of future IoT applications. As IoT continues to grow and embed itself in different aspects of everyday life, ensuring the confidentiality and integrity of the data will be crucial. Steganography, when used alongside additional security measures, shows significant potential to protect sensitive data in this highly dynamic environment.

ACKNOWLEDGMENT

The authors would like to thank Prince Sultan University for paying the APC.

REFERENCES

[1] (2024). *Medpix*. Accessed: Sep. 10, 2024. [Online]. Available: https://medpix.nlm.nih.gov/home

[2] B. Abd-El-Atty, A. M. Iliyasu, H. Alaskar, and A. A. A. El-Latif, "A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based e-healthcare platforms," *Sensors*, vol. 20, no. 11, p. 3108, May 2020.

[3] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[4] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[5] E. W. Abood, A. M. Abdullah, M. A. Al Sibahe, Z. A. Abduljabbar, V. O. Nyangaresi, S. Ahmad Ali Kalafy, and M. J. J. Ghrabta, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bull. Electr. Eng. Informat.*, vol. 11, no. 1, pp. 185–194, Feb. 2022.

[6] A. M. Adeshina, S. F. A. Razak, S. Yogarayan, and M. S. Sayeed, "Hardware-accelerated least significant bit framework: A low cost approach to securing clinical data," *Informatica*, vol. 48, no. 22, pp. 75–84, Dec. 2024.

[7] A. Agrawal, R. Soni, and A. Tomar, "Perspective chapter: Quantum steganography—Encoding secrets," in *Steganography-The Art of Hiding Information: The Art of Hiding Information*, 2024, pp. 115–129.

[8] E. Agustsson and R. Timofte, "NTIRE 2017 challenge on single image super-resolution: Dataset and study," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 1122–1131.

[9] S. Al-Eidi, O. Darwish, and Y. Chen, "Covert timing channel analysis either as cyber attacks or confidential applications," *Sensors*, vol. 20, no. 8, p. 2417, Apr. 2020.

[10] A. Alarood, N. Ababneh, M. Al-Khasawneh, M. Rawashdeh, and M. Al-Omari, "IoTSteg: Ensuring privacy and authenticity in Internet of Things networks using weighted pixels classification based image steganography," *Cluster Comput.*, vol. 25, no. 3, pp. 1607–1618, 1607.

[11] H. N. AlEisa, "Data confidentiality in healthcare monitoring systems based on image steganography to improve the exchange of patient information using the Internet of Things," *J. Healthcare Eng.*, vol. 2022, no. 1, 2022, Art. no. 7528583.

[12] N. Alghamdi and L. Berriche, "Capacity investigation of Markov chain-based statistical text steganography: Arabic language case," in *Proc. Asia Pacific Inf. Technol. Conf.*, 2019, pp. 37–43.

[13] S. Alkhliwi, "Encryption-based image steganography technique for secure medical image transmission during the COVID-19 pandemic," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 3, pp. 83–93, 2021.

[14] A. A. Alsabhany, F. Ridzuan, and A. H. Azni, "The adaptive multi-level phase coding method in audio steganography," *IEEE Access*, vol. 7, pp. 129291–129306, 2019.

[15] M. A. Aslam, M. Rashid, F. Azam, M. Abbas, Y. Rasheed, S. S. Alotaibi, and M. W. Anwar, "Image steganography using least significant bit (LSB)—A systematic literature review," in *Proc. 2nd Int. Conf. Comput. Inf. Technol. (ICCIT)*, Aug. 2022, pp. 32–38.

[16] S. Ben Atitallah, M. Driss, and I. Almomani, "A novel detection and multi-classification approach for IoT-malware using random forest voting of fine-tuning convolutional neural networks," *Sensors*, vol. 22, no. 11, p. 4302, Jun. 2022.

[17] S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, "Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions," *Comput. Sci. Rev.*, vol. 38, Nov. 2020, Art. no. 100303.

