Journal of Information Hiding and Multimedia Signal Processing ©2024 ISSN 2073-4212
Ubiquitous International Volume **15**, Number **1**, March **2024**

Recent Information Hiding Techniques in Digital Systems: A Review

Thi-Kien Dao[1,2], Trong-The Nguyen[1,2,*]

[3]Multimedia Communications Lab.,
VNU-HCM, University of Information Technology, Vietnam
[4]Vietnam National University, Ho Chi Minh City 700000, Vietnam
{thent, kiendt}@uit.edu.vn

Thi-Xuan-Huong Nguyen[3,4], Trinh-Dong Nguyen[3,4]

[3]Software Engineering Department,
University of Information Technology, Vietnam
[4]Vietnam National University, Ho Chi Minh City 700000, Vietnam
{huongntx, dongnt}@uit.edu.vn

Corresponding author: Trong-The Nguyen

Received October 14, 2023, revised January 15, 2024, accepted February 27, 2024.

Abstract. *The ease of exchanging data through communication channels made possible by the industrial and informational revolutions has both advantages and disadvantages. The drawbacks of using information-hiding techniques as a security strategy must be taken into account. This paper provides a comprehensive review of information hiding techniques in digital systems. The paper aims to explore and analyze various methods used to conceal sensitive data within digital assets, such as images, audio files, videos, and documents. It discusses the importance of information hiding techniques in different industries and applications, along with their advantages, challenges, and potential ethical considerations. The findings of this review aim to enhance the understanding of information hiding techniques and their relevance in today's digital landscape.*

Keywords: Information Hiding Technique; digital assets; Digital Systems; industrial and informational revolutions.

1. **Introduction.**

The rapid advancements in digital technology have brought about a significant increase in the volume and importance of sensitive data being transmitted and stored [1][2]. With the growing concerns of unauthorized access, data breaches, and privacy violations, the need for effective information hiding techniques [3] has become paramount [4]. Information hiding techniques refer to the methods used to conceal sensitive data within digital assets, making it difficult for unauthorized individuals to access or detect the hidden information [5].

This research paper provides a comprehensive review of information hiding techniques (IHT) in digital systems [6]. It explores various methods such as steganography, watermarking, encryption, obfuscation, data masking, and covert channels [7]. Each technique has its unique characteristics and applications, and understanding their strengths and limitations is crucial for implementing effective data protection strategies. Figure 1 illustrates a process of digital image steganography procedures. The technique uses to hide secret information within a digital image without arousing suspicion; that involves two main procedures: embedding and extraction [8].

The embedding procedure is the process of hiding secret information within the digital image that uses the least significant bits (LSBs) [9]. The secret information, which can be in the form of text, images, or any other data, is encoded and then embedded in the image. The goal is to make the modifications imperceptible to the human eye so that the image appears unchanged to an observer. There are various techniques used for embedding secret information. One common approach is the LSB substitution method, where the LSBs of the image pixels are replaced with the secret data bits [10]. Another technique is the spread spectrum method, which spreads the secret data across multiple pixels in a way that is difficult to detect. Other advanced methods include transform domain techniques, such as discrete cosine transform (DCT) or discrete wavelet transform (DWT), which exploit the frequency domain properties of the image to embed the secret information. Once the secret information is embedded, the extraction procedure is used to retrieve the hidden data from the stego-image, which is done by reversing the embedding process [11]. The stego-image is analyzed, and the modifications made during embedding are detected and reversed to obtain the original secret information. The extraction process requires knowledge of the embedding algorithm and any encryption or compression techniques used during embedding [12].

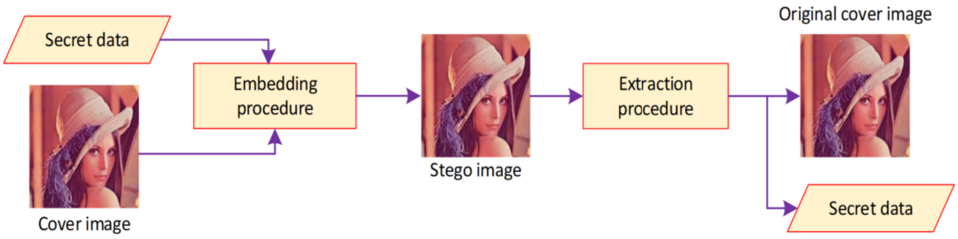

Figure 1. A process of digital image steganography procedures.

