|  |  |
| --- | --- |
| **Тема:** | Деструкція стеганограм з використанням методів сліпого розділення сигналів |
| **Виконав:** | Колодько Євген Сергійович |
| **Керівник:** | Прогонов Дмитро Олександрович |

АНОТАЦІЯ

У роботі проведено порівняльний аналіз використання методів сліпого розділення сигналів та традиційних методів активного стегоаналізу для деструкції повідомлень, прихованих у цифрових зображеннях згідно методам Дея, Агарваля та Джозефа.

Для оцінки спотворень стеганограм та стегоданих було використано функціонали якості деструкції стегоданих та спотворень контейнера. Дослідження проводилося з використанням тестового пакету зі 9000 псевдовипадково обраних зображень із стандартного пакету MIRFLICKR-25000.

Для проведення розрахунків було підготовано програмні модулі на мові програмування Python. Набір статистики при обробці незаповнених та заповнених контейнерів проводився з використанням обрахункових ресурів кластера НТУУ «КПІ». Час розрахунку склав 16 днів, було задіяно 48 обрахункових вузла суперкомпютера НТУУ «КПІ».

За результатами дослідження з’ясовано що використання методів сліпого розділення сигналів спричиняє у декілька разів менші спотворення контейнера, ніж традиційні методи, але дає порівняні значення деструкціх стегоданих при використанні одноетапних методів формування стеганограм.

Отримані результати можуть бути використаними для підвищення ефективності існуючих підсистем автоматичної деструкції вбудованих повідомлень у системах контролю трафіку.

ABSTRACT

The paper’s research is about comparing analysis of using blind signal separation methods and traditional active stegoanalysis methods for destruction of messages embedded in digital images due to Dey’s, Agarwal’s and Joseph’s algorithms.

Functionals of destruction quality of stegodata and container for the steganograms and stegodata assessments were used to estimate a quality of stegoanalysis methods. Research conducted using test package of digital images, consisted of 9000 pseudorandom picked fullcolor digital images from the standard package of images MIRFLICKR-25000.

Software Python-modules were written for the research calculations. The set of statistics was conducted using the cluster of NTUU “KPI”. Time calculation was 16 days using the 48 calculation nodes of supercomputer of NTUU “KPI”.

The research evaluated the using of blind signal separation methods can decrease the destruction of container in a few times, comparing to traditional methods, but the value of stegodata destruction stays the same using one-step methods of forming steganograms.

The results can be used for the improving the efficiency of existing subsystems of automatic destruction of messages in traffic control systems.

ВСТУП

Фахівцями з інформаційної безпеки було показано, що зловмисники використовують відкриті джерела, такі як соціальні мережі, для обміну секретними повідомленнями та координації терористичних атак [1]. Одним із способів секретної комунікації є передача стеганограм. Трафік сучасних соціальних мереж вимірюється терабайтами, тому немає можливості застосовувати до всіх зображень статистичні пасивні стегоаналізатори. Аналіз займає великий час (рахунок іде на секунди та десятки секунд), тому може застосовуватись лише в каналах з низькою пропускною здатністю, де є підвищені вимоги до безпеки.

Натомість в каналах з великою пропускною здатністю можливе застосування активних методів, метою яких є деструкція вбудованих стегоданих, що досягається незначними спотвореннями зображення-контейнера (ЗК). Оскільки сторона атаки не знає, яким чином було сформовано стеганограму, використані методи та параметри, доцільним є застосування методів сліпого розділення сигналів (blind source separation) у цілях активного стегоаналізу. Ці методи направлені на те, щоб розділити сигнал (зображення) на компоненти, спираючись лише на інформацію про їх суміш.

Метою даної роботи є аналіз ефективності застосування методів сліпого розділення сигналів для деструкції стеганограм з даними, вбудованими в області перетворення контейнера.

Для досягнення поставленої цілі необхідно вирішити наступні задачі:

1. Виконати огляд сучасних методів стеганографії (методи Дея, Агарваля та Джозефа) та активного стегоаналізу цифрових зображень(медіанна, вінерівська та гаусівська фільтрації).
2. Провести адаптацію сучасних методів сліпого розділення сигналів (метод головних компонент та метод незалежних компонент) для застосування у задач активного стегоаналізу.
3. Провести порівняльний аналізу відомих та запропонованих методів деструкції стеганограм.

Новизна роботи полягає у аналізі ефективності застосування методів сліпого розділення сигналів для вирішення задач активного стегоаналізу.