Recent Digital Systems Information Hiding Techniques via Internet Technology: A Review

Trong-The Nguyen[1], Truong-Giang Ngo[2], Shu-Chuan Chu[3], Thi-Kien Dao[1,4], Thi-Thanh-Tan Nguyen[5]*

[1] School of Electronic Engineering, Fuzhou Institute of Technology, China
[2] Faculty of Computer Science and Engineering, Thuyloi University, Vietnam
[3] College of Computer Science and Engineering, Shandong University of Science and Technology, China
[4] MMLab, University of Information Technology, Vietnam
[5] Information Technology Faculty, Electric Power University, Vietnam
1100405110@nkust.edu.tw, giangnt@tlu.edu.vn, scchu0803@gmail.com,
1101405123@nkust.edu.tw, tanntt@epu.edu.vn

Abstract

Recent advancements in digital systems and internet technology have raised concerns about information security and privacy. Information hiding techniques (IHTs), such as steganography, watermarking, and covert channels, play a crucial role in protecting sensitive data from unauthorized access. This research review paper provides a comprehensive overview of the recent developments in information hiding techniques via internet technology. The paper discusses methodologies, algorithms, and tools used to conceal information within digital media, network protocols, and web applications. It also explores the challenges and future directions in this field, highlighting the need for enhanced security measures and privacy protection. This review serves as a valuable resource for researchers, practitioners, and policymakers interested in understanding and advancing information hiding techniques in the digital era over the internet.

Keywords: Information hiding techniques, Recent digital systems, Internet technology, Steganography

1 Introduction

In the digital age with Internet technology, where information is readily accessible and transmitted through various digital systems, ensuring sensitive data's security and privacy has become paramount [1-2]. Cyberattacks and unauthorized access to information pose significant threats to individuals, organizations, and governments [3-4]. Information hiding techniques (IHTs) have emerged as a crucial aspect of information security [5], allowing the concealment of data within digital objects to protect it from unauthorized detection or extraction [6]. With the pervasive use of internet technology in our daily lives [7], it becomes essential to examine the recent advancements in information hiding techniques specifically tailored for digital systems using internet-based technologies [8].

The rapid growth of digital systems and the widespread use of the internet have led to an exponential increase in data transfer and storage capabilities [9]. This growth has also brought forth numerous security challenges, with hackers and cybercriminals constantly evolving their techniques to exploit vulnerabilities [10]. Information hiding techniques, rooted in the concept of steganography and watermarking, have been employed for centuries to hide messages and protect the integrity of data [11]. However, with the advent of internet technology, new challenges and opportunities have emerged, necessitating the development of innovative information hiding techniques [12].

The motivation behind this research review paper lies in the need to comprehensively understand the recent advancements in IHTs that are specifically tailored for digital systems utilizing internet technology [13]. By exploring the latest methodologies, algorithms, and tools employed in information hiding, we can identify the strengths and limitations of existing techniques [14]. This understanding enables researchers, practitioners, and policymakers to develop more robust and effective approaches to protect sensitive information and enhance information security.

The objectives of this research review paper are listed as follows:

- To provide an extensive overview of recent advancements in information hiding techniques specifically designed for digital systems using internet technology.
- To categorize and analyze different information hiding methodologies, algorithms, and tools and examine their applicability in digital objects, network protocols, and web applications.
- To evaluate the strengths and limitations of existing information hiding techniques in terms of security, detectability, and resilience against attacks.
- To identify the challenges and obstacles faced by information hiding techniques in internet-based digital systems.

*Corresponding Author: Truong-Giang Ngo; Email: giangnt@tlu.edu.vn
DOI: https://doi.org/10.70003/160792642025092605007

- To propose potential future directions for research and development in the field of information hiding, considering emerging trends and technologies.

This research review paper focuses on recent information hiding techniques applicable to digital systems that utilize internet technology. It covers a broad range of methodologies, including steganography, watermarking, and covert channels, and examines their implementation in digital media, network protocols, and web applications. The paper also explores the challenges faced by information hiding techniques in terms of security, detectability, and privacy concerns. Although the scope is comprehensive, it is important to acknowledge that the paper may not include every single information hiding technique or address every specific application.

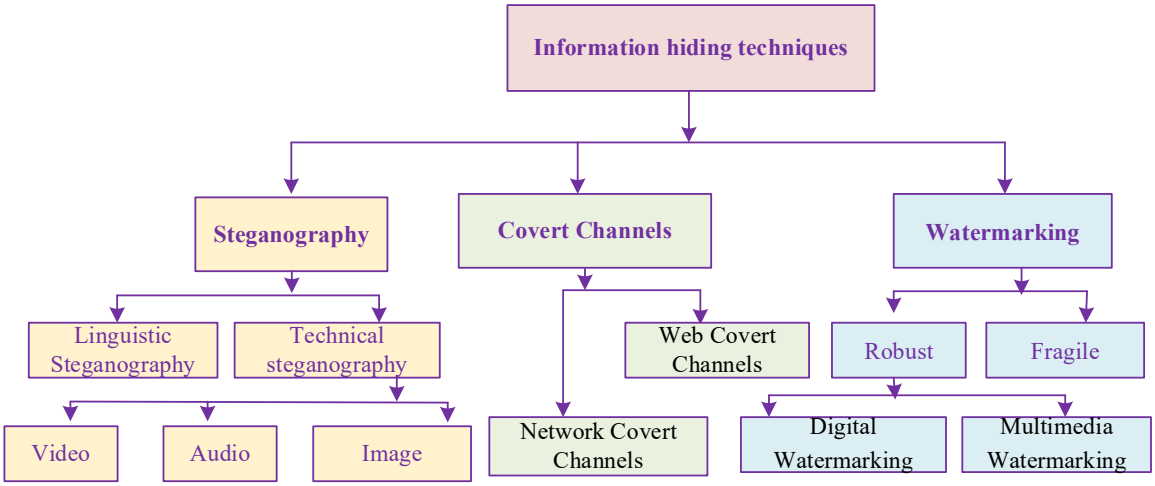

Figure 1. Classification of the IHTs: steganography, watermarking, and covert channel techniques

