https://doi.org/10.31891/csit-2025-4-3
UDC 004.681.3

SHELEST Mykhailo, PIDLISNYI Yurii
National University “Chernihivska Politechnika”
KAPUSTIAN Mariia
Khmelnytskyi National University

METHODS OF HIDING DATA IN COMPUTER NETWORKS: FROM CLASSICS TO IoT AND Ai

The article presents an overview of key methods in network steganography, including the classification of data hiding techniques in network protocols and discussion of promising directions for further research. Special attention is paid to the use of steganography in modern network environments such as IoT, as well as the application of artificial intelligence to traffic masking. The paper also outlines current approaches to hidden channel detection and threat modeling in digital communication systems.

Keywords: network steganography, covert channels, IoT, transmission protocols, cybersecurity, steganalysis, information security.

ШЕЛЕСТ Михайло, ПІДЛІСНИЙ Юрій
Національний університет «Чернігівська Політехніка»
КАПУСТЯН Марія
Хмельницький національний університет

МЕТОДИ ПРИХОВУВАННЯ ДАНИХ У КОМП’ЮТЕРНИХ МЕРЕЖАХ: ВІД КЛАСИКИ ДО IoT ТА ШІ

У статті здійснено комплексний аналіз сучасних методів приховування даних у комп’ютерних мережах, що формують окремий напрям інформаційної безпеки — мережеву стеганографію. Розглянуто еволюцію підходів до прихованої передачі інформації: від класичних методів модифікації полів мережевих пакетів до сучасних гібридних рішень, орієнтованих на середовища Інтернету речей (IoT), мобільні та високонавантажені мережі, а також нові транспортні протоколи. Запропоновано узагальнену класифікацію методів мережевої стеганографії залежно від змінюваних характеристик трафіку, зокрема модифікації вмісту пакетів, параметрів передачі та комбінованих підходів.

Особливу увагу приділено аналізу відомих представників мережевої стеганографії, таких як LACK, RSTEG, PadSteg, TranSteg, HICCUPS та методи, що використовують особливості сучасних протоколів, зокрема QUIC. Наведено порівняльну характеристику цих методів за показниками пропускної здатності, складності реалізації, вартості впровадження та стійкості до виявлення. Показано, що жоден із методів не є універсальним, а ефективність прихованого каналу визначається компромісом між обсягом переданих даних і рівнем його маскування.

Окремо розглянуто сучасні підходи до виявлення прихованих каналів, включаючи статистичний аналіз трафіку, методи машинного навчання, глибокий аналіз пакетів і часові методи стеганоаналізу. Обґрунтовано необхідність формалізації загроз, пов’язаних із використанням прихованих каналів, та оцінювання їх впливу на конфіденційність, цілісність і доступність інформації. Визначено перспективні напрями подальших досліджень, пов’язані з інтеграцією штучного інтелекту, розвитком IoT-інфраструктур і формуванням адаптивних систем протидії мережевій стеганографії.

Ключові слова: мережева стеганографія, приховані канали, IoT, протоколи передачі, кібербезпека, стеганоаналіз, інформаційна безпека.

Received / Стаття надійшла до редакції 04.10.2025
Accepted / Прийнята до друку 14.12.2025

Introduction

In modern steganography, *network steganography* is actively developing as a separate direction. Unlike cryptography, which hides the content of a message, steganography hides the very fact of the existence of a message, which makes it especially relevant in the context of digital censorship, cyber surveillance and data leakage.

Related works

Network steganography encompasses methods of hiding information in network traffic structures, such as packet headers, time characteristics, service fields and protocol logic [1,2]. It is based on the principles of computer steganography, in particular, the detection of insignificant fragments in the digital environment and replacing them with hidden messages [3, 4, 5, 6]. A significant feature of the current stage of development of network steganography is the emergence of new environments for hiding:

-the emergence of highly loaded mobile networks with dynamic routing (5G);

-IoT infrastructure, characterized by a large number of devices with limited resources and weak security;

-quickly changing application protocols (QUIC, HTTP/3), which have greater complexity and flexibility compared to their predecessors.

These changes create new challenges: on the one hand, the possibility of masking information in new traffic formats increases, and on the other hand, it becomes more difficult to detect covert channels. A particularly promising and at the same time dangerous trend is the use of artificial intelligence (AI) in network steganography:

-for the purpose of automatic adaptive masking of steganographic traffic;

-for building communication channels resistant to detection;

-at the same time - in the development of intelligent systems for detecting covert channels (deep steganography).

