

ПРИХОВУВАННЯ ДАНИХ В ФАЙЛАХ ЗОБРАЖЕНЬ

Денисюк Н.В.

Науковий керівник – доц., к.т.н. Майданюк В. П.

Розрізняють дві групи методів приховування повідомлень в графічних файлах: спектральні методи; методи прямої модифікації зображення.

Перевагою використання в якості контейнера графічних файлів є можливість приховувати в них достатньо великі об'єми повідомлень різних типів та форматів. Спектральні методи ґрунтуються на використанні дискретних унітарних перетворень: Фур'є, Уолша-Адамара, Карунена-Лоева, та інших. При використанні методів цієї групи повідомлення приховується в спектральних складових зображення. Спектральні методи дозволяють вмонтовувати в контейнер більше інформації у порівнянні з методами прямого приховування, однак вимагають значних обчислювальних ресурсів.

Найбільш відомим серед методів прямої модифікації зображення є метод LSB (Least Significant Bit - найменший значущий біт). Суть цього методу полягає в заміні молодших бітів в кожному пікселі зображення на біти повідомлення, що приховується. Наприклад, якщо в якості контейнера використовуються кольорові зображення у форматі RGB, то в кожному пікселі зображення можна приховати до 6 біт повідомлення без помітної втрати якості. Єдиною умовою є те, щоб об'єм прихованих даних не перевищував розмір зображення-контейнера. Інший підхід, відомий як Appendix, ґрунтується на приховуванні повідомлень в області службової інформації. В будь-якому типі графічних файлів після області з даними знаходиться область службової інформації. Якщо записати приховане повідомлення в цю область, то при перегляді зображення помітити його неможливо. Оскільки, для не ущільнених типів файлів легко встановити розмір, знаючи параметри зображення, то повідомлення за допомогою даного методу краще приховувати в ущільнених форматах (jpg, gif та ін.). Цей метод простий в реалізації, його можна використовувати для приховування повідомлень практично в усіх типах файлів мультимедіа, але його легко виявити і видалити. Якщо керуватись критерієм максимальної швидкості приховування, то безсумнівні переваги мають методи прямої модифікації зображення, зокрема метод LSB, оскільки він є не тільки швидким, але і дозволяє приховувати повідомлення великого розміру. Однак, з точки зору стійкості до стегоаналізу, цей метод вимагає удосконалення, наприклад, за рахунок використання криптографічних методів до приховування або в процесі приховування. З урахуванням факту приховування тут достатньо найпростіших методів криптографічного захисту – гамування та розсіювання біт повідомлення по довжині зображення з використанням генератора псевдовипадкових чисел.