**УДК 004.056**

**Y. O. Sharko**

**S. O. Kot**

# DIGITAL WATERMARKING AND STEGANOGRAPHY IN THE MODERN DIGITAL WORLD

*Vinnytsia National Technical University*

***Анотація***

*У статті розглядаються методи прихованої передачі даних та захисту інтелектуальної власності в умовах глобальної цифровізації. Стеганографія та цифрові водяні знаки (ЦВЗ) визначаються як ключові інструменти забезпечення конфіденційності та автентичності інформації. Проаналізовано основні алгоритми вбудовування даних, їх стійкість до атак та роль у сучасних кіберфізичних системах. Наголошується на необхідності поєднання стеганографічних методів з криптографічним захистом для створення багаторівневих систем безпеки.*

**Ключові слова:** стеганографія, цифрові водяні знаки, захист інформації, криптографія, інтелектуальна власність, кібербезпека.

***Abstract***

*The article deals with methods of hidden data transmission and intellectual property protection in the context of global digitalization. Steganography and digital watermarking (DWM) are defined as key tools for ensuring confidentiality and authenticity of information. The main data embedding algorithms, their resistance to attacks, and their role in modern cyber-physical systems are analyzed. The emphasis is placed on the necessity of combining steganographic methods with cryptographic protection to create multi-layered security systems.*

**Keywords:** steganography, digital watermarking, information protection, cryptography, intellectual property, cybersecurity.

## Introduction

The current risk of unauthorized data access and intellectual property infringement in modern society is arguably as high as it has ever been. While cryptography focuses on concealing the content of a message, steganography goes a step further by hiding the very existence of the communication [1]. In an era of global change and heightened cyber threats, these technologies have become essential for securing sensitive information and protecting digital assets.

With the rapid advancement of technology and the increasing number of devices connected to the internet, digital media files such as images, audio, and video have become ideal containers for embedding hidden information. This opens significant opportunities for both legitimate content protection and new challenges related to the covert distribution of information.

## The evolution of data hiding in the digital age

Steganography is one of the oldest methods of protection, which has gained a new dimension in the digital era. The primary goal of modern computer steganography is to embed a secret message into a digital object-container in such a way that it remains imperceptible to an outside observer [2].

The most common method utilized is the Least Significant Bit (LSB) technique. This approach involves replacing the last bits of pixels in an image or samples in an audio signal with the bits of the secret message. Because the human eye or ear is unable to detect such minute changes, the hidden information remains secure. However, much like traditional warfare, there is an ongoing struggle between the developers of concealment methods and experts in steganalysis who use statistical methods to detect anomalies within files.

## Digital watermarking: A shield for intellectual property

Unlike general steganography, where the main goal is covert communication, digital watermarking (DWM) is specifically aimed at protecting the container itself [3]. A digital watermark is a mark embedded into content to identify the owner, track distribution, or verify the integrity of the file.

The effectiveness of DWM systems is measured by several key criteria:

- Robustness: The ability of the watermark to withstand various signal processing operations, such as compression (e.g., JPEG), cropping, or scaling.
- Imperceptibility: The embedded mark should not degrade the perceived quality of the original content.
- Capacity: The amount of data that can be reliably embedded without compromising the transparency of the watermark.

In the context of global markets, the use of DWM has become vital for combating piracy and ensuring the authenticity of digital evidence in legal proceedings [4].

## Cyber-criminality and global implications

Just as cyber warfare can paralyze infrastructure, the misuse of steganographic techniques can undermine the trust in digital information systems [5]. A significant challenge is the use of steganography within cyber-criminal activities. There have been recorded instances where malware used steganographic images to receive commands from command-and-control servers, allowing them to bypass traditional intrusion detection systems (IDS).

The international community emphasizes the importance of developing robust standards for verifying the authenticity of digital content. The combination of cryptographic protection and steganography (stego-cryptosystems) provides a "double barrier". Even if the fact of transmission is discovered, the adversary cannot read the contents without the corresponding private key.

## Conclusion

The designation of steganography and digital watermarking as strategic tools for information protection emphasizes their growing relevance in deciding the outcomes of modern security challenges. As digital threats become more sophisticated, nations and organizations must prioritize the development of effective data-hiding solutions to protect their interests. Future research must focus on increasing the robustness of DWM against AI-driven attacks. It is necessary to implement multi-layered security systems

that combine steganography with asymmetric encryption. The advancement of steganalysis is critical for the timely detection of hidden threats in global networks. Nations may better protect their digital sovereignty and build a more secure world by mastering these particular techniques and taking proactive actions to guard against the illicit use of information hiding.

## REFERENCES


1. Johnson N. F. Exploring Steganography: Seeing the Unseen / N. F. Johnson, S. Jajodia // Computer. – 1998. – Vol. 31, No. 2. – P. 26–34
2. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fridrich. – Cambridge : Cambridge University Press, 2009. – 448 p.
3. Digital Watermarking and Steganography / I. J. Cox, M. L. Miller, J. A. Bloom [et al.]. – 2nd ed. – Burlington : Morgan Kaufmann Publishers, 2007. – 616 p.
4. Wayner P. Disappearing Cryptography: Information Hiding: Steganography & Watermarking / P. Wayner. – 2nd ed. – Amsterdam : Morgan Kaufmann Publishers, 2002. – 432 p.
5. Rise of cyber warfare: The growing threat of cyber-attacks in modern conflicts [Electronic resource]. – 2023. – Mode of access: https://www.techuk.org/resource/natsec2023-wbd-20jan23.html.



**Yurii O. Sharko –** fourth-year student of Vinnytsia National Technical University, Faculty of Information Technologies and Computer Engineering, Vinnytsia, e-mail: sharko.yura2601@gmail.com.

**Sergii O. Kot -** Candidate of Philological Sciences, Associate Professor of the Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e–mail: kot.sergii@vntu.edu.ua.