The paper discusses the applications and industries where these techniques are crucial, including banking and finance, healthcare, media and entertainment, government and defense, and e-commerce. It highlights the advantages of information hiding techniques, such as protecting sensitive data and enhancing privacy and confidentiality [13]. However, the paper also acknowledges the challenges and limitations associated with these techniques, such as capacity constraints and vulnerabilities to advanced attacks. Ethical considerations and potential misuse are also discussed [14]. The importance of staying updated with the latest techniques is emphasized, as the field of cybersecurity is constantly evolving [15]. Overall, this research paper aims to enhance understanding and promote further research and innovation in information hiding techniques [16]. The paper also delves into the applications and industries where information hiding techniques play a vital role. Industries such as banking and finance, healthcare, media and entertainment, government and defense, and e-commerce heavily rely on these techniques to safeguard sensitive information [17], protect intellectual property, and ensure compliance with privacy regulations [18].

Advantages of information hiding techniques include the protection of sensitive data, enhanced privacy and confidentiality, detection and deterrence of data breaches, and improved data integrity and authenticity [19]. However, implementing these techniques also comes with challenges and limitations, such as capacity constraints, vulnerabilities to advanced attacks, and the need to balance security with usability [20].

Ethical considerations and potential misuse of information hiding techniques are also discussed in this review. While these techniques are primarily intended for legitimate purposes, there is a potential for misuse in illegal activities, invasion of privacy concerns, and ethical implications related to covert surveillance and espionage [21]. It is crucial for individuals and organizations to be aware of these ethical considerations and ensure responsible use of information hiding techniques [22]. Staying updated with the latest information hiding techniques is of utmost importance in today's digital landscape. The field of cybersecurity is constantly evolving, and new threats and vulnerabilities emerge regularly. By staying informed and adapting to new challenges, individuals and organizations can better protect their sensitive data and mitigate risks [23].

This review research paper provides a comprehensive overview of information hiding techniques in digital systems. By exploring various techniques, applications, advantages, challenges, and ethical considerations, it aims to enhance the understanding of these techniques and their relevance in today's digital age. The findings of this review contribute to the existing knowledge base and emphasize the importance of continuous research and innovation in information hiding techniques.

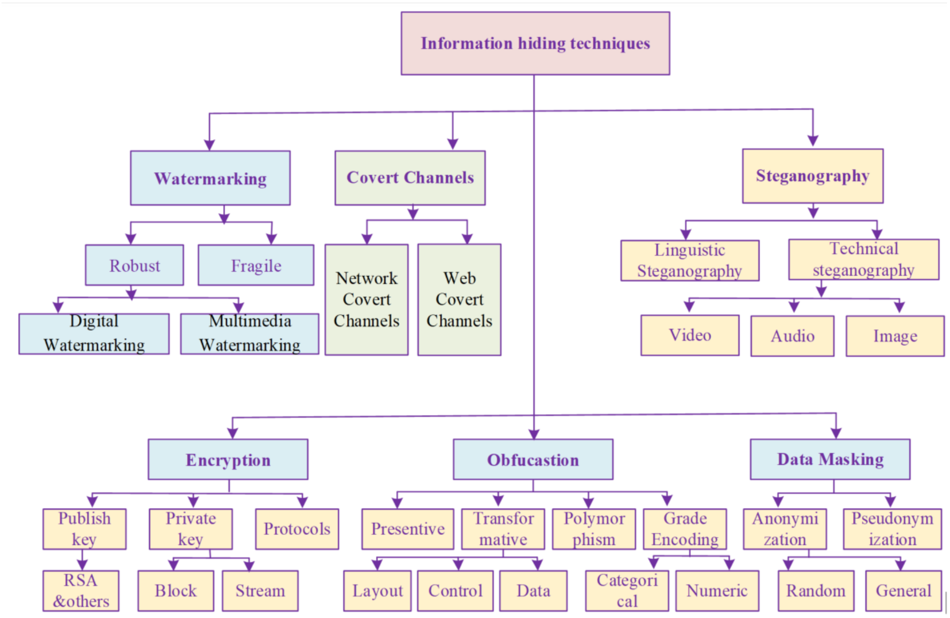

FIGURE 2. Several selected types of information hiding techniques.