[18] S. Ben Atitallah, M. Driss, and H. Ben Ghezala, "FedMicro-IDA: A federated learning and microservices-based framework for IoT data analytics," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100845.

[19] S. B. Atitallah, M. Driss, and H. B. Ghézala, "Revolutionizing disease diagnosis: A microservices-based architecture for privacy-preserving and efficient IoT data analytics using federated learning," *Proc. Comput. Sci.*, vol. 225, pp. 3322–3331, Aug. 2023.

[20] S. B. Atitallah, M. Driss, and H. B. Ghzela, "Microservices for data analytics in IoT applications: Current solutions, open challenges, and future research directions," *Proc. Comput. Sci.*, vol. 207, pp. 3938–3947, May 2022.

[21] S. Ben Atitallah, C. Ben Rabah, M. Driss, W. Boulila, and A. Koubaa, "Exploring graph mamba: A comprehensive survey on state-space models for graph learning," 2024, *arXiv:2412.18322*.

[22] M. Bai, J. Yang, K. Pang, Y. Huang, and Y. Gao, "Semantic steganography: A framework for robust and high-capacity information hiding using large language models," 2024, *arXiv:2412.11043*.

[23] T. Baker, C. Liang, and Y. Li, "A reliable covert channel for stealthy data transmission for Internet-of-Underwater-Things," *IEEE Internet Things Mag.*, vol. 5, no. 4, pp. 42–46, Dec. 2022.

[24] P. Bedi and A. Dua, "Network steganography using extension headers in IPv6," in *Proc. Int. Conf. Inf., Commun. Comput. Technol.* Cham, Switzerland: Springer, Jan. 2020, pp. 98–110.

[25] S. B. Atitallah, M. Driss, W. Boulila, and I. Almomani, "An effective detection and classification approach for DoS attacks in wireless sensor networks using deep transfer learning models and majority voting," in *Proc. Int. Conf. Comput. Collective Intell.* Cham, Switzerland: Springer, Jan. 2022, pp. 180–192.

[26] D. Bi, S. Kadry, and P. M. Kumar, "Internet of Things assisted public security management platform for urban transportation using hybridised cryptographic-integrated steganography," *IET Intell. Transp. Syst.*, vol. 14, no. 11, pp. 1497–1506, Nov. 2020.

[27] J. Bian, A. A. Arafat, H. Xiong, J. Li, L. Li, H. Chen, J. Wang, D. Dou, and Z. Guo, "Machine learning in real-time Internet of Things (IoT) systems: A survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8364–8386, Jun. 2022.

[28] S. Bistarelli, M. Ceccarelli, C. Luchini, I. Mercanti, and F. Santini, "A survey of steganography tools at layers 2–4 and HTTP," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–9.

[29] S. Biswas, R. S. Goswami, and K. H. K. Reddy, "Advancing quantum steganography: A secure IoT communication with reversible decoding and customized encryption technique for smart cities," *Cluster Comput.*, vol. 27, no. 7, pp. 9395–9414, Oct. 2024.

[30] K. Cabaj, P. Żórawski, P. Nowakowski, M. Purski, and W. Mazurczyk, "Efficient distributed network covert channels for Internet of Things environments," *J. Cybersecurity*, vol. 6, no. 1, Jan. 2020, Art. no. tyaa018.

[31] A.-M.-V. M. Calo, F. B. Calanda, and R. P. Medina, "Novel self-sufficient coverless video steganography for secured Internet of Things (IoT) communication," in *Proc. IEEE 4th Int. Conf. Electron. Commun., Internet Things Big Data (ICEIB)*, Apr. 2024, pp. 133–138.

[32] Y. Cao, J. Li, K. Chao, J. Xiao, and G. Lei, "Blockchain meets generative behavior steganography: A novel covert communication framework for secure IoT edge computing," *Chin. J. Electron.*, vol. 33, no. 4, pp. 886–898, Jul. 2024.

[33] E. Chae, J. Choi, and J. Kim, "An elementary review on basic principles and developments of qubits for quantum computing," *Nano Converg.*, vol. 11, no. 1, pp. 11–18, Mar. 2024.

