

ТЕОРЕТИКО-ІНФОРМАЦІЙНІ ОЦІНКИ СПОТВОРЕНЬ
КОНТЕЙНЕРІВ ПРИ ФОРМУВАННІ СТЕГАНОГРАМ

Проконов Д. О., к.т.н.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна

Особлива увага при розробці систем захисту критичної інформаційної інфраструктури приділяється створенню високоточних методів раннього виявлення несанкціонованої передачі конфіденційних даних, зокрема з використанням адаптивних стеганографічних методів (АСМ) [1, 2]. Тому актуальною та важливою задачею є створення методів, що дозволять з високою точністю виявляти стеганограми навіть у випадку відсутності або обмеженості апріорних даних щодо використовуваних АСМ.

Поширеним підходом до виявлення стеганограм є застосування методу калібрування файлу-контейнера, наприклад цифрового зображення [3] — оцінки статистичних характеристик вихідного (незаповненого) зображення-контейнеру (ЗК). Для оцінки «віддаленості» розподілів значень елементів зображення-контейнеру P_C та стеганограми P_S використовуються теоретико-інформаційні показники, зокрема відстань (дивергенція) Кульбака-Лейблера D_{KL} [1]:

$$D_{KL}(P_C, P_S) = \sum_{q \in Q} P_C(q) \cdot \log_2(P_C(q)/P_S(q)), \quad (1)$$

де Q – діапазон значення яскравості q пікселів зображення. Проте застосування D_{KL} для виявлення спотворень ЗК, обумовлених використанням сучасних АСМ, зокрема алгоритмів HUGO, WOW, має суттєві обмеження, внаслідок мінімізації відмінностей між розподілами значень P_C та P_S . Тому метою роботи є пошук теоретико-інформаційні методів, що дозволять підвищити точність виявлення слабких відмінностей в розподілі значень елементів незаповненого ЗК та стеганограм, сформованих згідно АСМ.

Для підсилення відмінностей між P_C та P_S в роботі пропонується використовувати спеціалізовані оцінки відстаней між імовірнісними розподілами, зокрема відстані Бхаттачарая D_B та Хеллінгера D_H , χ^2 -відстань D_{χ^2} [4], а також спектр відстаней Реньї D_R [5]:

$$D_H(P_C, P_S) = \sqrt{\sum_{q \in Q} (\sqrt{P_C(q)} - \sqrt{P_S(q)})^2} / \sqrt{2}, \quad (2)$$

$$D_B(P_C, P_S) = -\ln(1 - D_H^2(P_C, P_S)), \quad (3)$$

$$D_{\chi^2}(P_C, P_S) = \sum_{q \in Q} (P_C(q) - P_S(q))^2 / P_S(q), \quad (4)$$

$$D_R^\alpha(P_C, P_S) = \log_2 \left(\sum_{q \in Q} P_C^\alpha(q) \cdot P_S^{1-\alpha}(q) \right) / (\alpha - 1), \alpha \in (0; +\infty) \setminus \{1\}. \quad (5)$$

Дослідження ефективності застосування запропонованих показників проводилося з використанням вибірки 10,000 зображень зі стандартного тестового пакету MIRFlickr-25k [6]. Тестові зображення-контейнери були ма-

сштабовані до однакового розміру 640·480 (пікселів) та представлені в градаціях сірого кольору. Розглянуто випадок формування стеганограм згідно адаптивних методів HUGO [7] та WOW [8].

Відстані Кульбака-Лейблера (1), Хеллінгера (2) та Бхаттачарая (3) між розподілами значень яскравості пікселів незаповненого ЗК та стеганограм наведені на рис. 1.

