УДК 004.7:004.65

Оболонська Я. О.

СТЕГАНОГРАФІЯ ЯК МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. *Технологія стеганографії використовується для захисту цифрової інформації шляхом приховання даних у графічних файлах без зміни їх зовнішнього вигляду.*

Ключові слова: *Стеганографія, цифрові зображення, LSB, DCT, DWT, водяні знаки, інформаційна безпека, криптографія.*

Abstract. *Steganography technology is used to protect digital information by storing data in graphic files without changing their appearance.*

Keywords: *steganography, digital images, LSB, DCT, DWT, watermarks, information security, cryptography.*

Вступ

У сучасному інформаційному середовищі безпечна передача даних є ключовим аспектом для організацій усіх рівнів від державних установ до комерційних компаній. Одним із методів захисту є стеганографія, яка забезпечує приховане передавання інформації шляхом вбудовування її в цифрові файли, зокрема зображення. На відміну від традиційного шифрування, яке лише робить дані незрозумілими для сторонніх, стеганографія приховує їх існування. Це дозволяє ефективно передавати конфіденційну інформацію, не викликаючи підозр у потенційних спостерігачів. Технологія знаходить застосування у захисті авторських прав, контролі достовірності цифрових документів та забезпеченні конфіденційності у різних сферах діяльності.

Результати дослідження

Стеганографія - це спеціальна технологія прихованого передавання інформації, яка дозволяє вбудовувати секретні дані в цифрові файли, зокрема графічні, щоб сторонній спостерігач не міг помітити їх наявність. Основна відмінність стеганографії від криптографії полягає в тому, що криптографія лише шифрує зміст, тоді як стеганографія маскує сам факт існування даних. Це дозволяє не лише захистити інформацію, а й приховати сам процес її передачі, що є критично важливим у державних, військових та корпоративних структурах, де виявлення факту передачі інформації може створювати серйозну загрозу [1].

У цифрових зображеннях приховані дані найчастіше вбудовують у пікселі за допомогою найменш значущих бітів (LSB). Метод LSB дозволяє записувати бінарну інформацію без помітної зміни кольору пікселів і є простим у реалізації. Він ефективний для невеликих обсягів даних, проте має суттєвий недолік є вразливість до стискання зображень або зміни їх формату, що може повністю зруйнувати приховану інформацію [2].

Щоб підвищити стійкість стеганографічних систем, застосовують частотні методи, такі як дискретне перетворення (DCT, DWT). У цих методах дані вбудовуються у коефіцієнти перетвореного зображення. Це робить їх менш помітними для ока та більш стійкими до змін розміру, стиснення або впливу шумів. Наприклад, при застосуванні DCT дані можуть бути вбудовані у середньочастотні коефіцієнти блоків зображення, що дозволяє зберегти приховану інформацію навіть після стискання у формат JPEG [2].

Стеганографія має широкий спектр практичного застосування. Одним із найпоширеніших напрямів є захист авторських прав. У цифрові зображення вбудовують водяні знаки, які підтверджують авторство та справжність контенту. Також стеганографія використовується для прихованої передачі конфіденційної інформації, де критично важливо, щоб сторонні особи не здогадалися про передачу даних [3].

Для підвищення рівня безпеки приховані дані часто шифрують перед вбудовуванням, створюючи подвійний рівень захисту. Навіть якщо приховану інформацію вдасться виявити, її зміст залишиться недоступним без відповідного ключа шифрування. Вона дозволяє маркувати та аутентифікувати цифрові зображення, контролювати їх цілісність і виявляти несанкціоновані

зміни. Це особливо важливо у медіа, судових доказах, освітніх матеріалах та корпоративних документах, де потрібно підтвердити авторство і захистити контент від підробки [3].

Незважаючи на численні переваги, стеганографія не позбавлена ризиків. Існує стегоаналіз – це спеціальні методи та програмне забезпечення, призначені для виявлення прихованих даних. Щоб протидіяти цьому, сучасні алгоритми вдосконалюються застосовують адаптивне або випадкове вбудовування, спеціальне кодування та стійкі до обробки методи, які зберігають дані навіть після зміни формату зображення або стискання [4].

Стеганографія тісно поєднується з іншими технологіями інформаційної безпеки. Наприклад, вона може використовуватися разом із криптографією, цифровими підписами та технологією блокчейн. Це дозволяє створювати багаторівневі системи захисту даних, де приховування факту передачі інформації, шифрування та перевірка цілісності відбуваються одночасно. Такі комбіновані підходи підвищують надійність і безпеку цифрової інформації, роблячи її стійкою до різних атак та несанкціонованого доступу [4].

Стеганографія є не лише інструментом прихованої передачі даних, а й основою сучасних технологій захисту цифрових зображень у медіа, освіті, судочинстві, корпоративних системах і військовій сфері. Вона дозволяє ефективно поєднувати маскування та шифрування даних, забезпечуючи високий рівень безпеки, конфіденційності та цілісності інформації. Сучасні дослідження підтверджують, що стеганографія продовжує залишатися актуальною та ефективною технологією захисту цифрових даних [4].

Висновки

Стеганографія є потужним засобом для захисту цифрової інформації, поєднуючи маскування даних та їх стійкість до обробки. Методи дозволяють ефективно інтегрувати дані у зображення, зберігаючи їх навіть після змін формату або стискання. Інтеграція стеганографії з криптографією, цифровими підписами та іншими технологіями безпеки дозволяє формувати комплексні механізми захисту, що гарантують конфіденційність, цілісність та контроль достовірності інформації. Незважаючи на потенційні загрози стегоаналізу, сучасні підходи, такі як адаптивне вбудовування та стійке кодування, підвищують рівень захищеності прихованих даних.

Список використаних джерел:

1. Комп'ютерна стеганографія : навчальний посібник / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець — Вінниця: ВНТУ, 2017. - 155 с.
2. Stuti Goel Stuti Goel. A Review of Comparison Techniques of Image Steganography. IOSR Journal of Electrical and Electronics Engineering. URL: https://www.researchgate.net/publication/272713701_A_Review_of_Comparison_Techniques_of_Image_Steganography.
3. Simplilearn. What is Steganography? A Complete Guide with Types & Examples. Simplilearn.com. URL: https://www.simplilearn.com/what-is-steganography-article.
4. Applied Sciences. Access Denied. URL: https://www.mdpi.com/journal/applsci/special_issues/multimedia_security#published.

Оболонська Яна Олександрівна *– студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, громадянка кафедри Військової підготовки, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com*

Obolonska Yana Oleksandrivna *- student of group 1BS-22b, faculty of information technologies and computer engineering, citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com*