[34] J. Chaharlang, "A novel quantum steganography-steganalysis system for audio signals," *Multimedia Tools Appl.*, vol. 79, no. 19, pp. 13903–13921, 2020, doi: 10.1007/s11042-020-08694-z.

[35] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wireless Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, Feb. 1667.

[36] C. C. Chang, Y. Liu, and T. S. Nguyen, "A novel turtle shell based scheme for data hiding," in *Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2014, pp. 89–93.

[37] K. Chen, F. Yan, A. M. Iliyasu, and J. Zhao, "Exploring the implementation of steganography protocols on quantum audio signals," *Int. J. Theor. Phys.*, vol. 57, no. 2, pp. 476–494, Feb. 2018.

[38] S. Chen, C.-C. Chang, and I. Echizen, "Steganographic secret sharing with GAN-based face synthesis and morphing for trustworthy authentication in IoT," *IEEE Access*, vol. 9, pp. 116427–116439, 2021.

[39] J. P. Cohen, P. Morrison, L. Dao, K. Roth, T. Q. Duong, and M. Ghassemi, "COVID-19 image data collection: Prospective predictions are the future," 2020, *arXiv:2006.11988*.

[40] X. Dai, Z. He, X. Zhang, and Z. Fu, "SCGM: Asymmetric steganographic embedding cost learning with adaptive modulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 11, pp. 12073–12085, Nov. 2024.

[41] N. J. D. L. Croix, T. Ahmad, and F. Han, "Comprehensive survey on image steganalysis using deep learning," *Array*, vol. 22, Jul. 2024, Art. no. 100353.

[42] M. De Vincenzi, J. Moore, B. Smith, S. E. Sarma, and I. Matteucci, "Security risks and designs in the connected vehicle ecosystem: In-vehicle and edge platforms," *IEEE Open J. Veh. Technol.*, vol. 6, pp. 442–454, 2025.

[43] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, and S. K. Pani, "SSII: Secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT," *IEEE Access*, vol. 9, pp. 87563–87578, 2021.

[44] C. Ding, Z. Fu, Z. Yang, Q. Yu, D. Li, and Y. Huang, "Context-aware linguistic steganography model based on neural machine translation," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 32, pp. 868–878, 2024.

[45] X. Ding, Y. Xie, P. Li, M. Cui, and J. Chen, "Image steganography based on artificial immune in mobile edge computing with Internet of Things," *IEEE Access*, vol. 8, pp. 136186–136197, 2020.

[46] F. Djebbar, "Securing IoT data using steganography: A practical implementation approach," *Electronics*, vol. 10, no. 21, p. 2707, Nov. 2021.

[47] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP J. Audio, Speech, Music Process.*, vol. 2012, no. 1, pp. 1–16, Dec. 2012.

[48] H. Dutta, R. K. Das, S. Nandi, and S. R. M. Prasanna, "An overview of digital audio steganography," *IETE Tech. Rev.*, vol. 37, no. 6, pp. 632–650, Nov. 2020.

[49] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The Pascal visual object classes (VOC) challenge," *Int. J. Comput. Vis.*, vol. 88, no. 2, pp. 303–338, Jun. 2010.

[50] O. Evsutin, A. Melman, and A. A. A. El-Latif, "Overview of information hiding algorithms for ensuring security in IoT based cyber-physical systems," in *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*. Cham, Switzerland: Springer, 2022, pp. 81–115.

[51] W. Fei, H. Ohno, and S. Sampalli, "A systematic review of IoT security: Research potential, challenges, and future directions," *ACM Comput. Surv.*, vol. 56, no. 5, pp. 1–40, May 2024.

[52] K. Gao, J.-H. Horng, C.-C. Chang, and C.-C. Chang, "Linguistic secret sharing via ambiguous token selection for IoT security," *Electronics*, vol. 13, no. 21, p. 4216, Oct. 2024.