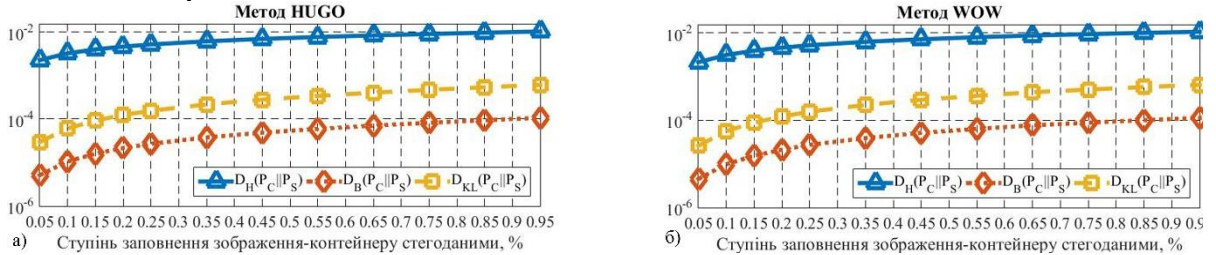


Рисунок 1. Відстані Кульбака-Лейблера, Хеллінгера та Бхаттачарая між розподілами P_C та P_S при використанні стеганографічних методів (а) HUGO та (б) WOW

Надзвичайно малі значення показників D_{KL} , D_H та D_B (10^{-2} - 10^{-6} , рис. 1), суттєво обмежує їх використання в задачах виявлення стеганограм. Зважаючи на отримані результати, становить інтерес дослідження «зворотної» відстані $D(P_S, P_C)$ між розподілами P_S та P_C . Відносні відстані Кульбака-Лейблера (1) та χ^2 -відстань (4) між розподілами P_C та P_C наведені на рис.2.

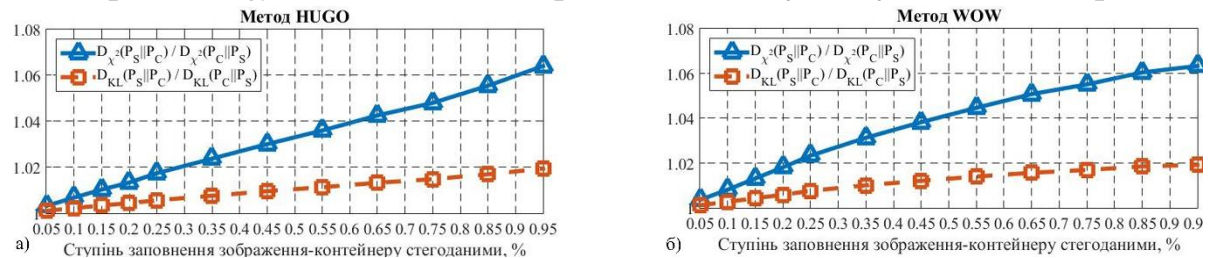


Рисунок 2. Відносні відстань Кульбака-Лейблера та χ^2 -відстань між розподілами P_C та P_S при використанні стеганографічних методів (а) HUGO та (б) WOW

Близькість до одиниці відносних значень D_{KL} та D_{χ^2} між розподілами P_C та P_S свідчить про несуттєві відмінності даними розподілами. Для підсилення виявлених слабких відмінностей також були розраховані загальна $D_R^\Sigma = \sum_{\alpha} D_R^\alpha$ та гранична $D_R^{+\infty}$ відстані Реньї (5) між розподілами значень яскравості пікселів ЗК та стеганограм (рис. 3).

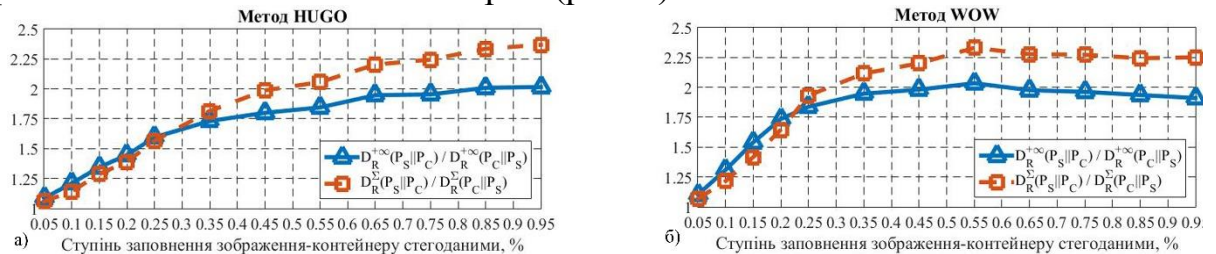


Рисунок 3. Загальна D_R^Σ та гранична $D_R^{+\infty}$ відстані Реньї між розподілами P_C та P_S при використанні стеганографічних методів (а) HUGO та (б) WOW

