

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТЕГANOГРАФІЧНИХ АЛГОРИТМІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЗОБРАЖЕННЯХ

COMPARATIVE ANALYSIS OF STEGANOGRAPHIC ALGORITHMS FOR HIDE INFORMATION IN IMAGES

Стеганографія – наука про методи захисту інформації шляхом приховування факту її існування в певному середовищі. Приховування факту існування таємного повідомлення завжди видавалося доцільним для його захисту, а наявність різних технічних, хімічних, фізичних і психологічних методів такого приховування забезпечувало можливість його реалізації.

Стеганографічна система або стегосистема – це сукупність засобів та методів, що використовуються для забезпечення прихованого каналу передачі даних^[3]. Основними елементами узагальненої стеганографічної системи зображено на рис. 1.



Рисунок 1. Елементи узагальненої стеганографічної системи

Контейнер – будь-яка інформація, призначена для приховування таємних повідомлень^[1]. Порожній контейнер – контейнер без вбудованого повідомлення. Заповнений контейнер або стегоконтейнер – контейнер, що містить вбудовану інформацію^[2]. Вбудоване (приховане або секретне) повідомлення – повідомлення, яке вбудоване в контейнер. Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації^[3].

При приховуванні даних у нерухомих зображеннях можливі такі методи:

- приховування даних у просторовій області;
- приховування даних в частотній області;
- розширення спектру.

Приховування даних у просторовій області може здійснюватися за допомогою наступних методів:

- метод заміни найменш значущого біта;
- метод псевдовипадкового інтервалу;
- метод псевдовипадкової перестановки;
- метод блокового приховування;
- метод заміни палітри;
- метод квантування зображення;

- метод Кутгера-Джордана-Боссена;
- метод Дармстедтера-Делейгла-Квісквотера-Макка.

Приховування даних в частотній області можливе при використанні таких методів:

- метод відносної заміни величин коефіцієнтів дискретно косинусного перетворення;
- метод Бенгама-Мемона-Ео-Юнга;
- метод Хсу і Ву;
- метод Фрідріха.

Оскільки, існує значна кількість стеганографічних методів приховування інформації у зображеннях, тому необхідно дослідити переваги та недоліки кожного з них, з метою ідентифікації доцільності застосування того чи іншого методу в конкретній ситуації та умовах.

Для виконання порівняльного аналізу стеганографічних методів приховування інформації у зображеннях було обрано наступні критерії:

- стійкість системи до модифікації контейнера;
- ефективність для стеганоаналізу;
- максимальний об'єм приховуваних даних.

Стеганографічні методи приховування інформації в зображеннях є доцільними при забезпеченні обмеженого доступу до інформації та її захисту. Розуміння того чи іншого методу, його переваги аз певних умов застосування сприятиме досягненню надійного рівня безпеки та захисту.

Література

1. Кузнецов О. О. К89 Стеганографія: навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с. [Електронний ресурс] – Режим доступу до ресурсу: <https://bit.ly/3mq3s6c>.
2. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.
3. О. В. Генне, ТОВ "Конфідент" журнал "Захист інформації. Конфідент", № 3, 2000.