[53] J. S. Garofolo, L. F. Lamel, W. M. Fisher, and J. G. Fiscus, "Getting started with the darpa timit CD-ROM: An acoustic phonetic continuous speech database," NIST, Gaithersburgh, MD, USA, Tech. Rep. NISTIR 4930, 1988, vol. 107.

[54] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arabian J. Sci. Eng.*, vol. 45, no. 4, pp. 2631–2644, Apr. 2020.

[55] Y. Hajjaji, W. Boulila, I. R. Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100318.

[56] D. Hasan and M. Driss, "SUBLμME: Secure blockchain as a service and microservices-based framework for IoT environments," in *Proc. IEEE/ACS 18th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2021, pp. 1–9.

[57] S. S. Hashmi, A. A. K. Mohammad, A. M. Abdul, C. Atheeq, and M. K. Nizamuddin, "Enhancing data security in multi-cloud environments: A product cipher-based distributed steganography approach," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 1, pp. 47–61, Feb. 2024.

[58] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A novel image steganography method for industrial Internet of Things security," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7743–7751, Nov. 2021.

[59] S. Heidari, M. Vafaei, M. Houshmand, and N. Tabatabaey-Mashadi, "A dual quantum image scrambling method," *Quantum Inf. Process.*, vol. 18, no. 1, pp. 9–15, Jan. 2019.

[60] N. Hou, X. Xia, and Y. Zheng, "CloakLoRa: A covert channel over LoRa PHY," *IEEE/ACM Trans. Netw.*, vol. 31, no. 3, pp. 1159–1172, Mar. 2022.

[61] *Methods for Subjective Determination of Speech Quality*, ITU-T Recommendation, Geneva, Switzerland, 2003.

[62] *Perceptual Evaluation of Speech Quality (PESQ), and Objective Method for End-to-End Speech Quality Assessment of Narrowband Telephone Networks and Speech Codecs*, ITU, Geneva, Switzerland, 2000, p. 862.

[63] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: A comprehensive review," *Health Technol.*, vol. 12, no. 1, pp. 9–31, Jan. 2022.

[64] A. Jan, S. A. Parah, B. A. Malik, and M. Rashid, "Secure data transmission in IoTs based on CLoG edge detection," *Future Gener. Comput. Syst.*, vol. 121, pp. 59–73, Aug. 2021.

[65] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "PadSteg: Introducing inter-protocol steganography," *Telecommun. Syst.*, vol. 52, pp. 1101–1111, Sep. 2011.

[66] N. Jiang, N. Zhao, and L. Wang, "LSB based quantum image steganography algorithm," *Int. J. Theor. Phys.*, vol. 55, no. 1, pp. 107–123, Jan. 2016.

[67] S. Jiang, D. Ye, J. Huang, Y. Shang, and Z. Zheng, "SmartSteganography: Light-weight generative audio steganography model for smart embedding application," *J. Netw. Comput. Appl.*, vol. 165, Sep. 2020, Art. no. 102689, doi: 10.1016/j.jnca.2020.102689.

[68] L. Jiyu. (2024). *Bossbase: A Dataset for Blind/No-Reference Image Quality Assessment, 2024*. Accessed: Sep. 10, 2024. [Online]. Available: https://www.kaggle.com/datasets/lijiyu/bossbase

[69] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[70] R. Joshi, A. Gupta, K. Thapliyal, R. Srikanth, and A. Pathak, "Hide and seek with quantum resources: New and modified protocols for quantum steganography," *Quantum Inf. Process.*, vol. 21, no. 5, p. 164, May 2022.

[71] V. Kanth and B. Hale, "Blockchain-based authenticated stego-channels and application to Ethereum," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 1, pp. 373–387, Jan. 2025.

[72] T. Karras, T. Aila, S. Laine, and J. Lehtinen, "Progressive growing of GANs for improved quality, stability, and variation," 2017, *arXiv:1710.10196*.