Table 1. A comprehensive information-hiding techniques with specific features

Techniques	Subcategories	Explanation features
Steganography [13, 17]	Image Steganography	Hides information within digital images using techniques like LSB manipulation, allowing secret communication or copyright protection.
	Audio Steganography	Conceals information within audio files without perceptible changes, using techniques like LSB manipulation or spread spectrum modulation.
	Video Steganography	Hides information within video files, employing techniques such as LSB manipulation, motion vectors, or temporal/spatial transformations.
Watermarking [14, 18-19]	Digital Watermarking	Embeds a digital signature or identifier directly into digital content, ensuring authenticity, ownership, or copyright protection.
	Multimedia Watermarking	Extends digital watermarking to multiple types of multimedia data, ensuring integrity and ownership across different media types.
Covert channels [20]	Network Covert Channels	Utilizes existing network protocols or functionalities to transmit hidden information, bypassing security measures within network traffic.
	Web Covert Channels	Utilizes web technologies and protocols to transmit data surreptitiously, hiding information within HTTP headers, web page structures, etc.

2 Information Hiding Techniques

The majority of IHTs have steganography, watermarking, and covert channel techniques [5, 15]. The IHTs refer to various methods and strategies to conceal or protect sensitive or valuable information from unauthorized access or detection. These techniques aim to ensure data confidentiality, integrity, and availability [16]. Figure 1 illustrates the classification of most IHTs, e.g., steganography, watermarking, and covert channel techniques. The section presents some standard information-hiding techniques.

2.1 Steganography

Steganography is the practice of hiding information within other data (the carrier) in such a way that it is concealed from unauthorized viewers [13, 17]. Steganography is the practice of concealing information within another form of data, such as an image, audio file, or video, in order to hide its existence. It involves embedding the secret message into the cover medium in a way that is imperceptible to human senses. Let *C* be the cover medium, and M be the secret message. The following steps can represent the steganography process.

Step 1. Input the cover medium *C* and the secret message *M*.

Step 2. Convert the cover medium C into a suitable format (e.g., image, audio, video)

Step 3. Analyze the cover medium to identify potential areas for embedding the secret message

Step 4. Encode the secret message M into a format suitable for embedding (e.g., binary, ASCII)

Step 5. Embed the encoded secret message into the cover medium C, following a specific algorithm or technique

Step 6. Generate the stego medium Stego by combining the modified cover medium C and the embedded secret message

Step 7. Output the stego medium Stego

Algorithm 1 displays a pseudocode of a basic steganography scheme.

Algorithm 1. A pseudocode of basic steganography scheme

```
function steganography (coverImage, secretMessage):
    stegoImage = copy(coverImage)  // Create a copy of the cover image
    secretBits = convertToBits(secretMessage)
    // Convert secret message to binary bits
    index = 0  // Initialize index for secret bits
    for each pixel in stegoImage:
        if index < length(secretBits):
            pixelBits = convertToBits(pixel)
            // Convert pixel value to binary bits
            // Modify the least significant bit of each
            color channel of the pixel
            pixelBits[0] = secretBits[index]
            // Convert modified pixel bits back to
            decimal value
            modifiedPixel =
convertToDecimal(pixelBits)
            stegoImage.setPixelValue(pixel, modifiedPixel)
            //Update pixel value in stego image
            index = index + 1
            // Move to the next secret bit
        else:
            break
    // All secret bits have been embedded
    return stegoImage
```

Note that this pseudocode assumes a simple LSB (Least Significant Bit) steganography technique, where the least significant bit of each color channel in the cover image is modified to embed the secret message. The convertToBits() and convertToDecimal() functions are used to convert between binary and decimal representations of pixel values [11]. Figure 2 shows the structure of the steganography scheme.

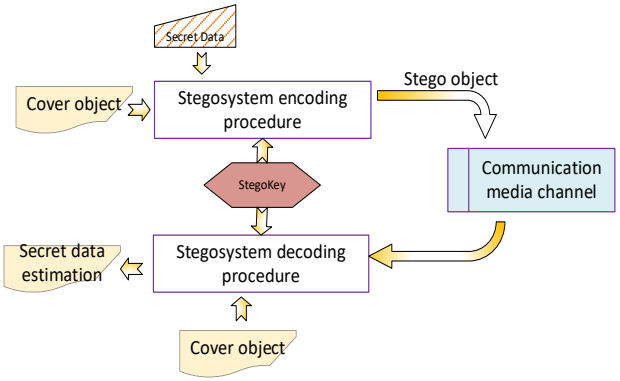

Figure 2. A structure of the steganography scheme

The subcategories of steganography is expressed as follows.

Image steganography involves concealing information within digital images. Various techniques use the least significant bit (LSB) manipulation to embed data into the pixel values without significantly altering the visual representation of the image. This technique is commonly used for secret communication or copyright protection purposes.

***Audio Steganography*:** audio steganography refers to hiding information within audio files without causing perceptible changes to the audio quality. Techniques such as LSB manipulation, phase encoding, and spread spectrum modulation are used to embed data within the audio signal, often imperceptible to human ears. Audio steganography is primarily employed for covert communication or digital rights management purposes.