The [2] presents a method for detecting steganography in network protocols based on multi-level analysis of derived and aggregated metrics using machine learning. The goal is to provide steganography in networks with a large number of devices. Performance considerations, results, and application of the method for multi-level detection of the RSTEG technique are presented.

In [7] a visually robust image steganography (VRIS) model is designed for double deception is presented. VRIS improves visual security by optimizing the extraction and merging of features of secret and cover images, ensuring their high similarity. To deceive machine learning models, VRIS uses supervised Gaussian noise and a discriminator that learns to distinguish between noisy encrypted images and original covers. In the process of competitive learning, VRIS and the discriminator are mutually improved, improving the deception ability. In addition, the model offers a new method for extracting and reconstructing secret images, which guarantees information protection and allows legitimate users to recover data from multi-scale features. Experimental results demonstrate the high efficiency of VRIS: significant PSNR and SSIM values on LFW and a misclassification rate of 99.24% compared to ResNet50 on Mini-ImageNet.

As AI becomes more sophisticated, traditional digital steganography methods become more vulnerable to detection and armed attacks. To improve security, [9] proposes a new AI-driven steganography framework with a multi-stage embedding process that combines basis, residual, and dense encoders. Additional robustness is provided by integrating wavelet transform with convolutional, Bayesian, and graph neural networks. Experiments on FashionMNIST and MNIST demonstrate high performance against various attacks. Although CNNs provide the highest baseline accuracy, BNNs show significantly better robustness against gradient attacks: during the FGSM attack on MNIST, BNN models maintained over 98% accuracy, while CNNs dropped to 10–18%. The proposed approach is a robust solution for creating secure next-generation steganography systems.

The paper [10] presents a multi-secret steganography system for the Internet of Things that uses two convenient sensors — a thumb joystick and a touch sensor — for covert data entry. The system allows embedding multiple messages into a single container using different algorithms, using two low-resource video steganography methods for mp4 files: videostego and metastego. The selected sensors can be replaced by others with similar functionality.

Unlike traditional methods, generative steganography creates carriers directly from messages, avoiding modifications detectable by analysis. Game-behavior-based steganography naturally integrates into real-world scenarios, ensuring high imperceptibility. The paper [11] proposes a method based on Chinese Chess (Xiangqi) records. Using the AlphaZero model, secret information is encoded by selecting chess moves that satisfy a probability threshold strategy. To ensure realistic gameplay, game process control and a fixed opening database are applied. The method hides an average of 413 bits per carrier and effectively resists attacks. Anti-steganalysis accuracy on XuNet and YeNet reached 0.498 and 0.497, respectively, demonstrating superiority over other behavior-based data hiding technologies.

Traditional audio steganography alters cover features, making hidden data easily detectable by neural networks. To address this, a coverless steganography model based on WaveGAN is proposed in [12], which directly synthesizes stego-audio. A specially designed extractor with resolution blocks reconstructs the secret signal without modifying any external carriers. In this work experiments confirmed that due to the absence of an original cover, modern steganalysis fails to detect the secret. The MOS metric indicates high audio quality, while the capacity reaches 50% of the file size or 22–37 semantic bits in a two-second recording. Spectrogram analysis and robustness tests proved that the extractor successfully recovers semantics even in the presence of noise, ensuring reliable transmission.

[13] presents Stego-STFAN, an innovative approach to video steganography. By employing Spatial-Temporal Adaptive Filter Network (STFAN) alongside an Attention mechanism, the model effectively combines temporal and spatial domains for data hiding. This leverages video redundancy and fine details (edges, fast-moving pixels) to generate high-quality stego-frames. The method utilizes Discrete Wavelet Transform (DWT) for additional feature extraction, enhancing secret recovery. Stego-STFAN achieved metrics of 27.03 and 23.09, approaching state-of-the-art results. This solution expands data transmission channels while adhering to the core steganographic principle: message security is inversely proportional to its size, making video an ideal carrier for large volumes of information.

Image steganography enables covert data transmission by embedding secret messages or images into a 'stego-carrier.' Although modern methods minimize visual distortion, they are often vulnerable to lossy compression (e.g., JPEG format), which hinders accurate information extraction during real-world transmission. To address this challenge, [14] proposes the JPEG Steganography Network (JSN) based on reversible neural networks. The method integrates the JPEG encoding process, utilizing Discrete Cosine Transform (DCT) and quantization to create standard-compliant stego-images. Extensive testing confirms the effectiveness and practicality of JSN for secure data transmission in real-world environments.