[73] M. Kaur, A. A. AlZubi, T. S. Walia, V. Yadav, N. Kumar, D. Singh, and H. N. Lee, "Egcrypto: A low-complexity elliptic Galois cryptography model for secure data transmission in IoT," *IEEE Access*, vol. 11, pp. 90739–90748, 2023.

[74] S. Khan, N. Abbas, M. Nasir, K. Haseeb, T. Saba, A. Rehman, and Z. Mehmood, "Steganography-assisted secure localization of smart devices in Internet of Multimedia Things (IoMT)," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17045–17065, May 2021.

[75] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 73–80, Jan. 2020.

[76] K. Koptyra and M. R. Ogiela, "Steganography in IoT: Information hiding with APDS-9960 proximity and gestures sensor," *Sensors*, vol. 22, no. 7, p. 2612, Mar. 2022.

[77] K. Koptyra and M. R. Ogiela, "Steganography in IoT: Information hiding with joystick and touch sensors," *Sensors*, vol. 23, no. 6, p. 3288, Mar. 2023.

[78] B. Kumar Pandey, D. Pandey, V. K. Nassa, T. Ahmad, C. Singh, A. S. George, and M. A. Wakchaure, "Encryption and steganography-based text extraction in IoT using the EWCTS optimizer," *Imag. Sci. J.*, vol. 69, nos. 1–4, pp. 38–56, May 2021.

[79] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: Recent advances and challenges," *Multimedia Tools Appl.*, vol. 82, no. 27, pp. 41943–41985, Nov. 2023.

[80] S. Latif, W. Boulila, A. Koubaa, Z. Zou, and J. Ahmad, "DTL-IDS: An optimized intrusion detection framework using deep transfer learning and genetic algorithm," *J. Netw. Comput. Appl.*, vol. 221, Jan. 2024, Art. no. 103784.

[81] S. Lazzaro and F. Buccafurri, "Stealthy messaging: Leveraging message queuing telemetry transport for covert communication channels," *Appl. Sci.*, vol. 14, no. 19, p. 8874, Oct. 2024.

[82] F. Lehner, W. Mazurczyk, J. Keller, and S. Wendzel, "Inter-protocol steganography for real-time services and its detection using traffic coloring approach," in *Proc. IEEE 42nd Conf. Local Comput. Netw. (LCN)*, Oct. 2017, pp. 78–85, doi: 10.1109/LCN.2017.32.

[83] J. Li, C. Yu, B. B. Gupta, and X. Ren, "Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4545–4561, Feb. 2018, doi: 10.1007/s11042-017-4452-0.

[84] S. Li, T. Zhu, F. Duan, L. Chen, H. Ning, C. Nugent, and Y. Wan, "HARMamba: Efficient and lightweight wearable sensor human activity recognition based on bidirectional mamba," *IEEE Internet Things J.*, vol. 12, no. 3, pp. 2373–2384, Feb. 2025.

[85] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft COCO: Common objects in context," in *Proc. Eur. Conf. Comput. Vis.*, 2014, pp. 740–755.

[86] J. Liu, Y. Ke, Z. Zhang, Y. Lei, J. Li, M. Zhang, and X. Yang, "Recent advances of image steganography with generative adversarial networks," *IEEE Access*, vol. 8, pp. 60575–60597, 2020.

[87] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, Mar. 2019.

[88] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 225–229, May 2014.

[89] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *J. Comput. Commun.*, vol. 3, no. 5, pp. 164–173, 2015.

[90] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," *Mathematics*, vol. 9, no. 21, p. 2829, Nov. 2021.

[91] J. K. Mandal, S. Dey, and A. Kumar, "A novel steganographic approach for secured communication via boustrophedon transformation to develop IoT-based smart city," *IETE J. Res.*, vol. 69, no. 9, pp. 5764–5772, Sep. 2023.

[92] P. Maurya, L. Daksha, V. Kahar, and A. A. Kherani, "Performance analysis of CoLoRa: Covert channel over LoRa PHY," in *Proc. Nat. Conf. Commun. (NCC)*, Feb. 2024, pp. 1–6.