Video steganography involves concealing information within video files. Similar to image and audio steganography, techniques like LSB manipulation, temporal and spatial transformations, and motion vectors are used to embed data in video frames. Video steganography finds applications in areas such as copyright protection, surveillance, and covert communication. Table 1 provides comprehensive information-hiding techniques with specific features.

2.2 Watermarking

Watermarking is a technique used to embed a digital signature or identifier into multimedia data to prove authenticity, ownership, or copyright protection [11, 19]. The watermarking technique can be divided as subcategories [21]:

Digital watermarking entails embedding a watermark (a sequence of bits or a signature) directly into digital content, such as images, audio, documents, or video files. The watermark is imperceptible or difficult to remove, allowing the identification or authentication of the content and asserting the ownership or integrity of the data.

Multimedia watermarking extends the concept of digital watermarking to multiple types of multimedia data (e.g., images, audio, and video) simultaneously. It aims to embed a watermark across different media types to ensure the integrity and ownership of the entire multimedia content.

Algorithm 2 shows a basic pseudocode scheme for a watermarking algorithm.

Algorithm 2. A pseudocode of basic watermarking scheme

```
function watermarking (coverImage, watermarkImage, alpha):
    watermarkedImage = copy(coverImage)
// Create a copy of the cover image
  for each pixel in watermarkImage:
      coverPixel =
watermarkedImage.getPixelValue(pixel)
    watermarkPixel = watermarkImage.getPixelValue(pixel)
// Apply watermarking algorithm to blend the watermark pixel with the cover pixel
    watermarkedPixel = (1 - alpha) * coverPixel + alpha * watermarkPixel
    watermarkedImage.setPixelValue(pixel, watermarkedPixel)
// Update pixel value in watermarked image
  return watermarkedImage
```

In this pseudocode, 'coverImage' represents the original image, 'watermarkImage' represents the watermark to be embedded, and 'alpha' represents the blending factor that determines the strength of the watermark. The algorithm blends each corresponding pixel value from the watermark image with the cover image based on the specified blending factor. Figure 3 shows the structure of digital watermarking.

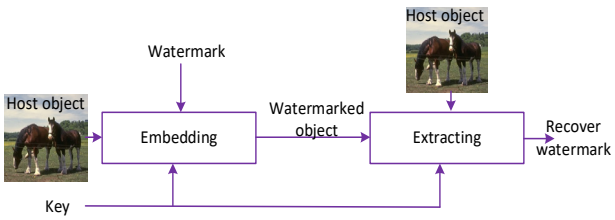

Figure 3. A structure of digital watermarking

Moreover, a comprehensive understanding of the diverse applications and types of watermarking schemes is needed, including detailed explanations of robust watermarking for copyright protection, fragmented watermarking for authentication, and visible watermarking for warning.

Robust watermarking for copyright protection is considered a robust watermarking technique that plays a crucial role in safeguarding digital content by embedding imperceptible watermarks that resist various attacks and manipulations, thus proving content ownership. For instance, spread spectrum embedding and quantization-based approaches are commonly employed to ensure the robustness of watermarks against intentional or unintentional alterations. These methods enable extracting copyright information even after the content has undergone significant modifications, ensuring the protection of intellectual property rights.

Fragile watermarking for authentication uses error-correcting codes and perceptual hashing to ensure content integrity and authenticity. By embedding sensitive watermarks that are easily destroyed by even minor modifications, these techniques enable tamper detection and provide a means to verify the originality of digital content. This makes them particularly valuable in applications where detecting any alterations to the content is critical, such as in legal or forensic contexts.

Visible watermarking for warning is a method that uses visible watermarking techniques, including logos, semi-transparent text overlays, and digital seals, to serve as a deterrent against unauthorized copying or piracy by visibly marking ownership or conveying warnings about restricted usage. These visible watermarks not only indicate ownership but also act as a visual reminder of copyright protection, thereby discouraging unauthorized usage and distribution of digital content. In addition to serving as a warning, visible watermarks contribute to brand recognition and can be an effective tool for promoting the creator's identity and work.

By incorporating these detailed explanations of robust watermarking for copyright protection, fragile watermarking for authentication, and visible watermarking for warning, we can gain a comprehensive understanding of the diverse techniques employed in watermarking schemes for digital content protection.

2.3 Covert Channels

Covert channels involve hiding and transmitting data within existing communication channels without arousing suspicion. Covert channels can be classified as follows:

Network covert channels involve utilizing existing network protocols or exploiting network functionalities to transmit hidden information. Techniques include covert timing channels, covert storage channels, and protocol manipulation to bypass security measures and hide data within network traffic.

Web covert channels operate within the web environment, taking advantage of web technologies and

communication protocols to transmit data surreptitiously. Techniques include hiding information within HTTP headers, embedding data within web page structures or images, or utilizing specific encoding schemes to conceal the data transfer.

Covert channels refer to a method of communication that allows information to be transmitted in a way that is hidden or disguised within a legitimate communication channel. Algorithm 3 displays the pseudocode of basic covert channels scheme.

Algorithm 3. A pseudocode of basic covert channels scheme

```
function covertChannel (transmitChannel, secretMessage):
    for each bit in secretMessage:
        if bit == 0:
transmitChannel.sendData(legitimateData)
 // Send legitimate data through the channel
        else:
transmitChannel.sendData(secretData)
 // Send secret data through the channel
 // Introduce a delay or variation to disguise the transmission pattern
        introduceDelay()
        transmitChannel.close()
// Close the covert channel
```

In this pseudocode, transmitChannel represents the legitimate communication channel through which the covert communication is taking place, and secretMessage represents the message to be transmitted covertly. The algorithm iterates through each bit of the secret message and sends either legitimate data or secret data through the channel based on the value of the bit [22]. Additionally, a delay or variation is introduced to disguise the transmission pattern and make it more difficult to detect [12]. Figure 4 shows an example of covert channels in Internet communication.