Виявлено відмінність з значеннях відстані Реньї між розподілами значень яскравості пікселів ЗК та стеганограми при розрахунку даної відстані відносно контейнеру ($D_R^\alpha(P_C, P_S)$) або стеганограми ($D_R^\alpha(P_S, P_C)$), що може

бути використана для підвищення точності стегоаналізу.

За результатами проведеного дослідження показано вагомі обмеження використання в задачах стегоаналізу мультимедійних даних поширених оцінок відстаней між розподілами значень елементів контейнеру та стеганограми, зокрема відстані Кульбака-Лейблера, Хеллінгера, Бхаттачарайя та χ^2 -відстані. Для подолання виявлених обмежень запропоновано використовувати спектр відстаней Реньї, що дало можливість підсилити слабкі відмінності між розподілами значень елементів контейнеру та стеганограми.

Перелік посилань

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / Fridrich J. – 1st Edition. – New York: Cambridge University Press, 2009 – p. 437.
2. Progonov D. Multiclass detector for modern steganographic methods / Progonov D. // International Journal “Information Theories and Applications”. – Vol. 24, No. 3. – 2017. – pp. 55-71.
3. Kodovsky J., Fridrich J. Calibration revisited / Kodovsky J., Fridrich J. Proceeding of the 11th ACM workshop on multimedia and security. – Princeton, 2009. p. 63-74.
4. Bishop C. Pattern Recognition and Machine Learning / Bishop C. – 1st Edition. – New York: Springer-Verlag, 2006 – p. 738.
5. Renyi A. On measures of information and entropy / Renyi A. // Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability 1960. pp. 547-561.
6. Huiskes M. J., Lew M. S. The MIR Flickr Retrieval Evaluation / Huiskes M. J., Lew M. S. // ACM International Conference on Multimedia Information Retrieval (MIR'08).
7. Filler T., Fridrich J. Gibbs Construction in Steganography / Filler T., Fridrich J. // IEEE Transactions on Information Forensics and Security. – Vol. 5, Issue 4, 2010.
8. Holub V., Fridrich J. Designing steganographic distortion using directional filters / Holub V., Fridrich J. // IEEE International Workshop on Information Forensics and Security. – 2012.

Анотація

Показано вагомі обмеження використання поширених теоретико-інформаційних оцінок відстаней між розподілами значень елементів зображень-контейнерів та стеганограм, зокрема відстані Кульбака-Лейблера. Для підсилення слабких відмінностей між даними розподілами запропоновано використовувати спеціалізовані відстані Хеллінгера, Бхаттачарайя, χ^2 -відстані та спектр відстаней Реньї.

Ключові слова: стегоаналіз, цифрові зображення, спектр відстаней Реньї.

Аннотация

Показано существенные ограничения использования распространенных теоретико-информационных оценок для определения расстояний между распределениями значений элементов изображений-контейнера и стеганограмм, в частности расстояния Кульбака-Лейблера. Для усиления слабых различий между данными распределениями предложено использовать специализированные расстояния Хеллингера, Бхаттачарайя, χ^2 -расстояния та спектра расстояний Реньи.

Ключевые слова: стегоанализ, цифровые изображения, спектр расстояний Реньи.

Abstract

It is shown significant limitation of usage the widespread information-theoretical estimations of distance between cover and stego file's elements distributions, such as Kullback-Leibler divergence. For enhancement the weak differences between these distributions it is proposed to use specialized measurements – Hellinger divergence, Bhattacharayya divergence, χ^2 -divergence and Renyi divergence.

Keywords: steganalysis, digital images, Renyi divergence.