[93] W. Mazurczyk, P. Szary, S. Wendzel, and L. Caviglione, "Towards reversible storage network covert channels," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, Aug. 2019, pp. 1–8.

[94] T. Mihara, "Quantum steganography using prior entanglement," *Phys. Lett. A*, vol. 379, nos. 12–13, pp. 952–955, Jun. 2015.

[95] A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, and W. Mazurczyk, "Comprehensive analysis of mqtt 5.0 susceptibility to network covert channels," *Comput. Secur.*, vol. 104, Jun. 2021, Art. no. 102207.

[96] N. Min-Allah, N. Nagy, M. Aljabri, M. Alkharraa, M. Alqahtani, D. Alghamdi, R. Sabri, and R. Alshaikh, "Quantum image steganography schemes for data hiding: A survey," *Appl. Sci.*, vol. 12, no. 20, p. 10294, Oct. 2022.

[97] F. Mir and F. Meziane, "Novel adaptive DCOPA using dynamic weighting for vector of performances indicators optimization of IoT networks," *Expert Syst. Appl.*, vol. 247, Aug. 2024, Art. no. 123212.

[98] A. Mukherjee, S. Ghosh, S. K. Ghosh, and R. Buyya, "Mobi-sense: Mobility-aware sensor-fog paradigm for mission-critical applications using network coding and steganography," *J. Supercomput.*, vol. 79, no. 15, pp. 17495–17518, Oct. 2023.

[99] S. Namasudra, "A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure," *Comput. Electr. Eng.*, vol. 104, Dec. 2022, Art. no. 108426.

[100] H. A. Nassrullah, W. N. Flayyih, and M. A. Nasrullah, "Enhancement of LSB audio steganography based on carrier and message characteristics," *J. Inf. Hiding Multim. Signal Process.*, vol. 11, no. 3, pp. 126–137, 2020.

[101] N. N. Alghamdi, L. Berriche, and M. Alrabiah, "Steganalysis of Markov chain-based statistical text steganography," *Int. J. Comput. Digit. Syst.*, vol. 12, no. 1, pp. 1553–1559, Dec. 2022.

[102] M. R. Nur Octafian, L. Novamizanti, I. Safitri, and R. P. Sitepu, "Audio steganography technique using DCT-SWT with RC4 encryption," in *Proc. Int. Conf. Data Sci. Its Appl. (ICoDSA)*, Jul. 2022, pp. 35–40.

[103] V. Panayotov, G. Chen, D. Povey, and S. Khudanpur, "Librispeech: An ASR corpus based on public domain audio books," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 5206–5210.

[104] S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2101–2132, 3rd Quart., 2018.

[105] L. Y. Por, T. Ang, and B. Delina, "Whitesteg: A new scheme in information hiding using text steganography," *WSEAS Trans. Comput.*, vol. 7, no. 6, pp. 735–745, 2008.

[106] R. Prabhu, P. Archana, S. Anusooya, and P. Anuradha, "Improved steganography for IoT network node data security promoting secure data transmission using generative adversarial networks," *Sci. Temper*, vol. 14, no. 3, pp. 938–943, Sep. 2023.

[107] O. A. Qasim and S. Golshannavaz, "Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography," *e-Prime-Adv. Electr. Eng., Electron. Energy*, vol. 10, Dec. 2024, Art. no. 100834.

[108] J. Qin, J. Cheng, S. Liang, Z. Yan, H. Lu, and X. Jia, "Noiseless and efficient quantum information transmission for fiber-based continuous-variable quantum networks," *Phys. Rev. Appl.*, vol. 21, no. 6, Jun. 2024, Art. no. 064026.

[109] Z. Qu, Z. Chen, X. Ning, and P. Tiwari, "QEPP: A quantum efficient privacy protection protocol in 6G-quantum Internet of Vehicles," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 1, pp. 905–916, Jan. 2024.

