Заснований на DHT ефективний метод стеганоперетворення

УДК 004.056.5

Ірина Борисенко[1], Ігор Якименко[2]

Національний університет «Одеська політехніка», [1]borisenko.i.i@op.edu.ua,
Західноукраїнський національний університет, [2]iyakymenko@ukr.net

Значна кількість сучасних стегометодів використовує дискретне перетворення Адамара (DHT) зображення-контейнера для вбудовування повідомлення [1,2]. Існує багато схем приховування повідомлення в коефіцієнтах DHT, в основу яких покладено розбивку контейнера на блоки розміром *n* x *n*, а стегоалгоритми використовують різні стратегії приховування елементів повідомлення в кожному блоці [3]. Проте вбудовування відбувається переважно послідовно, а рішення приймається локально. У результаті алгоритм не завжди знаходить найкращий глобальний варіант розподілу блоків повідомлення по блоках контейнера. Саме ця проблема визначає втрату потенційної ефективності алгоритму. Якщо для кожного фрагмента повідомлення існує кілька можливих блоків контейнера, в яких він може бути розміщений із невеликою кількістю корекцій, то природно постає задача вибору не просто будь-якого допустимого варіанта, а найкращого з погляду всієї сукупності можливих вбудовувань.

Метою роботи є оптимізація розподілення блоків повідомлення по блокам контейнера, в сенсі їх подібності по заданому критерію, та дослідження стійкості одержаного стегоповідомлення до статистичних атак стегоаналізу.

Можна виділити основні критерії подібності: косинусна подібність (Cosine similarity), яка показує наскільки напрямок вектора повідомлення збігається з напрямком вектора контейнера; кореляція (Pearson correlation), яка враховує лінійну залежність між коефіцієнтами блоку контейнера і повідомлення; енергетичний критерій (Energy matching).

Для стеганографії найчастіше використовують кореляцію або косинусну подібність, оскільки вони показують, наскільки добре повідомлення відповідає структурі контейнера.

Алгоритм оптимізації (укрупнена схема).

1.Обчислити спектр повідомлення DHT для кожного блоку M_i.

2. Обчислити спектр контейнера для кожного блоку C_j.

3. Для кожного M_i знайти блок C_j, який має найбільшу: кореляцію або косинусну подібність.

4. Вбудувати M_i саме у цей найбільш подібний C_j.

Зауважимо, що для M_i може знайтись не один блок контейнера, що відповідатиме заданому критерію подібності, тому на третьому кроці алгоритму пропонується для кожного M_i знайти усі блоки C_j, які задовільнять заданому критерію з одночасною побудовою таблиці, рядки і стовпці якої відповідатимуть номерам блоків повідомлення та контейнера, а елементами таблиці будуть значення заданого критерія подібності. Проблема зводиться до вирішення задачі оптимального призначення, для розв'язку якої існує достатньо ефективних алгоритмів. Коли призначення визначено, тобто сформувались пари

$M_i \rightarrow C_j$, запускається процес вбудовування з одночасним формуванням ключа *K*, який є парами (i,j), де i,j – номери блоків.

Експериментальні дослідження показали: базове вбудовування (послідовне блок-за-блоком) дає збурення контейнера Δ RMS (Root Mean Square) =4,2, PSNR (дБ)=38, BER (%)=12; оптимізоване вбудовування Δ RMS=2,7 PSNR (дБ)=42, BER (%)=6.

Стійкість до деяких статистичних атак стеганоаналізу представлена графіками на рис.1.

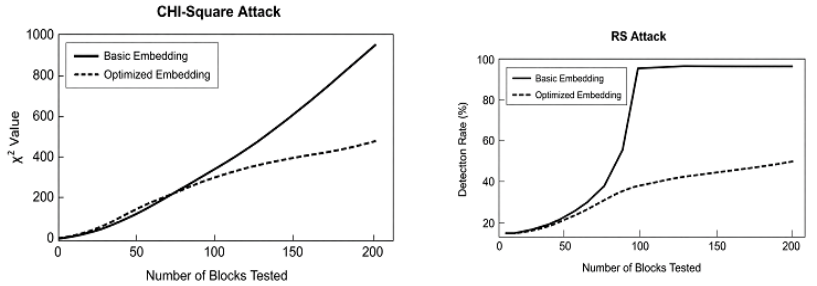

Рис.1. Графіки стійкості стего до атаки Хі-квадрат (зліва) та RS-атаки (справа)

Аналіз побудованих графіків показує, що оптимізоване вбудовування блоків повідомлення знижує статистичні відхилення, тому атака CHI-square менш ефективна. Це підтверджує, що адаптивний вибір блоків за критеріями подібності дає реальний виграш у стійкості. Оптимізоване вбудовування також знижує статистичну різницю між групами пікселів (Regular/Singular), тому RS-тест виявляє менше аномалій. Це підтверджує, що адаптивне вбудовування блоків за критеріями подібності підвищує стійкість не лише до CHI-square, а й до RS-атаки.

Алгоритм відновлення вбудованого повідомлення не вимагає вихідного зображення завдяки ключу *K* («сліпий»). Виконується зворотній процес: перетворення DHT обраного за ключем блока контейнера, застосування оберненого алгоритму вбудовування, а потім DHT до одержаного спектра.

Таким чином, оптимізація за критерієм подібності менше спотворює контейнер, а отже підвищує стійкість до статистичних атак стегоаналізу, дає вищу точність відновлення.

1. Zhang Y. Q., Zhong K., Wang X. Y. High-Capacity Image Steganography based on Discrete Hadamard Transform. IEEE Access. 2022. Vol. 10. P. 65141-65155. doi: 10.1109/ACCESS.2022.3181179
2. Helal S., Salem N. A Hybrid Watermarking Scheme Using Walsh Hadamard Transform and SVD. Procedia Computer Science. 2021. Vol. 194. P. 246-254. https://doi.org/10.1016/j.procs.2021.10.080
3. Prabha K., Sam I. S. A novel blind color image watermarking based on Walsh Hadamard Transform. Multimedia Tools and Applications. 2020. Vol. 79, No. 9. P. 6845-6869. doi: 10/1007/s11042-019-08212-w