2. **Types of Information Hiding Techniques.** Information hiding techniques play a crucial role in ensuring the security and integrity of sensitive data. These techniques offer a way to conceal information within various mediums, making it difficult for unauthorized individuals to detect or access the hidden data [24].

However, there are several challenges and limitations that organizations must consider when implementing information hiding techniques. Balancing robustness against detection with security, compatibility and interoperability issues, legal and ethical considerations, human factor vulnerabilities, and limitations of steganography are some of the challenges that organizations may face . It is essential to understand and address these challenges to effectively implement and utilize information hiding techniques. Figure 2 shows a taxonomy of selected types of information-hiding techniques.

Additionally, ethical considerations and the potential misuse of these techniques must be carefully evaluated. Privacy protection, intellectual property rights, misrepresentation and deception, law enforcement and national security, and ethical responsibility are important factors to consider [25]. Organizations must ensure that information hiding

Table 1. Types of Information Hiding Techniques

Technique	**Description**
Steganography [27]	Hides information within other digital media, such as images, audio files, or videos, in an imperceptible manner.
Watermarking [4][28]	Embeds a unique identifier or signature into digital media for purposes such as copyright protection, content authentication, and tamper detection.
Encryption [4][29]	Converts data into an unreadable format using cryptographic algorithms, ensuring that only authorized individuals can access the data.
Obfuscation [30]	Modifies the source code or structure of a program to make it difficult to understand or reverse engineer, protecting intellectual property.
Data Masking [24][31]	Replaces sensitive data with realistic, but fictional, data to maintain privacy and compliance during testing, development, or analysis.
Covert Channels [32]	Hidden communication channels within legitimate channels, used for secure communication or malicious activities like data exfiltration.

techniques are used responsibly, within legal boundaries, and in compliance with privacy laws and regulations [26]. By understanding these challenges, limitations, and ethical considerations, organizations can make informed decisions about implementing information hiding techniques and ensure that they are used in a responsible, transparent, and ethical manner. Proper guidelines, policies, and oversight mechanisms should be established to promote ethical use and mitigate potential risks.

Table 1 lists types of information hiding techniques includes Steganography [27], Watermarking [28], Encryption [29], Obfuscation, and Obfuscation [30], Data Masking [31], and Covert Channels [32] teachniques. Steganography is a concealing information within digital media without arousing suspicion. Watermarking is a embedding a unique identifier into digital assets for copyright protection or authentication purposes. Encryption is form of transforming data into a coded form to prevent unauthorized access. Obfuscation is kind of modifying code or data to make it difficult to understand or reverse engineer [33]. Data masking is a replacing sensitive data with fictitious or masked values. Covert Channels is a way of establishing hidden communication channels within a system.

Steganography: Steganography is the art of hiding information within other digital media, such as images, audio files, or videos [27]. This technique involves embedding the hidden data in a way that is imperceptible to human senses. Steganography can be used to conceal sensitive information, such as passwords or confidential documents, within seemingly innocuous files. Figure 3 displays a flowchart of the stegosystem coding procedures.

Watermarking: Watermarking is a technique used to embed a unique identifier or signature into digital media, such as images or videos [28]. These watermarks can be visible or invisible and serve various purposes, including copyright protection, content authentication, and tamper detection. Watermarking helps to establish the ownership and integrity of digital assets. Encryption: Encryption is a widely used technique for securing data by converting it into an unreadable format using cryptographic algorithms

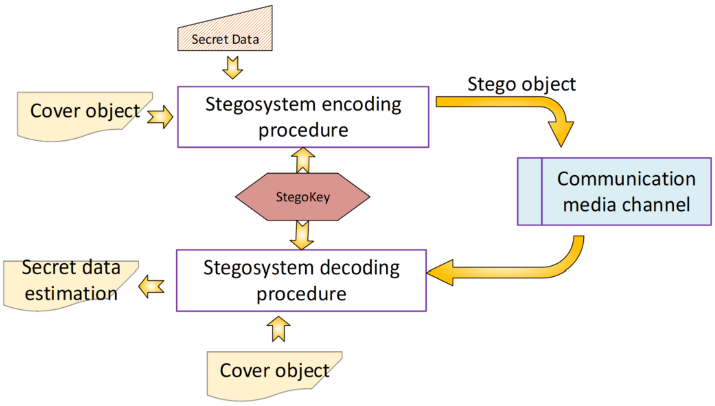
Secret Data
Cover object
Stegosystem encoding procedure
Stego object
StegoKey
Communication media channel
Secret data estimation
Stegosystem decoding procedure
Cover object

FIGURE 3. A flowchart of the stegosystem coding procedures.