[110] M. Ragab, S. Alshehri, H. A. Alhadrami, F. Kateb, E. B. Ashary, and S. Abdel-Khalek, "Encryption with image steganography based data hiding technique in IIoT environment," *Comput., Mater. Continua*, vol. 72, no. 1, pp. 1323–1338, 2022.

[111] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the Internet of Things based on steganography and chaotic functions," *Optik*, vol. 258, May 2022, Art. no. 168864.

[112] S. Anguraj, S. P. Shantharajah, and J. J. Emilyn, "A steganographic method based on optimized audio embedding technique for secure data communication in the Internet of Things," *Comput. Intell.*, vol. 36, no. 2, pp. 557–573, May 2020.

[113] G. S. Septinaputri, A. W. C. D'Layla, N. J. De La Croix, and T. Ahmad, "Enhanced spatial domain image steganography for improved IoT security and privacy applications," in *Proc. IEEE 21st Int. Conf. Mobile Ad-Hoc Smart Syst. (MASS)*, Sep. 2024, pp. 635–640.

[114] R. Severino, J. Rodrigues, J. Alves, and L. L. Ferreira, "Performance assessment and mitigation of timing covert channels over the IEEE 802.15.4," *J. Sensor Actuator Netw.*, vol. 12, no. 4, p. 60, Aug. 2023.

[115] Signal Image Process. Inst. (2024). *Usc-sipi Image Database*. Accessed: Sep. 5, 2024. [Online]. Available: https://sipi.usc.edu/database/

[116] A. Steane, "Quantum computing," *Rep. Prog. Phys.*, vol. 61, no. 2, p. 117, 1998.

[117] A. Stubbs and Ö. Uzuner, "Annotating risk factors for heart disease in clinical narratives for diabetic patients," *J. Biomed. Informat.*, vol. 58, pp. S78–S91, Dec. 2015.

[118] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021.

[119] E. A. S. S. Kola, "Review on lightweight cryptography techniques and steganography techniques for IoT environment," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 9, pp. 3436–3444, Nov. 2023.

[120] W. Tang, B. Li, M. Barni, J. Li, and J. Huang, "An automatic cost learning framework for image steganography using deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 952–967, 2021.

[121] S. Ullah, W. Boulila, A. Koubâa, and J. Ahmad, "MAGRU-IDS: A multi-head attention-based gated recurrent unit for intrusion detection in IIoT networks," *IEEE Access*, vol. 11, pp. 114590–114601, 2023.

[122] Ambika, Virupakshappa, and S. Veerashetty, "Secure communication over wireless sensor network using image steganography with generative adversarial networks," *Meas., Sensors*, vol. 24, Dec. 2022, Art. no. 100452.

[123] O. Veselska, O. Lavrynenko, R. Odarchenko, M. Zaliskyi, D. Bakhtiiarov, M. Karpinski, and S. Rajba, "A wavelet-based steganographic method for text hiding in an audio signal," *Sensors*, vol. 22, no. 15, p. 5832, Aug. 2022.

[124] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021.

[125] A. Waheed, M. Goyal, D. Gupta, A. Khanna, F. Al-Turjman, and P. R. Pinheiro, "CovidGAN: Data augmentation using auxiliary classifier GAN for improved COVID-19 detection," *IEEE Access*, vol. 8, pp. 91916–91923, 2020.

[126] M. Wang, S. Cao, and Y. Wang, "VoNR-IPD: A novel timing-based network steganography for industrial Internet," *Secur. Commun. Netw.*, vol. 2020, Jun. 2020, Art. no. 8846230.

[127] R. W. Wardhani, D. S. C. Putranto, T.-T.-H. Le, J. Ji, and H. Kim, "Toward hybrid classical deep learning-quantum methods for steganalysis," *IEEE Access*, vol. 12, pp. 45238–45252, 2024.

[128] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc.-Vis., Image, Signal Process.*, vol. 152, no. 5, pp. 611–615, 2005.

[129] L. Xiang, G. Guo, J. Yu, V. S. Sheng, and P. Yang, "A convolutional neural network-based linguistic steganalysis for synonym substitution steganography," *Math. Biosci. Eng.*, vol. 17, no. 2, pp. 1041–1058, 1041.

