УДК 681.511:3

АНАЛІЗ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ СИСТЕМ В МОДЕЛЯХ ПАСИВНОГО ТА АКТИВНОГО СУПРОТИВНИКІВ

Касянчук М.М.[1)], Квасниця О.В. [2)], Самарик П.С. [3)]
Тернопільський національний економічний університет
[1)] к.ф.-м.н., доцент; [2)] магістр; [3)] завідувач лабораторією

I. Постановка проблеми

На сьогодні цифрова стеганографія є досить наукоємкою дисципліною, інструментами для розвитку якої є методи теорії ймовірностей та математичної статистики, теорії швидких ортогональних перетворень, теорії апроксимації, теорії кодування, теорії складності, теорії похибок, цифрової обробки сигналів та зображень тощо. Разом з тим, зважаючи на її молодість, чимало проблем поки що знаходяться на початковій стадії свого вирішення.

Зокрема, мало уваги було присвячено аналізу стійкості запропонованих алгоритмів до різних атак та моделей активного та пасиного супротивників. Іншою важливою вимогою до стеганосистем є «непомітність» вбудованого повідомлення, для забезпечення якого спотворення, що вносяться у контейнер під час приховування в ньому інформації, повинні бути мінімальними, але забезпечувати при цьому необхідну стійкість до певних видів атак.

Крім того, на даний час не виявлено стеганографічних алгоритмів, що поєднують у собі відповідно високі стійкість та пропускну здатність за прийнятної обчислювальної складності своєї реалізації.

II. Мета роботи

Метою дослідження є системний аналіз стійкості різних стеганографічних систем при умові існування активного та пасивного супротивників.

III. Аналіз стійкості стеганографічних систем в моделях пасивного та активного супротивників

У роботі проаналізовано структури стеганографічних систем та здійснено системний аналіз методик оцінки їх стійкості, що дає змогу робити обгрунтований вибір типу стеганографічного перетворення в моделях пасивного та активного супротивників. Розроблено алгоритм побічної стеганографії в моделях активного і пасивного супротивників, який має більшу стійкість до стеганоаналізу.

Показано, що при організації стеганографічного каналу передачі інформації отримані у роботі результати дозволяють обґрунтовано вибирати параметри алгоритму Коха–Жао, які забезпечують необхідний рівень стійкості системи одночасно з максимально можливою «непомітністю» вбудованого повідомлення.

Для наочної демонстрації отриманих результатів побудовано узагальнені структурні моделі стеганографічних перетворень інформації з урахуванням пасивних і активних стегоаналітичних атак. Розроблено методи адаптивного вбудовування даних у сегменти зображень з використанням поліноміальних моделей та показано їх переваги в порівнянні з існуючими. Наведено практичні рекомендації по вибору відповідного параметра алгоритму Коха–Жао із заданою стеганографічною стійкістю до компресії контейнера. Зокрема, прийнятне значення параметра P алгоритму Коха–Жао перебуває в діапазоні $5 \le P \le 55$. Якщо $P < 5$, то повідомлення руйнується при найменшому стиску контейнера. Якщо $P > 55$, то видимі спотворення, внесені при вбудовуванні інформації в контейнер, надмірно великі. У випадку прийнятних значень параметра P алгоритм Коха–Жао може забезпечити стійкість до компресії контейнера з коефіцієнтом стиску $\alpha \ge 6$ при повній відповідності відновленого повідомлення або частковому його руйнуванні. Якщо потрібна стійкість до компресії контейнера з коефіцієнтом стиску $\alpha \le 5$, то алгоритм Коха–Жао непридатний.

Висновок

У роботі здійснено аналіз стійкості різних стеганографічних систем при умові існування активного та пасивного супротивників.

Список використаних джерел

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. – К.: МК–Пресс, – 2006. – 288 с.