

МЕТОДИ РЕКОНСТРУКЦІЇ КОНТЕЙНЕРІВ З ВИКОРИСТАННЯМ РОЗРІДЖЕНИХ ТА НАДЛИШКОВИХ БАЗИСІВ

Є. М. Терещенко^{1, а}, Д. О. Прогонов^{1, б}

¹ Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

В роботі представлені результати дослідження ефективності реконструкції зображень-контейнерів (ЗК) з використанням розріджених та надлишкових базисів в порівнянні з деструкцією стегоданих після проведення медіанної фільтрації (МФ). Порівняння проводилося з використанням стандартних метрик якості цифрових зображень (МЯ ЦЗ): MSE, NCC, SSIM. Вбудовування стегоданих відбувалося адаптивним алгоритмом HUGO.

Ключові слова: реконструкція контейнеру, медіанна фільтрація, розріджені та надлишкові базиси.

Вступ

Протидія витоку інформації прихованими (стеганографічними) каналами передачі конфіденційних даних відбувається з використанням активних та пасивних методів стегоаналізу. Обмеженість або відсутність апріорних відомостей щодо способу передачі та особливостей стеганографічного методу приховання повідомлень у файлах-контейнерах (ФК), зокрема цифрових зображеннях (ЦЗ), а також постійне вдосконалення існуючих та поява нових методів стеганографії суттєво ускладнюють виявлення стеганограм та підвищують їх стійкість при застосуванні відомих методів стегоаналізу.

Пасивні та активні методи стегоаналізу вирішують дві різні задачі: виявлення факту наявності прихованих даних в контейнері (з деякою ймовірністю) та деструкція стегоданих відповідно. На даному етапі актуальним завданням є повне відновлення вихідного контейнеру. Це дозволить прийняти рішення про віднесення ЦЗ до класу ЗК або до класу стеганограм (задача виявлення). До того ж, реконструкція ЗК автоматично знищує приховане повідомлення (стего), що відповідає задачі деструкції. Проте для відновлення невідомого ФК необхідно використовувати деякі базис та базу даних, на основі яких можна описати вихідний контейнер.

Таким чином, представляє інтерес розробка узагальненого методу реконструкції незаповненого контейнеру, що дозволить з високою точністю відновлювати ЗК в умовах наявності лише апріорних даних про контейнер.

1. Методи стегоаналізу цифрових зображень

Для знаходження каналів обміну стегоданими широко використовуються методи сигнатурного, статистичного стегоаналізу [1]. Сигнатурні методи направлені на певний метод вбудовування, а, отже, не завжди можуть протистояти новим загрозам. Обмеженням практичного застосування статистичних методів є їх висока обчислювальна складність, за рахунок чого зростає час налаштування стегодетектора. Цільові методи виявлення потребують апріорних даних щодо особливостей стеганографічного методу. Універсальні методи працюють незалежно від особливостей алгоритму вбудовування інформації, типу контейнера, проте вони не дозволяють виявляти стеганограми з високою точністю у випадку низького та середнього ступенів заповнення ЗК стегоданими [2, 3].

Зважаючи на існуючі обмеження методів пасивного стегоаналізу, використовують методи активного стегоаналізу: внесення спотворень або деструкція стегоданих, зокрема фільтрація, зміна масштабу ЦЗ, зміна значень яскравості пікселів ЦЗ за деяким нелінійним законом та інші [4].

Для очищення ЦЗ від шумів широко використовуються МФ [5]. Процедура фільтрації полягає у заміні значення яскравості пікселя на значення медіани розподілу яскравості всіх пікселів в деякому околі. Значення яскравості пікселів у певному блоці стеганограми впорядковуються за зростанням та знаходиться середнє значення – медіана. Значення центрального відліку у блоці замінюється медіаною. В результаті такої заміни біти вбудованого повідомлення змінюються і відбувається деструкція.

^аtereschenkoliza0511@gmail.com

^бprogonov@gmail.com

2. Реконструкція контейнерів з використанням розріджених та надлишкових базисів

Сигнали, які мають розріджене представлення в деякому базисі, можуть бути точно або наближено відновлені (реконструйовані) за своїми проекціями, причому число цих проекцій може бути значно менше розмірності вихідного сигналу [6].

Під розрідженим представленням розуміється, що частка ненульових коефіцієнтів розкладу сигналу $x(t)$ в деякому базисі функцій $\psi_1(t), \psi_2(t) \dots, \psi_n(t)$ є суттєво меншою за одиницю. Це дає можливість з високою точністю реконструювати сигнал, зберігаючи тільки значення та місця розташування найбільших коефіцієнтів сигналу.