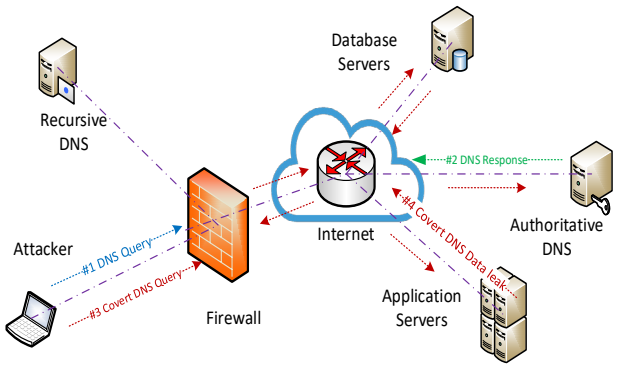

Figure 4. An example of covert channels in internet communication

Investigate cutting-edge techniques for encrypting data in DNS (Domain Name System) queries and responses to provide covert communication channels that evade standard network filtering and monitoring. These techniques are essential for information concealment and protection, guaranteeing the privacy, accuracy, and legitimacy of digital data in a variety of settings, such as communication, copyright protection, and monitoring.

3 Advancements in IHTs on Internet Technology

This section presents advancements in information-hiding techniques in Internet technology features. The Information-hiding related Internet technology and recent advances in IHTs are explored and discussed with security in collaborative scenarios.

3.1 Information-Hiding Related Internet Technology

Internet technology plays a crucial role in information-hiding techniques, offering various channels for transmitting and accessing digital data [9, 23]. Table 2 provides how internet technology features in information hiding techniques. Internet technology provides a powerful platform for implementing and utilizing various information hiding techniques, enabling covert communication, content protection, and secure transmission of hidden data. Table 2 provides the Internet technology features in information hiding techniques. An overview of how Internet technology intersects with information hiding is listed as: steganography in Internet communication, watermarking for online content protection, covert channels in Internet protocol, information hiding in web technologies, and secure transmission and encryption.

Table 2. Internet technology features in information hiding techniques

Aspects	Feature descriptions
Steganography in internet communication [13]	Internet communication channels, such as emails, social media platforms, and file-sharing platforms, can be utilized for transmitting steganographic data. Images, audio files, and videos can carry hidden information, allowing covert communication or copyright protection.
Watermarking for online content protection [24, 46-47]	Internet technologies facilitate the distribution and dissemination of watermarked digital media. Websites, social media platforms, and online stock photography platforms can host images with embedded watermarks, while audio and video files can be streamed or downloaded from online platforms, ensuring ownership and copyright protection.

Aspects	Feature descriptions
Covert channels in internet protocol [12]	Internet protocols offer potential covert channels for hiding information within regular data transmission. By manipulating timing information, unused fields, or employing encryption, sensitive data can be hidden and relayed. Covert channels within internet protocols can be used for covert communication, evading network monitoring or detection systems.
Information hiding in web technologies [23]	Web technologies provide opportunities for information hiding. Data can be embedded within HTML code, scripting languages like JavaScript can manipulate web page content or transmit data, and web APIs can be used for hidden communication. Web-based covert channels can facilitate covert messaging, data exfiltration, or bypassing network firewalls or security measures.
Secure transmission and encryption [25-26]	Internet technology plays a crucial role in secure transmission and encryption. Techniques like SSL/TLS encryption enable secure communication and data transmission, ensuring the confidentiality and integrity of hidden information. Secure transmission protocols prevent unauthorized access to hidden data during its transfer over the internet.

Steganography in Internet Communication: Steganography can be applied to internet-based communication channels, allowing hidden information to be transmitted across the internet without arousing suspicion. For example, images with hidden data can be shared through emails, file-sharing platforms, or social media platforms. Audio steganography techniques can be used to embed confidential messages within VoIP calls, online voice messages, or streaming audio. Similarly, video steganography can enable covert communication through video sharing platforms, video conferences, or streaming services.

Watermarking for Online Content Protection: Watermarking techniques are commonly employed in the online sphere to protect digital content from unauthorized use or copyright infringement. Internet technologies enable the efficient distribution and dissemination of watermarked digital media. For instance, digital images with embedded watermarks can be shared on websites, social media platforms, or online stock photography platforms. Watermarked audio files and videos can be streamed or downloaded from online platforms, ensuring ownership and copyright protection.

Covert Channels in Internet Protocol: Internet protocols offer potential covert channels for hiding information within the regular transmission of data packets. This can involve manipulating timing information, exploiting unused or reserved fields, or employing encryption techniques to hide and relay sensitive information. Covert channels within internet protocols can be used for covert communication, evading network monitoring or detection systems.

Information Hiding in Web Technologies: Web technologies provide a wide range of opportunities for information hiding. This includes embedding data within HTML code, using scripting languages like JavaScript to manipulate web page content or transmit data, and utilizing web APIs for hidden communication. Web-based covert channels can be leveraged for covert messaging, data exfiltration, or bypassing network firewalls or security measures.

Secure Transmission and Encryption: Internet technology also plays a vital role in secure transmission and encryption, which are crucial for maintaining the confidentiality and integrity of hidden information. Techniques like SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption enable secure communication and data transmission, preventing unauthorized access to hidden data during its transfer over the internet.