Image steganography aims to hide data within covers, yet deep neural network methods often produce visual artifacts due to shifting secret data coordinates during training. In [15] it is proposed a layerwise adversarial training method to resolve this issue. By integrating sub-networks and discriminators into each layer, we stabilized secret localization and reduced memory requirements. Testing across two datasets confirmed that the proposed approach significantly outperforms current state-of-the-art methods in preserving visual quality and data recovery accuracy.

Biometric research for authentication aims to replace passwords, but the public nature of physical traits makes digitised data protection critical. Integrating biometrics with steganography provides an additional security layer for access control and data transmission. However, this synergy has yet to find practical real-world application. A literature review suggests that future efforts should focus on establishing embedding standards, securing key exchange, addressing legal implications, and developing unified industry regulations for the implementation of these technologies. Based on a review of academic and industrial literature, in [16] it is proposed that future research focuses on identifying acceptable levels of data embedding, ensuring the secure exchange of steganographic keys, analyzing legal implications, and developing industry standards.

Thus, network steganography turns into a two-way technological competition, in which both concealment and countermeasures are involved, developing in parallel.

The relevance of the research lies in the need to adapt existing methods to modern conditions and develop new approaches to hiding data in computer networks.

Classification of network steganography methods

Network steganography uses network protocols of the OSI reference model - the network model of open systems interaction - as a carrier of hidden data. The methodological basis of network steganography is the theory of covert channels [1]. In general, network steganography methods are a family of methods that modify data in network protocol headers or in the payload fields of packets, or change the structure of packet transmission in a particular network protocol (sometimes several at the same time). The correct classification of such methods allows you to systematize and facilitate the choice of an approach depending on the specific conditions and requirements for the covert channel.

In the scientific literature, network steganography methods are conventionally divided into three main groups (Fig. 1), depending on which traffic characteristics are changed to hide information.

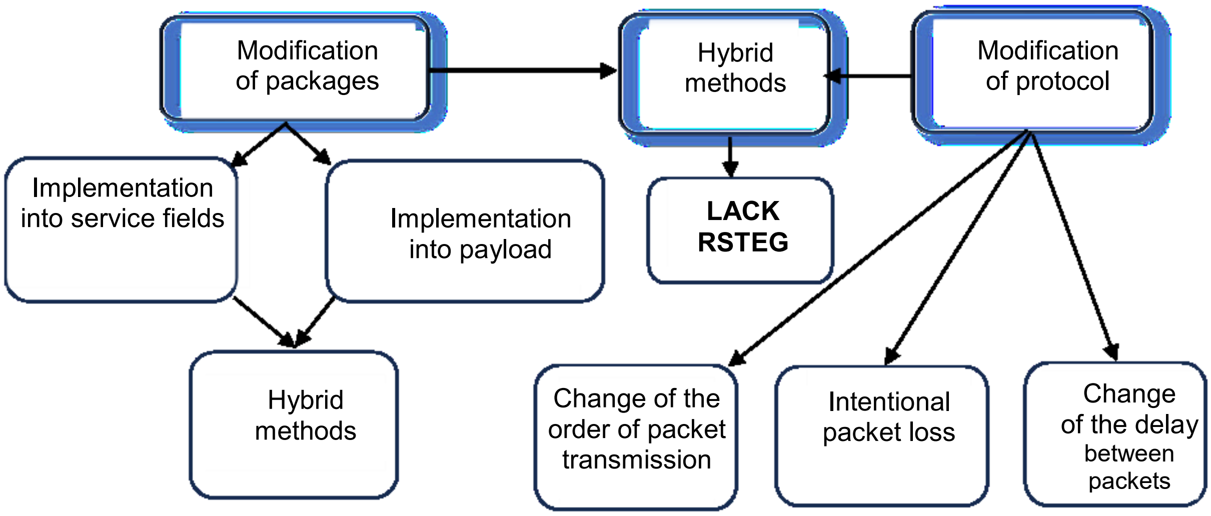
Modification of packages
Hybrid methods
Modification of protocol
Implementation into service fields
Implementation into payload
LACK RSTEG
Hybrid methods
Change of the order of packet transmission
Intentional packet loss
Change of the delay between packets

Fig.1. Classification of network steganography methods

1. Methods for modifying network packets. This group is based on direct modification of the content or service parts of network packets:

-Modification of protocol header fields - undefined or reserved bits in IP, TCP, UDP, ICMP, etc. are used. Example: use of the TTL field or URG/ACK flags in TCP.