Розглянемо дискретний сигнал, представлений вектором-стовпцем $x \in \mathbb{R}^N$ розміру $N \times 1$, що може бути виражений в деякому базисі простору $\mathbb{R}^N$, утвореному векторами $\{\psi_i\}_{i=1}^N$, кожен з яких має розмір $N \times 1$ елементів. Для спрощення розрахунків припустимо, що базис є ортонормованим. Використовуючи $N \times N$ базисну матрицю $\Psi = (\psi_1, \psi_2, \dots, \psi_N)$ зі стовпцями, утвореними цими векторами, сигнал x може бути виражений як $x = \sum_{i=1}^N c_i \psi_i$ або в матричній формі

$$x = \Psi c \quad (1)$$

де $c = N \times 1$ вектор-стовпець вагових коефіцієнтів $c_i = \langle c, \psi_i \rangle = \psi_i^T c$, "T" – операція транспонування, $\langle \rangle$ – скалярний добуток векторів, x та c – еквівалентні представлення сигналу.

Сигнал x називається s -розрідженим, якщо тільки s компонент c_i в (1) відмінні від нуля, а решта $(N - s)$ дорівнюють нулю. Такі сигнали можуть бути з високою точністю апроксимовані з використанням лише s базисних векторів.

Розглянемо процес вимірювання, в результаті якого обчислюються $M < N$ скалярних добутків векторів x та $\{\varphi_j\}_{j=1}^M$, як $y_j = \langle x, \varphi_j \rangle$. Якщо значення y_j представити у вигляді $M \times 1$ вектора-стовпця, а φ_j^T записати в якості рядків $M \times N$ матриці Φ , тоді в матричному вигляді:

$$y = \Phi x + n = \Phi \Psi c + n = \Theta c + n \quad (2)$$

де $\Theta = \Phi \Psi$ – матриця вимірів розміру $M \times N$, Φ – фіксована матриця змішування векторів (не залежить від x), n – шум. Оскільки $n \ll \Theta c$, в подальшому його враховувати не будемо. Тоді отримаємо:

$$y \cong \Phi x = \Phi \Psi c = \Theta c \quad (3)$$

Для вирішення задачі реконструкції ЗК необхідно відновити вектор c за вектором y . Так як $M < N$, система рівнянь (3) є недовизначеною, а, отже, має безліч рішень. Внаслідок цього однозначно відновити вектор c без додаткової інформації неможливо. Однак, якщо врахувати, що сигнал c є розрідженим в деякому базисі, то за певних умов його реконструкція стає можливою. Тобто необхідно вирішити завдання:

- 1) провести пошук універсальної матриці вимірів Φ , що дасть можливість отримати s -

розріджений сигнал без суттєвих втрат в точності його реконструкції;

- 2) розробити алгоритм відновлення сигналу x в розрідженому базисі Θ за кількістю вимірів, що приблизно дорівнює числу ненульових коефіцієнтів.

В роботі [6] доведено, що завданню (1) задовольняє випадкова матриця вимірів Φ розміру $M \times N$ з незалежними і однаково розподіленими (н.о.р.) елементами $\varphi_{i,j}$ з нормальною густиною розподілу з нульовим середнім значенням та дисперсією $1/s$, яка має дві корисних властивості:

- 1) якщо $0 < \delta < 1$ та $M \geq C_1 s \log(N/s)$, то матриця Φ задовольняє $RIP(\delta, M)$ (Restricted Isometry Property) з ймовірністю $\geq 1 - 2e^{-C_2 M}$ де $1, 2 > 0$ – малі константи, що залежать тільки від δ (а це означає, що s -розріджені та стискувані сигнали довжини N можуть бути з високою ймовірністю відновлені тільки за $M \ll N$ випадковими вимірами);
- 2) матриця Φ універсальна в тому сенсі, що істотна інформація про будь-який s -розріджений (або стискуваний) сигнал не буде пошкоджена при скороченні розмірності від $x \in \mathbb{R}^N$ до $y \in \mathbb{R}^M$, а також матриця $\Theta = \Phi \Psi$ буде випадковою матрицею з нормально розподіленими н.о.р. елементами. Таким чином, незалежно від вибору ортонормованого базису Ψ матриця Θ з високою ймовірністю буде мати властивість $RIP(\delta, M)$.