[29]. The encrypted data can only be accessed with the correct decryption key. Encryption is commonly used to protect sensitive information during transmission or storage, ensuring that only authorized individuals can access the data.

Obfuscation: Obfuscation involves modifying the source code or structure of a program to make it difficult to understand or reverse engineer. This technique is commonly used in software development to protect intellectual property and prevent unauthorized access to proprietary algorithms or sensitive information. Data Masking: Data masking is a technique used to protect sensitive data by replacing it with realistic, but fictional, data. This allows organizations to use real data for testing, development, or analysis purposes while ensuring that sensitive information is not exposed [31]. Data masking helps to maintain data privacy and compliance with regulations.

Covert Channels: Covert channels refer to the communication channels that are hidden within legitimate communication channels [32]. These channels are used to transmit information without detection or suspicion. Covert channels can be used for both legitimate purposes, such as secure communication in military or intelligence operations, and for malicious activities, such as data exfiltration.

3. **Applications of IHTs and Involved Industries.** This section presents the information hiding techniques used in applications and industries, e.g., Banking and finance [34]: Securing financial transactions and protecting customer data; Healthcare [35]: Ensuring privacy and confidentiality of patient records; Media and entertainment [20]: Preventing piracy and unauthorized distribution of content; Government and defense: Safeguarding classified information and communication channels; and E-commerce: Protecting customer information during online transactions. These applications and industries highlight the diverse range of sectors where information hiding techniques are applied to enhance data security, protect sensitive information, and ensure compliance with privacy regulations. Each industry has its own specific requirements and use cases for information hiding techniques, and implementing these techniques effectively contributes to the overall security and integrity of digital assets [36]. Table 2 illustrates a wide range of applications and industries of information-hiding techniques. Information hiding techniques have a wide range of applications and play a crucial role in various industries. Some of the common applications and industries where these techniques are utilized include:

Banking and Finance: In the banking and finance sector, information hiding techniques are used to secure sensitive financial data, such as customer records, transaction details, and account information [34]. Encryption and data masking are commonly employed

Table 2. A wide range of applications and industries of information-hiding techniques.

Application	**Involved Industries**
Banking and Finance [34]	Banking, Financial institutions.
Healthcare [35]	Hospitals, Clinics, Healthcare providers.
Media and Entertainment [24] [20]	Media companies, Entertainment industry.
Government and Defense [37]	Government agencies, Defense organizations .
E-commerce [39]	Online retailers, Payment processors.
Intellectual Property [40]	Software development, Digital content. creation, Engineering
Cybersecurity [13]	Information security companies, IT. departments

to protect financial data during transmission and storage, ensuring confidentiality and integrity.

Healthcare: Information hiding techniques are vital in the healthcare industry to safeguard patient data, ensure privacy compliance, and protect medical records [35]. Encryption and data masking techniques help prevent unauthorized access to sensitive patient information, while watermarking can be used to track and authenticate medical imaging data.

Media and Entertainment: The media and entertainment industry uses information hiding techniques for copyright protection and content authentication [20]. Watermarking is often applied to digital media files to establish ownership, detect unauthorized use, and prevent piracy.

Government and Defense: Information hiding techniques are heavily utilized in government and defense sectors to protect classified information, secure communication channels, and prevent data leaks [37]. Steganography and covert channels are used for secure and covert communication, while encryption is employed to protect sensitive government and defense data.

E-commerce: In the e-commerce industry, information hiding techniques are utilized to secure transactions, protect customer data, and prevent fraud. Encryption ensures that online transactions are encrypted, safeguarding sensitive financial information such as credit card details.

Intellectual Property Protection: Information hiding techniques help protect intellectual property in industries such as software development, digital content creation, and engineering [38]. Techniques like obfuscation are employed to make it difficult for unauthorized individuals to understand or reverse engineer proprietary algorithms or designs.

Cybersecurity: Information hiding techniques are essential in cybersecurity to protect sensitive information from cyber threats. Encryption is widely used for secure data transmission, while steganography can be employed to conceal the presence of malicious code or data within digital files.

These applications illustrate the wide-ranging significance and impact of information hiding techniques across various industries. Implementing these techniques in the right context helps ensure data security, confidentiality, and integrity in today's digital age.