-Modification of payload fields - hiding data directly in the packet body, for example, in the audio stream or in the MIME header fields.

-Combined methods - a combination of embedding data in both headers and payload.

Such methods are quite effective in conditions of stable traffic, but can be detected by deep packet inspection.

2. Transmission protocol modification methods. These approaches change the behavioral parameters of traffic without changing the data itself:

-Reordering packets — reordering packets based on the encoding of the hidden message;

-Modifying the intervals between packets — manipulating the delay time (timing channels);

-Injection of losses / retransmissions — intentional omissions or retransmissions of packets. For example, in TCP, the package number can be used as a container.

These methods are harder to detect, but their throughput is usually lower. Often used in real time (VoIP, streaming).

3. Mixed (hybrid) methods. This class combines modification of the transmission structure with manipulation of the content:

-LACK (Lost Audio Packets Steganography) — intentional retention of VoIP packets that will not be reproduced by the recipient, but may contain hidden information;

-RSTEG (Retransmission Steganography) — hidden data is transmitted in repeated TCP packets, which are artificially triggered;

Such methods are characterized by high stealth and adaptability, but often depend on network characteristics (delays, jitter, buffering).

Overview of representative network steganography methods

The most famous representatives of network steganography are the LACK, RSTEG, PadSteg, TranSteg and HICCUPS methods. Each of them has its own strengths: for example, TranSteg provides high throughput, but requires voice codec conversion; HICCUPS provides a high level of stealth, but is extremely limited in bandwidth. The further choice of a specific method depends on the requirements for bandwidth, stealth and the specifics of the network environment.

Let us consider the principles of operation of the main network steganography methods, which demonstrate a variety of approaches to hiding information in network traffic.

The **LACK (Lost Audio Packets Steganography) method** uses the features of the RTP protocol, which is used in IP telephony. The method consists in deliberately delaying audio packets that are considered lost by the receiver and are not reproduced. Hidden information is embedded in these packets. The advantages of this method are high real-time stealth and the use of standard VoIP mechanisms. Disadvantages include: limited bandwidth and possible degradation of audio quality if overused.

LACK steganalysis is difficult to perform because packet loss in IP networks is a "natural phenomenon" and therefore intentional losses introduced by LACK are not easily detected if they are within reasonable limits. Potential LACK steganalysis methods can be:

-Statistical analysis of lost packets in a subnet. This type of steganalysis can be implemented using a passive "watchdog" (or any other network node), for example, based on information included in Real-Time Transport Control Protocol (RTCP) reports. If for some calls the number of lost packets is higher than average, then such a criterion may indicate the potential use of LACK.

-Statistical analysis based on the duration of VoIP calls. If the probability distribution of call durations for a given subnet is known, then statistical steganalysis can be performed to detect VoIP sources that do not fit the distribution.

An active supervisor that analyzes all RTP streams in the network (the synchronization source identifier and the sequence number and timestamp fields from the RTP header) can identify packets that are too late and can no longer be used to restore the voice. The active supervisor can clean up their data fields or simply discard such packets. A potential problem that arises in this case is the removal of delayed packets that can be used to restore the conversation. Thus, the quality of the conversation can be significantly degraded. In addition, in this case, both steganographic calls and regular calls are affected.

The RSTEG (Retransmission Steganography) method is based on the mechanism of retransmission of packets in the TCP protocol. The sender intentionally does not confirm receipt of certain packets, forcing the sender to resend them. Hidden information is embedded in the resent packets. The advantages of this method are the use of the standard TCP mechanism and high resistance to packet loss. The disadvantages include the fact that its use may cause suspicion when analyzing traffic and reduce network efficiency due to additional transmissions.

The PadSteg method uses padding fields in Ethernet frames. Hidden information is embedded in these fields, which are usually filled with zeros. This provides ease of implementation and high invisibility at the Ethernet level. However, this limits bandwidth and depends on the specifics of the network equipment.

The TranSteg (Transcoding Steganography) method changes the audio stream codec to a smaller one, freeing up space for hidden data. For example, replacing the G.711 codec with G.729 allows embedding additional information without changing the packet size. The advantages of this method are its high throughput and invisibility for users, and the disadvantage is a possible decrease in sound quality.

