

СИСТЕМА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ КЛЮЧОВОЇ ІНФОРМАЦІЇ

Гладько А.І.

Науковий керівник – к.т.н, доцент, Войтович О.П.

На сьогодні досить важливим є питання збереження ключової інформації на серверах, що підключені до глобальної мережі Інтернет. Існує досить велика кількість способів взломати сервер, в тому числі оснований на тому, що найбільш важлива інформація зберігається в базах даних. Найчастіше зловмисники направляють основні зусилля на взлом баз даних. Альтернативою зберігання ключових даних у базах даних є їх захист за допомогою стеганографічних систем.

Для того щоб приховати ключову інформацію сервера в зображеннях пропонується використовувати модифікацію алгоритму теорії графів (Стефан Хетцль і Петра Мютцель). Основним принципом є модифікація значень елементів таким чином, що при поблочному зчитуванні за модулем m , отримується секретне повідомлення. Дані в блоках не змінюються, а лише обмінюються. Як стеганоконтейнери використовуються зображення типу JPEG та JPEG2000, а вибірками є коефіцієнти ДКП і вейвлет-перетворення.

Процес створення графу такий:

Створюється масив суміжностей. Для кожного значення s_i (елемент зображення, що використовується) створюється список можливих змін у визначеному радіусі r .

Створюється структура розповсюдженості вибірових значень.

Сортування вершин по рангу – кількості ребер, що з'єднані з даною вершиною.

Спочатку обмінюються вершини, що мають найменший ранг для забезпечення більшої кількості вершин з парами. Вершини, що не мають пар змінюють своє значення на необхідне.

Для того щоб отримати дані, їх необхідно зчитати поблочно з зображення за модулем r у порядку визначеним секретним ключем.

Для вбудовування ключових даних у зображеннях, пропонується використовувати окремий програмний продукт, доступ до якого має лише головний адміністратор. Дані про кожний з серверів приховуються в окремому зображенні, таким чином створюючи альбом. Вважається, що альбом має резервну копію, для захисту від активних атак. При роботі через мережу Інтернет рекомендується використовувати 2048-розрядні SSL-сертифікати.