4. **Advantages and Disadvantages of IHTs.** This section presents some advantages and disadvantages of information-hiding techniques. Several advantages are the protection of sensitive data from unauthorized access, enhanced privacy and confidentiality, detection and deterrence of data breaches, and improved data integrity and authenticity

Table 3. Several advantages of information-hiding techniques.

Advantage	**Feature Description**
Confidentiality[4] [5]	Ensures sensitive information remains confidential and accessible only to authorized individuals.
Integrity [19] [24]	Hospitals, Clinics, Healthcare providers.
Unauthorized Access Prevention[4] [24]	Maintains data integrity by preventing unauthorized modifications or tampering.
Compliance and Privacy [44]	Protects against unauthorized access to sensitive information.
Intellectual Property Protection [4][40]	Safeguards intellectual property from theft or misuse
Detection of Unauthorized Usage[4]	Identifies and detects unauthorized usage or distribution of digital assets.
Secure Communication [13]	Provides a means for secure and covert communication in sensitive environments.

[41]. In contrast, several disadvantages are the capacity limitations in steganography and watermarking techniques, vulnerabilities to advanced attacks and detection algorithms, balancing security and usability in encryption methods, and legal and ethical considerations in certain applications [42].

4.1. **Advantages of Information Hiding Techniques.** These advantages highlight the benefits of utilizing information hiding techniques in various industries to enhance data security, protect sensitive information, and ensure compliance with privacy regulations [43]. By implementing these techniques effectively, organizations can mitigate risks associated with unauthorized access, data breaches, and intellectual property theft. Table 3 lists several advantages of Information Hiding Techniques.

4.2. **Challenges and Limitations of IHTs.** Several disadvantages are the capacity limitations in steganography and watermarking techniques, vulnerabilities to advanced attacks and detection algorithms, balancing security and usability in encryption methods, and legal and ethical considerations in certain applications. Table 4 shows several Challenges and Limitations of information-hiding techniques.

5. **Ethical Considerations and Potential Misuse.** Ethical considerations and potential misuse of IHT are possible to be such as, Misuse of information hiding techniques for illegal activities, Invasion of privacy concerns, Ethical implications of covert surveillance and espionage [18]. Privacy Protection: Information hiding techniques can be used to protect individuals' privacy and sensitive data [47]. However, there is a potential for misuse, such as invading privacy or conducting illegal surveillance [41]. Organizations must ensure that these techniques are used responsibly and in compliance with privacy laws and regulations.

Intellectual Property Rights: Information hiding techniques can help protect intellectual property rights by hiding proprietary information [38]. However, there is a risk of misuse, such as unauthorized distribution or infringement of others' intellectual property [34]. Organizations should ensure that these techniques are used within legal boundaries and respect the rights of others.

Misrepresentation and Deception: Information hiding techniques, particularly in the context of steganography, can be used for deceptive purposes, such as spreading misinformation or conducting covert activities. Organizations must consider the ethical

Table 4. Challenges and Limitations of information-hiding techniques.

Challenge	Feature Description
Detection and Countermeasures [45]	Adversaries constantly develop new methods to detect and counter information hiding techniques.
Performance Impact [13]	Some techniques may introduce computational overhead or latency, impacting system performance.
Key Management [13] [34]	Proper management of encryption or steganographic keys is crucial for security and integrity.
Robustness and Security Trade-Off [46]	Balancing robustness against detection with security can be challenging.
Compatibility and Interoperability [5]	Implementing across different systems or platforms may face compatibility or interoperability issues.
Legal and Ethical Considerations [5][13]	Use of information hiding techniques may raise concerns regarding privacy, intellectual property, or regulatory compliance.
Human Factor Vulnerabilities [5][13]	Techniques can be vulnerable to human errors or social engineering attacks.
Limitations of Steganography[5][13]	Steganography techniques have limitations on data capacity and may be affected by file formats or compression algorithms.

implications of using these techniques for deceptive purposes and ensure transparency and honesty in their operations.

Law Enforcement and National Security: Information hiding techniques can be used by law enforcement and intelligence agencies for legitimate purposes, such as gathering evidence or protecting national security. However, there is a potential for misuse, such as unauthorized surveillance or violating civil liberties. Organizations and authorities must strike a balance between security needs and individual rights, ensuring proper oversight and adherence to legal frameworks [48].