The HICCUPS (Hidden Communication System for Corrupted Networks) method uses frame checksums in wireless networks. The sender intentionally creates frames with incorrect checksums that are ignored by standard receivers, but can be processed by special devices to extract hidden information. This provides high invisibility in wireless networks and the difficulty of detection by standard means, but at the same time the throughput decreases and there is a dependence on the specifics of the network equipment.

ICMP steganography uses the service fields of ICMP packets (for example, identifier, sequence number) to embed hidden information. Such packets can be transmitted between hosts without establishing a connection. The advantages of this approach are ease of implementation and the ability to transmit through network firewalls. The disadvantages include limited bandwidth and the possibility of detection during traffic analysis.

Steganography based on the QUIC protocol. The QUIC protocol is a modern transport protocol that combines the functions of TCP and TLS. Its features, such as stream multiplexing and header encryption, create new opportunities for hiding information. The advantages of this method include high stealth due to encryption and the complexity of traffic analysis, and the disadvantage is the high complexity of implementation and limited support in network equipment.

Comparative analysis of network steganography methods

None of the real network steganography methods is absolutely perfect or universal. The main dilemma is the compromise between bandwidth, implementation complexity, cost and resistance to detection. As the volume of hidden data increases, the probability of its detection by stegoanalysis increases. On the other hand, reducing the hidden load leads to a decrease in the efficiency of the communication channel.

It is especially important to take into account the dynamic nature of the network environment: for example, methods based on packet retransmission can cause excessive growth of packet losses, which attracts the attention of anomaly detection systems. In this case, it is necessary to dynamically control the intensity of retransmissions, taking into account background network activity.

The steganography method using packet retransmission RSTEG is an example of a hybrid approach that allows achieving higher bandwidth compared to methods based on changing the order or time of transmission, but at the same time increases the risk of detection. The implementation options of this method (based on RTO or SACK) significantly affect its characteristics.

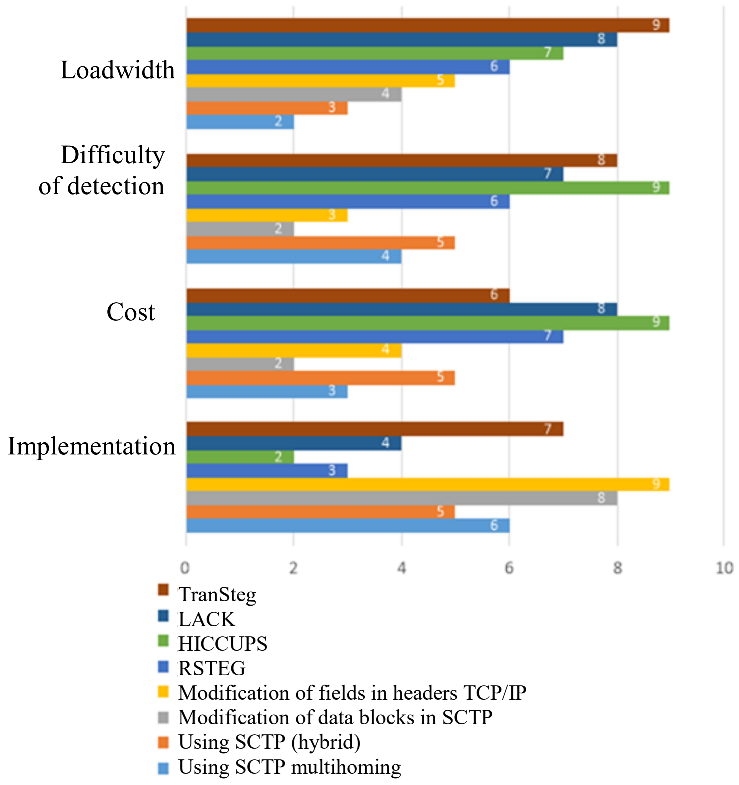

Fig. 2. Comparison of network steganography methods

Figure 2 shows a comparative diagram of different network steganography methods by four key parameters: throughput, detection difficulty, implementation cost and technical complexity of implementation. The assessment was carried out according to the data of generalized experimental studies [5–7]. The results are given in relative scores (from 1 to 10), where higher values indicate higher efficiency by the corresponding criterion.

Key conclusions from the analysis:

-TranSteg demonstrates the highest throughput, but has a high cost and implementation complexity.

-HICCUPS provides the highest resistance to detection at low cost and simple implementation, which makes it potentially the most balanced method.

-RSTEG and LACK have moderate indicators for all parameters, which allows them to be flexibly adapted to different scenarios.