В задачах реконструкції можна використовувати й інші випадкові матриці вимірів [7]:

- випадкова вибірка н.о.р. елементів $\varphi_{i,j}$ за симетричним розподілом Бернуллі $P(\varphi_{i,j} = \pm 1/\sqrt{M} = 1/2)$;
- випадкова вибірка н.о.р. елементів $\varphi_{i,j}$, коли $\varphi_{i,j} \in \{0, \pm \sqrt{3/M}\}$ з однаковою ймовірністю $1/3$;
- рівномірна випадкова вибірка N стовпців на одиничній сфері в $\mathbb{R}^M$;
- випадкова вибірка проектору та його нормалізація $\Phi = \sqrt{(N/M)P}$.

Алгоритми відновлення сигналів можна класифікувати таким чином [6, 7]:

- 1) Алгоритми ℓ_p -мінімізації: вібудується пошук діапазону сигналу, який найближче до спостережуваного сигналу в ℓ_p -нормі. Мінімізація ℓ_p забезпечує точне відновлення розрідженого сигналу.
- 2) Ітеративні алгоритми покладаються на ітеративну апроксимацію коефіцієнтів сигналу. Для апроксимації ℓ_0 -норми розглядаються зважені ℓ_p -норми при $\left(\sum_i \omega_i (c_j)^p\right)^{1/p}$, рівному одиниці або двом.
- 3) "Жадібні" алгоритми засновані на виборі найбільш «значущих» (за амплітудою) коефіцієнтів розкладу сигналу в обраному базисі функцій. Критерієм зупинки роботи алгоритму є забезпечення заданої точності реконструкції сигналу з використанням фіксованого порогу.

- 4) Комбінаторні алгоритми засновані на припущенні, що є n загальних елементів і k аномальних елементів, які необхідно знайти. Мета алгоритму — створити колекцію тестів, які дозволять ідентифікувати аномальні елементи, а також мінімізувати кількість виконаних тестів.

В роботі було використано відомий «жадібний» алгоритм OMP (Orthogonal Matching Pursuit) [6], який може відновити сигнал з m ненульових компонент при загальній кількості d компонент та дає $O(mlnd)$ випадкових лінійних відліків цього сигналу. Головні переваги OMP — це його простота виконання та швидкість [6]. Ідея алгоритму полягає у виборі стовпців матриці вимірів "жадібним" чином. На кожній ітерації вибирається стовпчик, що найбільш сильно корелює з частиною сигналу, яка залишилася. Потім віднімається його внесок у вектор відновлюваного сигналу і те саме повторюється на залишку. Таким чином, після m ітерацій алгоритм визначить правильний набір стовпчиків.

3. Отримані результати

Дослідження проводилося з використанням стандартного пакету ЦЗ MIRFlickr-1M, на основі якого було сформовано тестовий пакет зі 100 напівтонових зображень, масштабованих до однакового розміру 640x480 пікселів. Вбудовування стегоданих виконувалося адаптивним алгоритмом HUGO [8]. Ступінь заповнення ЗК стегоданими був рівний: 10%, 20%, 50%. В роботі були використані стандартні МЯ ЦЗ [9]:

- 1) Mean Square Error (MSE) — показує середньоквадратичну відмінність між пікселями контейнеру і стегограми;
- 2) Normalized Cross-Correlation (NCC, нормована взаємна кореляція) — показує ступінь кореляції пікселів контейнера і стегограми;
- 3) Structural Similarity (SSIM, структура подібність) — є мірою подібності зображень.

За результатами роботи OMP та медіанного фільтра (розміри ковзного вікна (KB): 3x3, 5x5, 7x7) були побудовані графіки залежності значень МЯ ЦЗ від ступеня заповнення ЗК стегоданими (рис. 1(а-в)).

Для МФ з параметрами KB 3x3 значення MSE є найменшим, а найбільшим — для OMP. Значення NCC та SSIM наближаються до одиниці для всіх випадків, що свідчить про високу якість відновлення та знешумлення, відмінність для OMP та МФ є порівняно несуттєвою. Слід звернути увагу на незалежність отриманих результатів від ступеня заповнення ЗК стегоданими.