3.2 Recent Advancements in IHTs

The recent advancements in information hiding techniques offer enhanced capabilities, improved security, and more diverse applications. Researchers and developers continue to explore new methodologies to ensure efficient and secure communication of hidden information. Table 3 shows recent advancements in information-hiding technology.

Some recent IHTs advancements is reviews as follows.

Advanced Steganography Techniques involes Steganography has evolved with more sophisticated methods to hide data within digital media. Advanced algorithms allow for embedding information in various formats like images, audio files, videos, or even 3D models. Techniques like adaptive steganography and deep learning-based steganography have improved the capacity and robustness of hidden data.

Adversarial Attacks and Countermeasures is to refer to Adversarial attacks aim to detect and disrupt information hiding techniques. Researchers are developing countermeasures to defend against such attacks. Adversarial machine learning techniques, like GANs (Generative Adversarial Networks), are used to create robust information hiding methods that can withstand detection or removal attempts.

Mobile Device Information Hiding is to refer to Mobile devices have become a popular platform

for information hiding due to their widespread use and advanced capabilities. Researchers are working on techniques that utilize device sensors and unique characteristics to hide data. For example, leveraging accelerometer data, location information, or device-specific features like battery usage patterns for covert communication.

Text-based Steganography is to refer to Steganography techniques have expanded beyond multimedia to include text-based approaches. Hidden messages can be embedded within text documents, emails, social media posts, or even in code snippets. Natural language processing (NLP) techniques, text encryption, and linguistic manipulations enable secure and imperceptible text-based information hiding.

Artificial Intelligence-enabled Detection is to refer to With the advancements in AI and machine learning, detection techniques for information hiding have also improved. AI algorithms can analyze digital media to identify hidden data with higher accuracy and efficiency. AI-enabled forensic tools are being developed to detect steganographic content, watermark removal, or other sophisticated hiding techniques.

Multi-modal Information Hiding involes Multi-modal techniques involve hiding information across different media types simultaneously. Integrating various forms like images, audio, video, and text enhances the capacity and security of hidden data [27]. Combining different modalities with advanced encryption and synchronization mechanisms provides robust information hiding solutions.

Table 3. Recent advancements in information-hiding technology via internet technology

Advancement	Feature explanation
Machine learning and deep learning approaches [27-28]	Machine learning and deep learning techniques have been used to develop advanced information hiding methods. These approaches leverage the power of artificial intelligence to automatically learn and extract hidden patterns or features in data. For example, deep neural networks can be trained to embed secret messages within images or audio files. This enables more robust and efficient information hiding capabilities, as the models can adapt and optimize the hiding process based on the input data.
Blockchain-based information hiding [29-30]	Blockchain technology has been explored for secure and distributed information hiding. By leveraging the immutable nature and decentralized characteristics of blockchain, it is possible to securely store and transmit hidden information. For example, blockchain-based hidden messaging systems can be created where messages are recorded on the blockchain and can only be accessed by the intended recipient. This ensures confidentiality and tamper-proof communication.
IoT and information hiding [15, 31-32]	The Internet of Things (IoT) has introduced new opportunities for information hiding. IoT devices can be used to transmit hidden information through various means, such as modulating data signals, embedding messages in sensor readings, or using covert communication channels. For instance, IoT devices can be utilized to exchange sensitive data covertly, such as in smart home environments, industrial control systems, or healthcare monitoring systems.
Cloud computing and information hiding [33]	Cloud computing platforms can be leveraged for information hiding, allowing users to store, process, and transmit hidden information efficiently. Cloud-based information hiding techniques can include distributed data storage, encryption, and decentralized communication. For example, users can utilize cloud storage services to store encrypted files or leverage cloud-based encryption services for secure transmission of hidden data.

4 Challenges and Future Directions

This section presents the challenges and future directions in information hiding related Internet technology features that achieved recent advances in IHTs with collaborative security scenarios.

4.1 Challenges and Trends in IHTs

Security and Detection Challenges:

- Adversarial Attacks: Adversaries constantly develop new techniques to bypass information hiding mechanisms. This leads to a cat-and-mouse game between information hiders and detectors. Developing robust hiding techniques that can withstand sophisticated attacks is a major challenge [34].
- Steganalysis: Steganalysis is the process of detecting hidden information. As hiding techniques become more advanced, the development of effective and efficient steganalysis methods is

crucial. Finding reliable indicators and algorithms for detecting hidden data presents an ongoing challenge.

- Real-time Detection: Real-time detection of hidden information is essential in applications like multimedia content sharing platforms or network traffic monitoring. Developing real-time detection algorithms that can quickly identify hidden content without introducing significant delays is a challenge [27].

Privacy Concerns: The advice regarding effective, safe, and private information-hiding methods.

- Ethical Use: Information hiding techniques raise concerns about the ethical use of hidden information [35]. It is crucial to establish ethical guidelines for the application of these techniques to prevent misuse or violation of individual privacy rights.
- Informed Consent: The use of information hiding without the knowledge or consent of individuals involved raises ethical and legal concerns [36]. Addressing the issue of informed consent in information hiding applications is essential to ensure privacy protection.

Table 4 shows addressing ways for secure, efficient, and privacy-preserving information-hiding techniques.

Emerging Trends and Technologies:

- Quantum Information Hiding: With the emergence of quantum technologies, there is a growing interest in quantum information hiding techniques. Quantum information hiding can leverage the unique properties of quantum systems, such as entanglement and superposition, to create more secure and efficient hiding methods [34].
- Homomorphic Encryption: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. Applying homomorphic encryption to information hiding can offer enhanced security and privacy, as the hidden data remains encrypted throughout the processing [12].
- Edge Computing: Information hiding techniques can benefit from edge computing, where data processing occurs closer to the source or on edge devices. Leveraging edge computing capabilities can enhance the efficiency and speed of information hiding, especially in real-time applications [39].
- Neural Network-based Hiding: Neural networks, particularly generative models like GANs, have shown potential in creating more advanced and secure information hiding techniques [40].