-Methods that use the features of the SCTP protocol (for example, multihoming) also show good results, especially in terms of cost.

Thus, the choice of method should take into account the concealment goals, environmental constraints, and the potential for countermeasures from security systems. Comparative analysis allows us to determine the most appropriate directions for using the respective approaches in different contexts.

Covert Channel Detection and Threat Formalization

One of the most critical aspects of ensuring information security is the detection of covert communication channels used in steganography to transmit information in an undetectable manner. Modern network steganography is constantly becoming more complicated, its resistance to detection is increasing, and therefore the issue of developing effective steganalysis methods is gaining particular importance.

The development and implementation of covert channel detection systems (Steganalysis Detection Systems, SDS) is carried out in several directions:

-anomalous traffic analysis, which is based on the detection of statistical deviations in traffic parameters (packet sizes, intervals between them, the ratio of requests and responses, etc.). For example, regular microdelays or changed entropy of a packet sequence can signal the use of steganography.

-machine learning methods that use classification algorithms (SVM, Random Forest, neural networks) trained on reference samples of "normal" and "hidden" traffic. This allows you to detect atypical patterns and structures in the behavior of network traffic.

-deep packet inspection (DPI) analyzes the content and structure of network packets at the application level. The method is effective for detecting inserted data, header manipulation, use of Padding fields or reserved bits.

-timing analysis, which is focused on detecting hidden messages transmitted through changes in the intervals between packets (covert timing channels). Such methods are especially effective in real time for VoIP, video or streaming services.

-cross-protocol analysis that detects mutual dependencies between traffic of different protocols, which may indicate the presence of a hidden connection.

For systematic counteraction to steganography, it is important not only to record the signs of covert channels, but also to classify them as threats. Formalization is carried out on the basis of the following criteria:

-penetration level: it is determined at which level of the OSI model (from channel to application) the steganography method operates.

-potential throughput: the maximum amount of information that can be transmitted through the covert channel without violating functionality is estimated.

-probability of detection: the complexity of recognition by active or passive protection is taken into account.

-the degree of threat to confidentiality, integrity and availability (CIA-three).

For example, a high-speed channel in a critical system can create a direct risk of data leakage. Based on these parameters, a steganochannel risk index is formed. It can be used in early warning systems for attacks, wireless network inspection subsystems, and traffic and cyberthreat audit tools.

The above-listed modern approaches are focused on creating adaptive monitoring systems capable of dynamically updating steganochannel signature databases, automatically adjusting threshold values, and taking into account the context of the network environment (QoS, access policies, user mobility). Thus, the synthesis of detection and formalization allows not only to record the fact of a hidden connection, but also to assess its significance, which is key for designing reliable cyber defense systems.

Prospects and research directions in the field of network steganography

Network steganography continues to actively develop, adapting to new technological conditions and challenges. The scientific community is paying more and more attention to the latest challenges: detection of covert channels in the traffic of new generation protocols (QUIC, HTTP/3), steganography in the IoT environment and mobile networks, the use of artificial intelligence methods for both masking traffic and its analysis. The development of adaptive steganography and deep steganoanalysis based on neural networks is especially promising. Current trends indicate several key directions that determine the prospects for research in this area, in particular:

-*Integration with the Internet of Things* (IoT). The growth in the number of IoT devices creates new opportunities for hiding data in their traffic. IoT features, such as limited resources, non-standard protocols, and weak security, make them attractive for use in steganography. For example, it is possible to embed hidden data in the service fields of MQTT or CoAP protocols, which are widely used in IoT environments.

-*Application of artificial intelligence* (AI). AI opens up new horizons for network steganography. On the one hand, machine learning can be used to create adaptive concealment methods that change their behavior depending on network conditions. On the other hand, AI can be used to detect steganographic channels by analyzing traffic for anomalies. For example, machine learning can help in analyzing traffic to detect anomalies.

-*Development of new protocols and their analysis*. The emergence of new network protocols, such as QUIC and HTTP/3, opens up new opportunities for steganography. These protocols have other features that can be used for data hiding. For example, stream multiplexing in QUIC allows information to be embedded in different streams, which makes it difficult to detect a steganographic channel.

-*Increasing resistance to detection*. Developing methods that are harder to detect with traditional traffic analysis tools is an important area of research. This includes using statistical methods to disguise steganographic traffic as normal, as well as developing new algorithms that minimize deviations from normal traffic.