[130] L. Xiang, C. Ou, and D. Zeng, "Linguistic steganography: Hiding information in syntax space," *IEEE Signal Process. Lett.*, vol. 31, pp. 261–265, 2024.

[131] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 3, pp. 44–57, 3rd Quart., 2007.

[132] Q. Zeng and K. Wang, "Steganographic text generation based on large language models in dialogue scenarios," in *Proc. CCF Int. Conf. Natural Language Process. Chin. Comput.* Cham, Switzerland: Springer, 2024, pp. 475–487.

[133] L. Zhu, X. Luo, C. Yang, Y. Zhang, and F. Liu, "Invariances of JPEG-quantized DCT coefficients and their application in robust image steganography," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 108015.

MAHA DRISS (Senior Member, IEEE) received the engineering (Hons.) and M.Sc. degrees in computer science from the National School of Computer Science, University of Manouba, Manouba, Tunisia, in 2006 and 2007, respectively, and the Ph.D. degree from the University of Rennes 1, Rennes, France, in 2011. From 2012 to 2015, she was an Assistant Professor of computer science with the National Higher Engineering School of Tunis, University of Tunis, Tunis, Tunisia. From 2015 to 2021, she was an Assistant Professor of computer science with Taibah University, Medina, Saudi Arabia. She is currently an Associate Professor of computer science with Prince Sultan University, Riyadh, Saudi Arabia, and an Active Researcher with the RIOTU Laboratory, Prince Sultan University. She published more than 80 papers in well-reputable journals and conferences. Her primary research interests include the IoT, AI, service computing, distributed systems, and cybersecurity. She is a member of ACM. She was a reviewer in several world-leading high-impact journals and she has chaired tracks and participated as a reviewer at a number of international conferences. She is among Stanford University's list of the World's Top 2% of Scientists.

LAMIA BERRICHE received the engineering degree from French National School of Civil Aviation (ENAC), in 2001, the master's degree in computer science, Networking and Telecommunication from the National Polytechnic Institute Toulouse, France, in 2001, and the Ph.D. degree in signal and image processing from Telecom Paris Tech, France, in 2006. From 2007 to 2019, she was an Assistant Professor with the Computer Science Department, Imam Muhammad Ibn Saud Islamic University, Saudi Arabia. She is currently an Assistant Professor with the Computer Science Department, Prince Sultan University, Saudi Arabia.

SAFA BEN ATITALLAH received the B.Sc. degree (Hons.) in information systems from the College of Computer Science and Engineering (CCSE), Taibah University, Saudi Arabia, in 2019, and the Ph.D. degree (Hons.) in computer science from the National School of Computer Science (ENSI), University of Manouba, Tunisia, in 2023. She is currently a Postdoctoral Researcher with the Robotics and Internet of Things (RIOTU) Laboratory, Prince Sultan University, Saudi Arabia, and a Senior Researcher with the RIADI Laboratory, Tunisia. She has contributed to several projects, focusing on the IoT and AI-based solutions. Her research focuses on cutting-edge technologies, including AI, DL, the IoT, federated learning, self-supervised learning, few-shot learning, and cybersecurity. Her work includes applications in smart healthcare, smart cities, and graph learning.

SIWAR REKIK received the M.Sc. degree in computer science and systems engineering from the University of Rouen, France, in 2007, and the Ph.D. degree in computer science (signals processing and telecommunications) from the University of Western Brittany (UBO), Brest, France, in 2012. From 2009 to 2012, she was a Lecturer in computer engineering with Canadian University Dubai, Dubai, United Arab Emirates. She was an Assistant Professor of computer science with Al-Imam University, Riyadh, Saudi Arabia, from 2012 to 2020. She is currently an Assistant Professor of computer technology with Prince Sultan University, Riyadh. Her research interests include speech steganography and watermarking, digital signal processing, information hiding, pattern recognition, image processing, and blockchain.