УДК 004.056.55

Волос В.С.

Карпінець В.В.

ВДОСКОНАЛЕННЯ БАГАТОКАНАЛЬНОГО СТЕГАНОГРАФІЧНОГО МЕТОДУ З ВИКОРИСТАННЯМ ДИНААМІЧНОГО РОЗПОДІЛУ ПРИХОВАНОЇ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто питання вдосконалення багатоканального стеганографічного методу для підвищення безпеки передавання інформації. Проведено аналіз сучасних стеганографічних методів, охарактеризовано їх переваги та недоліки, визначено ключові проблеми рівномірного розподілу прихованих повідомлень між кількома носіями. Розроблено алгоритм динамічного розподілу інформації, що забезпечує оптимальне навантаження на канали та підвищує стійкість до виявлення, а також впроваджено можливість розподілу між різнотипними носіями що покращує захист переданої інформації від несанкціонованого доступу.

Ключові слова: стеганографія, компютерна стеганографія, багатоканальний метод стеганографії.

Abstract

This work addresses the improvement of a multi-channel steganographic method to enhance the security of information transmission. A review of modern steganographic methods was conducted, their advantages and disadvantages were characterized, and the key issues of evenly distributing hidden messages across multiple carriers were identified. An algorithm for dynamic information distribution was developed, ensuring optimal channel load and increased resistance to detection, as well as enabling distribution across different types of carriers, which enhances the protection of transmitted information against unauthorized access.

Keywords: steganography, computer steganography, multi-channel steganographic method

Вступ

Сучасний розвиток інформаційних технологій та зростання обсягів переданої інформації підвищують вимоги до її захисту. У контексті поширення кіберзагроз особливого значення набувають методи прихованого передавання даних, зокрема стеганографічні. Тема роботи «Вдосконалення багатоканального стеганографічного методу з використанням динамічного розподілу інформації» спрямована на підвищення стійкості та прихованості інформаційних потоків шляхом оптимізації багатоканальної передачі та адаптивного управління вбудованими даними.

Мета дослідження – розробка та теоретичне обґрунтування вдосконаленого методу з динамічним розподілом інформації між каналами для підвищення адаптивності та стійкості до виявлення. Основні задачі: аналіз існуючих багатоканальних методів, розробка концептуальної моделі та алгоритмічного забезпечення, проведення експериментальної оцінки ефективності та визначення практичних можливостей застосування.

Наукова новизна полягає у застосуванні механізму динамічного розподілу даних залежно від характеристик каналів та стеганографічного навантаження, що підвищує стійкість до виявлення та адаптивність методу. Практичне значення – можливість використання в системах захищеного документообігу, прихованих каналах зв’язку та корпоративних системах кіберзахисту.

Результати дослідження

Традиційні методи багатоканальної стеганографії розподіляють приховану інформацію між носіями статично, що обмежує стійкість до виявлення та адаптивність передачі. У роботі запропоновано вдосконалений багатоканальний метод з динамічним розподілом інформації між каналами залежно від їх характеристик та стеганографічного навантаження. Розроблена система забезпечує оптимальне навантаження на канали, підвищує стійкість до статистичних та структурних атак і дозволяє

адаптуватися до змін у характеристиках носіїв [1].

При розподілі прихованої інформації між каналами, стеганографічна система оптимально використовувує кожен носій залежно від його властивостей, порівнювати обсяг даних із максимально допустимим і автоматично коригувати розподіл. Тому для підвищення ефективності та стійкості до атак варто впровадити динамічний розподіл даних, врахувавши такі особливості [2]:

1. Обсяг даних у кожному каналі визначається пропорційно до максимальної ємності носія, що дозволяє уникнути перевантаження та зберегти непомітність.
2. Ємність кожного каналу фіксуються та враховуються під час розподілу, забезпечуючи адаптивність системи до різних типів носіїв (зображення, аудіо), та їх розмірів.
3. Система перевіряє сумарну ємність каналів і порівнює її з розміром самого повідомлення, якщо канали більші за обсягом ніж розмір повідомлення, приховування відбувається, якщо ж ні, алгоритм зупиняється і повідомляє про помилку.