-*Steganography in wireless networks* (WLAN, 5G, 6G). With the development of wireless technologies such as 5G and the upcoming 6G, new opportunities for hiding information are emerging. The features of these networks, in particular high bandwidth and low latency, can be used to create steganographic channels. For example, manipulation of physical layer parameters such as signal modulation or frequency planning can serve as means of hiding data.

-*Quantum steganography*. Although quantum steganography is still in the research stage, it opens up new horizons for secure information transmission. The use of quantum properties, such as superposition and entanglement, can provide a high level of protection and invisibility of data transmission.

-*Ethical and legal aspects*. With the development of network steganography, questions of ethics and legality of its use arise. It is necessary to develop regulatory acts and ethical standards that regulate the use of steganography, especially in the context of personal data protection and national security.

-*Development of standards and regulatory framework*. With the growth of the use of steganography, there is a need to develop standards and regulatory documents that would regulate its use. This is especially important for ensuring the ethical use of technology and preventing its abuse.

The listed areas of research determine the future of network steganography and its role in ensuring information security in the context of rapid technological development.

Conclusions

Network steganography remains a dynamic area of research with a large number of practical applications, especially in the context of modern threats and the development of network technologies. The article considers modern approaches to the implementation of network steganography, which are based on the principle of hiding the very fact of message transmission in digital networks. The methods were systematized in three main areas: packet content modification, transmission logic change, and hybrid approaches. For each group, typical examples were considered and a comparative analysis of the main efficiency parameters was conducted.

With the growth of the size of computer networks, the widespread introduction of IoT devices, and the growing complexity of the data transmission infrastructure, both the potential and the risks associated with the use of covert communication channels are significantly expanding. The methodological base of steganographic technologies requires constant updating and adaptation to new network architectures, communication protocols, and traffic behavior models.

It is also important that steganographic channels can pose a serious threat to information security, as they are able to bypass traditional control measures without violating formal requirements for data formats and structures.

In the context of digital transformation and the rapid development of 5G/6G, AI and IoT, the following areas are becoming increasingly relevant:

-development of steganalysis methods with elements of machine learning;

-study of steganography in unstable and highly loaded networks;

-creation of secure traffic standards taking into account the possibilities of covert communication;

-integration of steganographic channel detection tools into network security tools.

Author Contributions according to CRediT

Conceptualization, M. Shelest; methodology, M. Shelest, M. Kapustian; software, Yu. Pidlisnyi; validation, Yu. Pidlisnyi, M. Shelest; formal analysis, M. Shelest; investigation, M. Kapustian; resources, M. Kapustian; data curation, Yu. Pidlisnyi; writing - original draft preparation, M. Shelest; writing - review and editing, M. Kapustian; visualization, M. Kapustian; supervision, M. Shelest; project administration, M. Kapustian; funding acquisition, M. Shelest. All authors have read and agreed to the published version of the manuscript.

Declaration on the use of generative artificial intelligence tools

In preparing this work, the authors used ChatGPT and Grammarly for: grammar and spelling checks, paraphrasing, and rephrasing. After using this tool/service, the authors reviewed and edited the content and take full responsibility for the content of this publication.

References

1. Mazurczyk W. Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications. Wiley-IEEE Press, 2016. 320 p.

2. Smolarczyk, M., Szczypiorski, K., & Pawluk, J. (2020). Multilayer Detection of Network Steganography. Electronics, 9(12), 2128. https://doi.org/10.3390/electronics9122128

3. Bohra, S.; Naik, C.; Batra, R.; Popat, K.; Kaur, H. Advancements in Modern Steganography Techniques for Enhanced Data Security: A Comprehensive Review. In Proceedings of the 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 28 February–1 March 2024; pp. 941–944.

4. Allasasmh, O.; Laila, A.D.; Aljaidi, M.; Alsarhan, A.; Samara, G. Integrated Approaches to Steganography: Embedding Static Information Across Audio, Visual, and Textual Formats. In Proceedings of the 2024 International Jordanian Cybersecurity Conference (IJCC), Amman, Jordan, 17–18 December 2024; pp. 33–39.

5. Katzenbeisser S., Petitcolas F. A. P. Information Hiding (Artech House Computer Security Series). Artech House, 2015. 312 p.

6. J.Mayer, Ed., 'Steganography - The Art of Hiding Information'. IntechOpen, Sept. 06, 2024. doi: https://doi.org/10.5772/intechopen.1001493

7. Zhang, F., Dong, Y., & Sun, H. (2024). Research on Key Technologies of Image Steganography Based on Simultaneous Deception of Vision and Deep Learning Models. *Applied Sciences*, *14*(22), 10458. https://doi.org/10.3390/app142210458.