Висновки

У роботі досліджено ефективність застосування «жадібного» алгоритму OMP для реконструкції ЗК та МФ для дедекції стегоданих в ЦЗ. За результатами аналізу отриманих даних:

- виявлено більш високу якість роботи МФ, в порівнянні з OMP, проте різниця не є суттєвою;

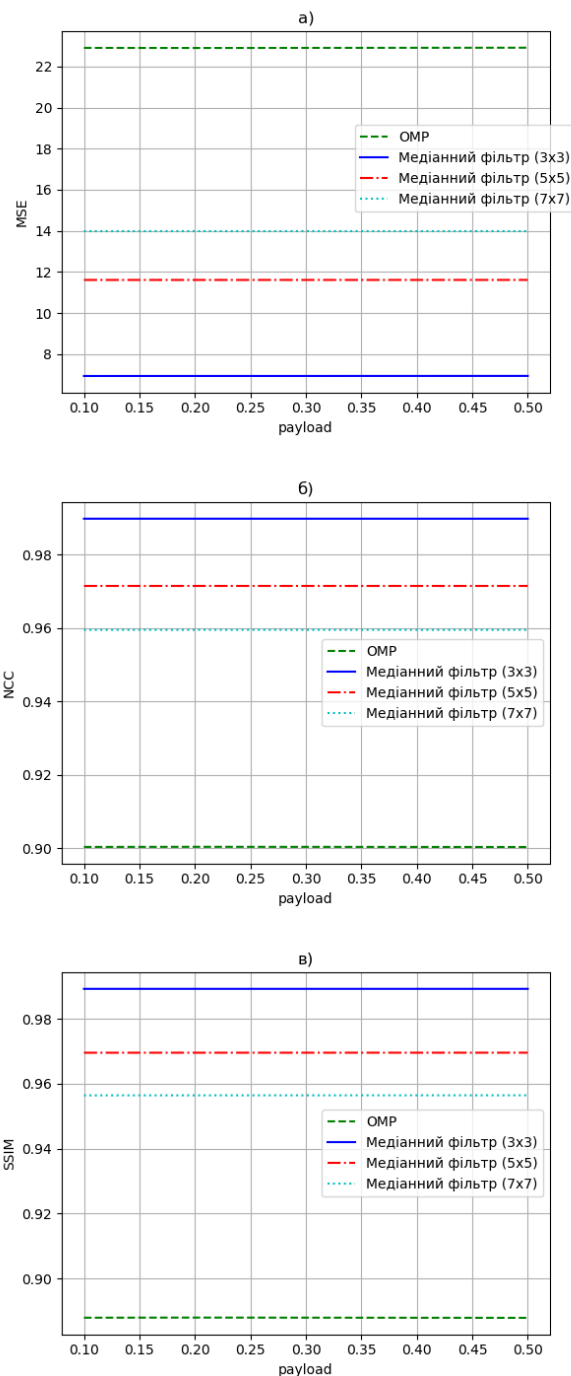


Рис. 1. Залежність значень МЯ ЦЗ від ступеня заповнення ЗК стегоданими: а) MSE, б) NCC, в) SSIM

- встановлено незалежність значень МЯ ЦЗ від ступеня заповнення ЗК стегоданими;
- становить інтерес подальше дослідження роботи OMP, в порівнянні з іншими алгоритмами стегоаналізу, а також іншими методами вбудовування стегоданих.

Перелік використаних джерел

1. J. Fridrich. Steganography in Digital Media: Principles, Algorithms and Applications. — New York, USA : Cambridge University Press, 2010. — P. 437.
2. Терещенко Є. М., Богайчук В. О., Прогонов Д. О. Виявлення стегограм, сформованих адаптив-

- ним методом SI-UNIWARD, при використанні універсальних стегодетекторів. — Львів : Видавництво Львівської політехніки, 2017.
3. Терещенко Є. М., Богайчук В. О., Прогонов Д. О. Ефективність універсальних стегодетекторів у випадку використання адаптивних методів формування стеганограм. — Черкаси : Черкаський державний технологічний університет, 2017.
 4. Черпахова К. В., Куш С. М., Прогонов Д. О. Медіанна, адаптивно-медіанна та двомірна вінеровська фільтрація стеганограм. — Київ : ВПІ ВПК «ПОЛІТЕХНІКА», 2015.
 5. Гонсалес Р., Вудс Р. Цифровая обработка изображений. — Москва : Техносфера», 2005. — С. 1072.
 6. An Introduction to Compressive Sensing / M. Davenport, R. Baraniuk, M. Duarte, C. Hegde. — New York, USA : Cambridge University Press, 2014. — P. 118.
 7. Candes E., Wakin M. An Introduction To Compressive Sampling. — IEEE Signal Processing Magazine, 2008. — P. 21–30.
 8. Filler T., Fridrich J. Gibbs Construction in Steganography. — IEEE Transactions on Information Forensics and Security, 2010. — P. 705–720.
 9. Голубничий В. О., Куш С. М., Прогонов Д. О. Демаскуючі ознаки вбудованих стегоданих. — Київ : ВПІ ВПК «ПОЛІТЕХНІКА», 2015.