Ethical Responsibility: Organizations and individuals using information hiding techniques have an ethical responsibility to use them in a responsible and lawful manner. This includes obtaining proper consent, respecting privacy rights, and ensuring transparency and accountability in their operations. Regular ethical assessments and reviews should be conducted to identify and address any potential ethical concerns or risks associated with the use of these techniques [49]. **Considering these ethical considerations** is vital to prevent the misuse of information hiding techniques and ensure that they are used in a responsible, transparent, and ethical manner. Organizations should establish clear guidelines, policies, and oversight mechanisms to promote ethical use and mitigate potential risks [50-51]. Importance of staying updated is listed as much, the evolving nature of digital threats and attacks, the need for continuous research and development in information-hiding techniques, the role of individuals and organizations in staying informed and adapting to new challenges [34]. For information-hiding strategies to be used responsibly, transparently, and ethically, it is crucial to consider certain ethical factors. Organizations should set clear rules, regulations, and supervision procedures to encourage ethical use and reduce potential hazards. IHTs can be used to safeguard people's privacy and sensitive information. Nevertheless, there is a chance for abuse, such as invasions of privacy or unauthorized surveillance. Companies must ensure these methods are applied sensibly and by privacy laws and regulations. By concealing confidential information,

information-hiding strategies can aid in protecting intellectual property rights. However, there is a chance of abuse, such as dissemination without authorization or stealing someone else's intellectual property. Organizations should ensure these methods are applied legally and about other people's rights. IHTS, mainly used in steganography, can be used for misleading actions like disseminating false information or carrying out covert operations [52][53]. Organizations must ensure openness and honesty in their operations and consider the ethical ramifications of adopting these strategies for dishonest ends.

Businesses and individuals who employ an information-hiding approach are ethically required to do so responsibly and legally [52]. This entails gaining valid consent, upholding privacy rights, and guaranteeing responsibility and transparency in their operations. To detect and resolve any potential ethical concerns or dangers connected with these procedures, routine moral assessments and reviews should be carried out[53].

6. **Conclusion.**

This review paper aims to provide a comprehensive understanding of information hiding techniques in digital systems. By exploring various methods, applications, advantages, challenges, and ethical considerations, it contributes to the existing knowledge base and emphasizes the importance of staying updated in this rapidly evolving field. Overall, information hiding techniques (IHTs) have the potential to enhance data security and protect sensitive information. However, it is crucial to approach their implementation with careful consideration of the challenges, limitations, and ethical implications involved. The review is hoped that this review will inspire further research and innovation, leading to more robust and effective information hiding techniques to protect sensitive data in the digital realm.

Acknowledgment. This study was partially supported by the Vietnam National University, Ho Chi Minh City (VNU-HCM) under the VNUHCM-University of Information Technology's Scientific Research Support Fund.

REFERENCES

[1] T. T. Nguyen, J. S. Pan, and T. K. Dao, "An Improved Flower Pollination Algorithm for Optimizing Layouts of Nodes in Wireless Sensor Network," *IEEE Access,* vol. 7, pp. 75985–75998, 2019, doi: 10.1109/ACCESS.2019.2921721.

[2] M. Pagani and C. Pardo, "The impact of digital technology on relationships in a business network," *Industrial Marketing Management,* vol. 67, pp. 185–192, 2017.

[3] T. K. Dao, T. S. Pan, T. T. Nguyen, and S. C. Chu, "A compact Articial bee colony optimization for topology control scheme in wireless sensor networks," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 6, no. 2, pp. 297–310, 2015.

[4] J.-S. Pan and H.-C. Huang, *Information hiding and applications,* vol. 227. Springer Science & Business Media, 2009.

[5] R. Gupta, S. Gupta, and A. Singhal, "Importance and techniques of information hiding: A review," *arXiv preprint arXiv:* 1404.3063, 2014.

[6] J.-S. Pan, P.-W. Tsai, and H.-C. Huang, *Advances in intelligent information hiding and multimedia signal processing.* Springer, 2020.

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

[8] P. K. Saraswat and R. K. Gupta, "A review of digital image steganography," *Journal of Pure and Applied Science & Technology,* vol. 2, no. 1, pp. 98–106, 2012.

[9] A. D. Ker, "Steganalysis of embedding in two least-significant bits," *IEEE Transactions on Information Forensics and Security,* vol. 2, no. 1, pp. 46–54, 2007.