8. Mazurczyk W., Caviglione L. Information Hiding as a Challenge for Malware Detection. IEEE Security & Privacy. 2015. T. 13, № 2. C. 89–93. DOI: https://doi.org/10.1109/MSP.2015.38

9. Huynh, N. D. N., Jiang, J., Chen, C.-H., & Yang, W.-C. (2025). AI-Based Steganography Method to Enhance the Information Security of Hidden Messages in Digital Images. Electronics, 14(22), 4490. https://doi.org/10.3390/electronics14224490

10. Koptyra, K., & Ogiela, M. R. (2023). Steganography in IoT: Information Hiding with Joystick and Touch Sensors. Sensors, 23(6), 3288. https://doi.org/10.3390/s23063288

11. Cao, Y., Du, Y., Ge, W., Huang, Y., Yuan, C., & Wang, Q. (2025). Generative Steganography Based on the Construction of Chinese Chess Record. Electronics, 14(3), 451. https://doi.org/10.3390/electronics14030451

12. Li, J., Wang, K., & Jia, X. (2023). A Coverless Audio Steganography Based on Generative Adversarial Networks. Electronics, 12(5), 1253. https://doi.org/10.3390/electronics12051253

13. Vergara, G. F., Giacomelli, P., Serrano, A. L. M., Mendonça, F. L. L. d., Rodrigues, G. A. P., Bispo, G. D., Gonçalves, V. P., Albuquerque, R. d. O., & Sousa Júnior, R. T. d. (2024). Stego-STFAN: A Novel Neural Network for Video Steganography. Computers, 13(7), 180. https://doi.org/10.3390/computers13070180

14. Su, P.-C., Cheng, Y.-H., & Kuo, T.-Y. (2024). JSN: Design and Analysis of JPEG Steganography Network. Electronics, 13(23), 4821. https://doi.org/10.3390/electronics13234821

15. Chen, B., Shi, L., Cao, Z., & Niu, S. (2023). Layerwise Adversarial Learning for Image Steganography. Electronics, 12(9), 2080. https://doi.org/10.3390/electronics12092080

16. McAteer, I., Ibrahim, A., Zheng, G., Yang, W., & Valli, C. (2019). Integration of Biometrics and Steganography: A Comprehensive Review. Technologies, 7(2), 34. https://doi.org/10.3390/technologies7020034

17. Wang, S., Zheng, N., & Xu, M. (2021). A Compression Resistant Steganography Based on Differential Manchester Code. Symmetry, 13(2), 165. https://doi.org/10.3390/sym13020165

18. Pan, Y., & Ni, J. (2024). Domain Transformation of Distortion Costs for Efficient JPEG Steganography with Symmetric Embedding. Symmetry, 16(5), 575. https://doi.org/10.3390/sym16050575

19. Hasić, A., Azizović, M., Azizović, E., & Saračević, M. (2025). Solvability and Nilpotency of Lie Algebras in Cryptography and Steganography. Mathematics, 13(11), 1824. https://doi.org/10.3390/math13111824

20. Siam, A.A.; Alazab, M.; Awajan, A.; Faruqui, N. A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity. IEEE Access 2025, 13, 14029–14050.

Mykhailo Shelest **Михайло Шелест**	DrS on Engineering, Professor of Cybersecurity and Mathematical Modelling Department, National University "Chernihivska Politechnika", Chernihiv, Ukraine. https://orcid.org/0000-0003-1090-0371 e-mail: mishel3141@gmail.com	доктор технічних наук, професор кафедри кібербезпеки та математичного моделювання, Національний університет «Чернігівська політехніка», Україна
Mariia Kapustian **Марія Капустян**	PhD, Associate Professor of Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine. https://orcid.org/0000-0001-9200-1622e-mail: kapustian.mariia@gmail.com	кандидат технічних наук, доцент кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, Хмельницький, Україна.
Yurii Pidlisnyi **Юрій Підлісний**	PhD student, recipient of the Doctor of Philosophy degree in specialty 122, Chernihiv Polytechnic National University, Chernihiv, Ukraine. https://orcid.org/0009-0001-9783-3898e-mail: ypodlesny@ukr.net	аспірант кафедри кібербезпеки та математичного моделювання, Національний університет «Чернігівська політехніка», Україна.