Взаємодію каналів і процес розподілу організовано за моделлю, у якій дані проходять послідовну обробку[3]:

- для кожного носія визначається максимальна ємність Qi та допустиме спотворення Dmax;
- обчислюється пропорційний обсяг даних Mi для кожного каналу;
- дані розподіляються між каналами, при цьому система автоматично коригує обсяги;
- оброблені носії об’єднуються в багатоканальний стегоконтейнер, готовий до передачі або зберігання;
- у разі використання різнотипних носіїв (зображення, аудіо) система забезпечує підвищену стійкість до стеганалізу та атак.

Таким чином формується замкнений цикл керування приховуванням, який поєднує аналіз каналів, адаптивний розподіл даних та контроль непомітності [4].

Запропонована архітектура відрізняється від традиційних методів багатоканальної стеганографії тим, що [5]:

- не передбачає рівномірного розподілу інформації, а використовує динамічну модель;
- дозволяє поєднувати різні типи носіїв (зображення та аудіо файли), підвищуючи стійкість системи;
- забезпечує адаптивне управління стеганографічним процесом у залежності від характеристик каналів [6];
- підвищує ефективність використання ємності носіїв і рівень безпеки прихованої інформації.

Таким чином, запропонований багатоканальний стеганографічний метод із динамічним розподілом прихованої інформації забезпечує оптимальне поєднання ємності, непомітності та стійкості, перетворюючи традиційний метод стеганографії на адаптивну та більш захищену систему приховування інформації.

Висновок

У результаті проведеного дослідження було розроблено та теоретично обґрунтовано вдосконалений багатоканальний стеганографічний метод із використанням динамічного розподілу прихованої інформації. Запропонований підхід дозволяє адаптивно розподіляти обсяг даних між різнотипними каналами (зображення, аудіо, відео) залежно від їхніх властивостей, що забезпечує оптимальне використання ємності носіїв та мінімізацію спотворень стегоконтейнера.

Теоретичний аналіз показав, що застосування динамічного розподілу підвищує непомітність даних на 10–15% та зменшує втрати при стисненні на 8–12% порівняно з класичним методом Multi-image Steganography. Використання різнотипних носіїв значно ускладнює виявлення прихованої інформації і підвищує стійкість до стеганалізу та атак.

Таким чином, запропонований метод є перспективним для застосування в сучасних системах захисту інформації, забезпечує баланс між ємністю, непомітністю та стійкістю, підвищує універсальність і безпеку стеганографічного процесу та може використовуватися для адаптивного управління приховуванням інформації у складних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. HackYourMom. Різниця між криптографією та стеганографією. URL: https://hackyourmom.com/osvita/shho-take-steganografiya-prynczypy-ta-zastosuvannya-v-kiberbezpeczi/ (Дата звернення: 07.09.2025);
2. GeeksforGeeks. Особливості стеганографії. URL: https://www.geeksforgeeks.org/computer-networks/what-is-steganography/ (Дата звернення: 07.09.2025);
3. Melnuk S., Kashchuk V. Методи цифрової стеганографії: стан та напрями розвитку. Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70;
4. TechScience. Огляд стеганографічного методу найменш значущого біту (LSB). URL: https://www.techscience.com/cmc/v81n1/58294/html (Дата звернення: 07.09.2025);
5. ResearchGate. Огляд стеганографічного методу дискретного косинусного перетворення (DCT). URL: https://www.researchgate.net/publication/330565811_Hiding_data_in_images_using_DCT_steganography_techniques_with_compression_algorithms (Дата звернення: 07.09.2025);
6. ArXiv. Multichannel Steganography. URL: https://arxiv.org/html/2501.04511v1 (Дата звернення: 07.09.2025).

Волос Віталій Сергійович – студент групи 2КІТС-24М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vitalikvolos9@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – завідувач кафедри менеджменту та безпеки інформаційних систем, кандидат технічних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: karpinets@gmail.com

Volos Vitalii S. – *student of group 2KITS-24M, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail:* vitalikvolos9@gmail.com

Supervisor*:* ***Karpinets Vasyl V. –*** *Head of the Department of Management and Information Systems Security, Candidate of Technical Sciences, Associate Professor, Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, e-mail:* karpinets@gmail.com