[10] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," *in International Conference on Computer Networks and Information Technology,* 2011, pp. 143–147.

[11] V. K. Ahire and V. Kshirsagar, "Robust watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for copyright protection of digital images," *IJCSNS International Journal of Computer Science and Network Security,* vol. 11, no. 8, pp. 208–213, 2011.

[12] S. Gupta and N. Dhanda, "Audio steganography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT)," *IOSR Journal of Computer Engineering,* vol. 17, no. 2, pp. 32–44, 2015.

[13] S. Katzenbeisser and F. Petitcolas, Information hiding. Artech house, 2016.

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

[15] T.-K. Dao, S.-C. Chu, T.-T. Nguyen, T.-D. Nguyen, and V.-T. Nguyen, "An Optimal WSN Node Coverage Based on Enhanced Archimedes Optimization Algorithm," *Entropy,* vol. 8, no. 24, 1018, 2022, doi: 10.3390/e24081018.

[16] J.-S. Pan, H.-C. Huang, L. C. Jain, and Y. Zhao, *Recent advances in information hiding and applications.* Springer, 2013.

[17] T.-T. Nguyen, T.-K. Dao, T.-T.-T. Nguyen, and T.-D. Nguyen, "An Optimal Microgrid Operations Planning Using Improved Archimedes Optimization Algorithm," *IEEE Access,* vol. 10, pp. 67940–67957, 2022, doi: 10.1109/ACCESS.2022.3185737.

[18] L. Li, S. Li, A. Abraham, and J.-S. Pan, "Geometrically invariant image watermarking using polar harmonic transforms," *Information Sciences,* vol. 199, pp. 1–19, 2012.

[19] H. Sajedi and S. R. Yaghobi, "Information hiding methods for E-Healthcare," *Smart health,* vol. 15, p. 100104, 2020.

[20] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications.* Cambridge University Press, 2009.

[21] T.-T. Nguyen, T.-K. Dao, M.-F. Horng, and C.-S. Shieh, "An Energy-based Cluster Head Selection Algorithm to Support Long-lifetime in Wireless Sensor Networks," *Journal of Network Intelligence,* vol. 01, no. 01, pp. 23–37, 2016.

[22] C.-Y. Jhou, J.-S. Pan, and D. Chou, "Reversible data hiding base on histogram shift for 3D vertex," *in Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007),* 2007, vol. 1, pp. 365–370.

[23] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan, "Genetic watermarking based on transform-domain techniques," *Pattern recognition,* vol. 37, no. 3, pp. 555–565, 2004.

[24] S. Weng, W. Tan, B. Ou, and 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, 2021.

[25] T.-T. Nguyen, J.-S. Pan, T.-Y. Wu, T.-K. Dao, and T.-D. Nguyen, "Node Coverage Optimization Strategy Based on Ions Motion Optimization," *Journal of Network Intelligence,* vol. 4, no. 1, pp. 1–9, 2019.

[26] T.-Y. Wu, C.-M. Chen, X. Sun, S. Liu, and J. C.-W. Lin, "A Countermeasure to SQL Injection Attack for Cloud Environment," *Wireless Personal Communications,* vol. 96, no. 4, pp. 5279–5293, 2017.

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

[28] I. Cox, M. Miller, J. Bloom, and C. Honsinger, "Digital watermarking," *Journal of Electronic Imaging,* vol. 11, no. 3, p. 414, 2002.

[29] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security,* vol. 2007, pp. 1–10, 2007.

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

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

[32] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials,* vol. 9, no. 3, pp. 44–57, 2007.

[33] F. Bélanger and R. E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," *MIS quarterly,* pp. 1017–1041, 2011.

[34] P. Gomber, J.-A. Koch, and M. Siering, "Digital Finance and FinTech: current research and future research directions," *Journal of Business Economics,* vol. 87, pp. 537–580, 2017.

[35] P. Eze, U. Parampalli, R. Evans, and D. Liu, “A new evaluation method for medical image information hiding techniques,” *in 2020 42nd annual international conference of the IEEE engineering in Medicine & Biology Society (EMBC),* 2020, pp. 6119–6122.

[36] T. Dao, J. Yu, T. Nguyen, and T. Ngo, “A Hybrid Improved MVO and FNN for Identifying Collected Data Failure in Cluster Heads in WSN,” *IEEE Access,* vol. 8, pp. 124311–124322, 2020, doi: 10.1109/ACCESS.2020.3005247.