Future developments may explore the use of neural networks for generating hiding patterns, optimizing hiding capacity, or creating more robust hiding mechanisms [41].

Table 4. Addressing ways for secure, efficient, and privacy-preserving information-hiding techniques

Challenges	Exploring trends	Description
Security and detection challenges [35, 37]	- Adversarial Attacks	Developing robust hiding techniques that can withstand sophisticated attacks.
	- Steganalysis	Developing effective and efficient methods for detecting hidden information.
	- Real-time Detection	Developing algorithms for quick identification of hidden content without significant delays.
Privacy concerns [27, 36]	- Ethical Use	Establishing ethical guidelines to prevent misuse or violation of individual privacy rights.
	- Informed Consent	Addressing the issue of informed consent in information hiding applications.
Emerging trends and technologies [18, 38]	- Quantum Information Hiding	Exploring the use of quantum technologies for more secure and efficient hiding methods.
	- Homomorphic Encryption	Applying homomorphic encryption to enhance security and privacy in information hiding.
	- Edge Computing	Leveraging edge computing capabilities for efficient and real-time information hiding.
	- Neural Network-based Hiding	Utilizing neural networks, particularly generative models, for advanced and robust hiding techniques.

Table 5. Comparison of advantages and disadvantages of the challenges in information hiding lies in addressing security and detection concerns

Technique name	Advantages/Disadvantages	Suggested directions for future research
Steganography [13, 17]	Advantages: High capacity, imperceptibility of hidden data, resistance to detection. Disadvantages: Vulnerability to statistical attacks.	Investigate robustness against advanced steganalysis techniques, explore novel hiding methods for improved security and capacity.
Watermarking [14, 18, 38]	Advantages: Robustness against attacks, ability to prove ownership. Disadvantages: Limited capacity, perceptibility of watermark.	Develop techniques for increasing capacity while maintaining imperceptibility, investigate robustness against more advanced attacks.
Covert channels [20, 42]	Advantages: Can bypass network security measures, difficult to detect. Disadvantages: Limited bandwidth, potential legal and ethical concerns.	Explore techniques for increasing bandwidth, investigate methods for detecting and preventing covert channel communication.
Data encryption [23, 36]	Advantages: Provides strong security, widely used and standardized. Disadvantages: Encryption overhead, vulnerability to key management issues.	Develop efficient encryption algorithms, explore techniques for secure key management and distribution.
Spread spectrum [27, 43]	Advantages: Robustness against noise and interference, resistance to detection. Disadvantages: Limited capacity, potential impact on communication quality.	Investigate methods for increasing capacity without compromising communication quality, explore hybrid approaches with other hiding techniques.
Visual cryptography [44-45]	Advantages: No computational overhead, easy to implement, secure against attacks. Disadvantages: Limited hiding capacity, requires multiple shares.	Develop techniques for increasing hiding capacity, investigate methods for improving the efficiency and usability of visual cryptography.
Linguistic steganography [26-27]	Advantages: Natural and inconspicuous hiding method, resistant to statistical analysis. Disadvantages: Limited capacity, potential language constraints.	Explore techniques for increasing capacity, investigate methods for hiding in different languages and text formats.

4.2 Exploring Emerging Trends in IHTs

The challenges in information hiding lie in addressing security and detection concerns, ensuring ethical use and informed consent, and keeping up with emerging trends and technologies [46]. Adversarial attacks and effective steganalysis methods require continuous research and development [23]. Privacy concerns necessitate the establishment of ethical guidelines and consent protocols. Emerging trends like quantum information hiding, homomorphic encryption, edge computing, and neural network-based hiding offer new possibilities for enhanced security and efficiency [47]. Table 5 compares the benefits and drawbacks of the difficulties in dealing with security and detection issues when hiding information.

As technology continues to evolve, IHTs will also be developing. Researchers and developers will strive to create more robust, secure, and efficient hiding mechanisms to meet the demands of an increasingly interconnected and data-driven world [40]. By addressing challenges and embracing emerging trends, the future of information hiding looks promising, with applications spanning from digital forensics and security to multimedia content protection and privacy preservation

5 Conclusion

This paper provided a comprehensive overview of recent advancements in information-hiding techniques for digital systems using internet technology. We have examined the applicability of digital objects, network protocols, and web applications by categorizing and analyzing various methodologies, algorithms, and tools. Evaluating existing information-hiding techniques has highlighted their strengths and limitations, particularly regarding security, detectability, and resilience against attacks. The analysis has highlighted the need for continuous research and development to address these techniques' challenges and obstacles in internet-based digital systems. Furthermore, this paper has suggested

potential future directions for research and development in the field of information hiding. By considering emerging trends and technologies, such as quantum information hiding, homomorphic encryption, edge computing, and neural network-based concealment, researchers can explore new avenues for enhancing information-hiding techniques' security, efficiency, and privacy-preserving capabilities. The review served as a valuable resource for researchers, practitioners, and stakeholders in information hiding. It provided an understanding of the current state of the art and highlights the importance of addressing challenges and embracing emerging trends to advance the field further. Focusing on these directions can pave the way for more secure, efficient, and privacy-preserving information hiding techniques in the future.

References

[1] S. Vaidya, P. Ambad, S. Bhosle, Industry 4.0–a glimpse, *Procedia manufacturing*, Vol. 20, pp. 233–238, 2018.