[37] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” *Proceedings of the IEEE,* vol. 87, no. 7, pp. 1062–1078, 1999, doi: 10.1109/5.771065

[38] W. Chen, K. Zhou, W. Fang, K. Wang, F. Bi, and B. Assefa, “Review on blockchain technology and its application to the simple analysis of intellectual property protection,” *International Journal of Computational Science and Engineering,* vol. 22, no. 4, pp. 437–444, 2020.

[39] J. M. Shaikh, “E-commerce impact: emerging technology–electronic auditing,” *Managerial Auditing Journal,* vol. 20, no. 4, pp. 408–421, 2005.

[40] G. Qu, “Keyless public watermarking for intellectual property authentication,” *in International Workshop on Information Hiding,* 2001, pp. 96–111.

[41] M. Binjubeir, A. A. Ahmed, M. A. Bin Ismail, A. S. Sadiq, and M. K. Khan, “Comprehensive survey on big data privacy protection,” *IEEE Access,* vol. 8, pp. 20067–20079, 2019.

[42] Y. Wang et al., “A survey on metaverse: Fundamentals, security, and privacy,” *IEEE Communications Surveys & Tutorials*, arXiv:2203.02662, 2022.

[43] S. E. Kruck, D. Gottovi, F. Moghadami, R. Broom, and K. A. Forcht, “Protecting personal privacy on the Internet,” *Information Management & Computer Security,* vol. 10, no. 2, pp. 77–84, 2002.

[44] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Z. I. Shamsuddin, “Information hiding using steganography,” *in 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.,* 2003, pp. 21–25.

[45] Z. Wang, N. Gao, X. Wang, J. Xiang, D. Zha, and L. Li, “HidingGAN: high capacity information hiding with generative adversarial network,” *in Computer Graphics Forum,* 2019, vol. 38, no. 7, pp. 393–401.

[46] H. Nakamura and Q. Zhao, “Information hiding based on image morphing,” *in 22nd International Conference on Advanced Information Networking and Applications-Workshops (aina workshops 2008),* 2008, pp. 1585–1590.

[47] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” *Journal of network and computer applications,* vol. 126, pp. 45–58, 2019.

[48] G. W. Burruss, M. J. Giblin, and J. A. Schafer, “Threatened globally, acting locally: Modeling law enforcement homeland security practices,” *Justice Quarterly,* vol. 27, no. 1, pp. 77–101, 2010.

[49] E. Hassan, O. Yaqub, and S. Diepeveen, ”Intellectual property and developing countries: a review of the literature”. *RAND,* 2010.

[50] K.-S. Nguyen, T.-L Cao and V. A. Pham Van, “Efficient reversible data hiding using block histogram shifting with invariant peak points”, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 13, no. 1, pp. 78-97, March 2022.

[51] T.-T. Nguyen, T-D. Nguyen, T-G Ngo, V.-T. Nguyen, “An Optimal Thresholds for Segmenting Medical Images Using Improved Swarm Algorithm”, *Journal of Information Hiding and Multimedia Signal Processing,* vol. 13, no. 1, pp. 12-21, March 2022.

[52] H. Candelin-Palmqvist, B. Sandberg, and U.-M. Mylly, “Intellectual property rights in innovation management research: A review,” *Technovation,* vol. 32, no. 9–10, pp. 502–512, 2012.

[53] P. Hanel, “Intellectual property rights business management practices: A survey of the literature,” *Technovation,* vol. 26, no. 8, pp. 895–931, 2006.

[54] K. S. Nguyen, X. T. Tran, and T. H. Mai, ”Reversible Data Hiding based on dual images adapt to the secret message,” *Journal of Information Hiding and Multimedia Signal Processing,* vol. 14, no. 1, pp. 20-30, March 2023.

[55] M. A. Belhamra, and E. M. Souidi, “An Information Hiding Scheme for Live P2P Streaming Based on the R2 Protocol,” *Journal of Information Hiding and Multimedia Signal Processing,”* vol. 12, no. 2, pp. 102-115, June 2021.

[56] J.-S Pan, M. Zhu and S.-C. Chu, “Robust digital watermarking with parallel compact sparrow search algorithm applied for QR code”, *Journal of Information Hiding and Multimedia Signal Processing,* vol. 13, vo. 2, pp. 124-144, June 2022.