[2] J.-S. Pan, X.-X. Sun, H. Yang, V. Snášel, S.-C. Chu, Information hiding based on two-level mechanism and look-up table approach, *Symmetry*, Vol. 14, No. 2, Article No. 315, February, 2022.

[3] D. Kannan, M. Gobi, An extensive research on robust digital image watermarking techniques: A review, *International Journal of Signal and Imaging Systems Engineering*, Vol. 8, No. 1–2, pp. 89–104, January, 2015.

[4] C.-J. Weng, S.-J. Liu, J.-S. Pan, L. Liao, T.-T. Nguyen, W.-D. Zeng, P. Zhang, L. Huang, Enhanced Secret Hiding Mechanism Based on Genetic Algorithm, *Proceedings of the 15th International Conference on IIH-MSP in conjunction with the 12th International Conference on FITAT, Advances in Intelligent Information Hiding and Multimedia Signal Processing*, Jilin, China, 2020, pp. 79–86.

[5] P. Moulin, J. A. O'Sullivan, Information-theoretic analysis of information hiding, *IEEE Transactions on information theory*, Vol. 49, No. 3, pp. 563–593, March, 2003.

[6] T. F. Chan and J. Shen, *Image processing and analysis: variational, PDE, wavelet, and stochastic methods*, SIAM, 2005.

[7] H. Sajedi, S. R. Yaghobi, Information hiding methods for E-Healthcare, *Smart health*, Vol. 15, Article No. 100104, March, 2020.

[8] S. M. Thampi, Information hiding techniques: a tutorial review, *arXiv preprint arXiv:0802.3746*, February, 2008. https://arxiv.org/abs/0802.3746

[9] B. Bayar, M. C. Stamm, Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 11, pp. 2691–2706, November, 2018.

[10] T.-T. Nguyen, T.-K. Dao, H.-Y. Kao, M.-F. Horng, C.-S. Shieh, Hybrid Particle Swarm Optimization with Artificial Bee Colony optimization for topology control scheme in wireless sensor networks, *Journal of Internet Technology*, Vol. 18, No. 4, pp. 743-752, July, 2017.

[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, Elsevier Inc., 2008.

[12] L. Robert, T. Shanmugapriya, A study on digital watermarking techniques, *International journal of Recent trends in Engineering*, Vol. 1, No. 2, p. 223-225, May, 2009.

[13] J. Fridrich, M. Goljan, R. Du, Reliable detection of LSB steganography in color and grayscale images, *Proceedings of the 2001 workshop on Multimedia and security: new challenges*, Ottawa, Ontario, Canada, 2001, pp. 27–30.

[14] J. Seitz, *Digital watermarking for digital media*, IGI Global, 2005.

[15] S. Katzenbeisser, F. Petitcolas, *Information hiding*, Artech house, 2016.

[16] M. T. Ahvanooey, Q. Li, H. J. Shim, Y. Huang, A comparative analysis of information hiding techniques for copyright protection of text documents, *Security and Communication Networks*, Vol. 2018, Article No. 5325040, April, 2018.

[17] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal processing*, Vol. 90, No. 3, pp. 727–752, March, 2010.

[18] J.-S. Pan, H.-C. Huang, L. C. Jain, *Information hiding and applications*, Vol. 227. Springer Science & Business Media, 2009.

[19] C. Honsinger, Book Reviews: Digital watermarking, *Journal of Electronic Imaging*, Vol. 11, No. 3, Article No. 1494075, July, 2002.

[20] S. Zander, G. Armitage, P. Branch, A survey of covert channels and countermeasures in computer network protocols, *IEEE Communications Surveys & Tutorials*, Vol. 9, No. 3, pp. 44–57, Third Quarter, 2007.

[21] M. Begum, M. S. Uddin, Digital image watermarking techniques: a review, *Information*, Vol. 11, No. 2, Article No. 110, February, 2020.

[22] C. F. Tsai, T. K. Dao, T. S. Pan, T. T. Nguyen, J. F. Chang, Parallel bat algorithm applied to the economic load dispatch problem, *Journal of Internet Technology*, Vol. 17, No. 4, pp. 761–769, July, 2016.

[23] M. T. Ahvanooey, M. X. Zhu, W. Mazurczyk, M. Bendechache, Information hiding in digital textual contents: Techniques and current challenges, *Computer*, Vol. 55, No. 6, pp. 56–65, June, 2022.

[24] J. Nin, S. Ricciardi, Digital watermarking techniques and security issues in the information and communication society, *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, Barcelona, Spain, 2013, pp. 1553–1558.

[25] S. Weng, W. Tan, B. Ou, J.-S. Pan, Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm, *Information Sciences*, Vol. 549, pp. 13–33, March, 2021.

[26] R. J. Santos, J. Bernardino, M. Vieira, A data masking technique for data warehouses, *Proceedings of the 15th Symposium on International Database Engineering & Applications*, Lisboa, Portugal, 2011, pp. 61–69.

[27] S. Miller, D. Childers, *Probability and random processes: With applications to signal processing and communications*, Academic Press, 2012.

[28] P. Khan, M. F. Kader, S. M. R. Islam, A. B. Rahman, M. S. Kamal, M. U. Toha, K.-S. Kwak, Machine learning and deep learning approaches for brain disease diagnosis: principles and recent advances, *IEEE Access*, Vol. 9, pp. 37622–37655, February, 2021.

[29] M. H. Abidi, H. Alkhalefah, U. Umer, M. K. Mohammed, Blockchain-based secure information sharing for supply

chain management: optimization assisted data sanitization process, *International journal of intelligent systems*, Vol. 36, No. 1, pp. 260–290, January, 2021.

[30] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, J. H. Park, Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems, *Sensors*, Vol. 22, No. 4, Article No. 1371, February, 2022.

[31] K. Koptyra, M. R. Ogiela, Steganography in IoT: information hiding with APDS-9960 proximity and gestures sensor, *Sensors*, Vol. 22, No. 7, Article No. 2612, April, 2022.

[32] K. Koptyra, M. R. Ogiela, Steganography in IoT: Information Hiding with Joystick and Touch Sensors, *Sensors*, Vol. 23, No. 6, Article No. 3288, March, 2023.

[33] Y. Fan, Y. Liao, F. Li, S. Zhou, G. Zhang, Identity-based auditing for shared cloud data with efficient and secure sensitive information hiding, *IEEE Access*, Vol. 7, pp. 114246–114260, August, 2019.

[34] B. A. Shaw, T. A. Brun, Hiding quantum information in the perfect code, *arXiv preprint arXiv:1007.0793*, March, 2010. https://arxiv.org/abs/1007.0793

[35] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, W.-C. Hong, Internet of things: Evolution, concerns and security challenges, *Sensors*, Vol. 21, No. 5, Article No. 1809, March, 2021.

[36] I. You, K. Yim, Malware obfuscation techniques: A brief survey, *2010 International conference on broadband, wireless computing, communication and applications*, Fukuoka, Japan, 2010, pp. 297–300.

[37] C.-M. Pun, C. Yan, X.-C. Yuan, Image alignment-based multi-region matching for object-level tampering detection, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 2, pp. 377–391, February, 2017.

[38] C. Fontaine, F. Galand, A survey of homomorphic encryption for nonspecialists, *EURASIP Journal on Information Security*, Vol. 2007, pp. 1–10, December, 2007.

[39] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. S. Ho, S. Khan, S. N. B. Musa, A. Z. B. Taha, Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities, *IEEE Access*, Vol. 8, pp. 76541–76567, April, 2020.

[40] M. Chanchal, P. Malathi, G. Kumar, A comprehensive survey on neural network based image data hiding scheme, *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, Palladam, India, 2020, pp. 1245–1249.

[41] T.-T. Nguyen, T.-K. Dao, T.-D. Nguyen, V.-T. Nguyen, An Improved Honey Badger Algorithm for Coverage Optimization in Wireless Sensor Network, *Journal of Internet Technology*, Vol. 24, No. 2, pp. 363–377, March, 2023.

[42] N. B. Lucena, G. Lewandowski, S. J. Chapin, Covert channels in IPv6, *Privacy Enhancing Technologies: 5th International Workshop, PET 2005*, Cavtat, Croatia, pp. 147–166.

[43] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, K. Murali, Chaos based spread spectrum image steganography, *IEEE transactions on consumer Electronics*, Vol. 50, No. 2, pp. 587–590, May, 2004.

[44] D. R. Ibrahim, J. S. Teh, R. Abdullah, An overview of visual cryptography techniques, *Multimedia Tools and Applications*, Vol. 80, No. 21-23, pp. 31927–31952, September, 2021.

[45] Y.-C. Hou, Visual cryptography for color images, *Pattern recognition*, Vol. 36, No. 7, pp. 1619–1629, July, 2003.

[46] J.-S. Pan, H. Luo, Z.-M. Lu, Visible watermarking for halftone images, *IEICE transactions on fundamentals of electronics, communications and computer sciences*, Vol. E90-A, No. 7, pp. 1487-1490, July, 2007.

[47] H. Luo, J.-S. Pan, Z. M. Lu, Content adaptive visible watermarking during ordered dithering, *IEICE transactions on information and systems*, Vol. E90-D, No. 7, pp. 1113-1116, July, 2007.

Biographies

Trong-The Nguyen received his Ph.D. degree in Communication Engineering from the National Kaohsiung University of Applied Sciences, Taiwan, in 2016. He is currently an Associate Professor at the School of Electronic Engineering, Fuzhou Institute of Technology, China, and a researcher with MMLab, University of Information Technology, Vietnam. His research interests include computational intelligence, wireless sensor networks, cryptography and security, signal processing, and information hiding.

Truong-Giang Ngo obtained a Ph.D. in mathematical theory for informatics from the Graduate University of Science and Technology, Vietnam Academy of Science and Technology, Vietnam, in 2017. He currently serves as a lecturer at the Faculty of Computer Science and Engineering at Thuyloi University, Vietnam. His research interests include machine learning, data mining, networking, and wireless sensor networks.

Shu-Chuan Chu received the Ph.D. degree in evolutionary algorithms and artificial intelligence from the School of Computer Science, Engineering and Mathematics, Flinders University, Adelaide, SA, Australia, in 2004. In December 2009, she joined Flinders University, after nine years with Cheng Shiu University, Kaohsiung, Taiwan. She has been a Research Fellow with the College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, China, since 2019. Her research interests include swarm intelligence, intelligent computing, and data mining.

Thi-Kien Dao received her Ph.D. degree in Electronics Engineering from the National Kaohsiung University of Science and Technology, Taiwan, in 2019. She is currently an Associate Professor at the School of Electronic Engineering, Fuzhou Institute of Technology, China, and a researcher with MMLab, University of Information Technology, Vietnam. Her research interests include computational intelligence, data mining, wireless sensor networks, and cryptography and security.

Thi-Thanh-Tan Nguyen received her Ph.D. degree in computer science from Hanoi University of Vietnam, in 2012, respectively. She is currently the Head of the Department of Computer Science and Information Systems, Electric Power University, Vietnam. Her current research interests include content-based image retrieval, intelligent image processing, and multimedia systems, computational intelligence, and grid computing.