УДК 004.056.5

В. І. Чистов, К.С. Васюта

ДОСЛІДЖЕННЯ МЕТОДІВ ПАСИВНОГО СТЕГОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Анотація

Проведено огляд основних методів виявлення стеганограм з даними, вбудованими у цифрові зображення. Визначено їх область застосування, основні переваги та недоліки в процесі виявлення стеганограм при обробці, зберіганні та передачі цифрових зображень в інформаційно-телекомунікаційних системах (ІТКС).

Ключові слова: стеганографічні системи зв'язку, стегоаналіз, інформаційно-телекомунікаційні системи, найменш значущий біт.

Abstract

The main methods of detecting steganograms with data embedded in digital images are reviewed. Their scope of application, main advantages and disadvantages in the process of detecting steganograms during processing, storage and transmission of digital images in information and telecommunication systems (ITCS) are defined.

Keywords: steganographic communication systems, stegoanalysis, information and telecommunication systems, least significant bit.

На фоні Російської збройної агресії проти України все більшого розповсюдження набуває практика використання державою-терористом методів впливу на критичну інфраструктуру нашої держави для досягення переваги у економічній, політичній та військовій сферах. Для проведення атак в тому числі застосовуються стеганографічні системи зв'язку (ССЗ) , що засновані на вбудовуванні каналів передачі даних в існуючі інформаційні потоки в інформаційно-телекомунікаційних системах (ІТКС).

Найбільш розповсюдженим типом мультимедійних даних, які використовуються у ССЗ в якості файлів-контейнерів, є цифрові зображення. Для протидії функціонуванню таких ССЗ при обробці трафіку, що передається у ІТКС, використовуються методи пасивного та активного стегоаналізу.

Перші методи приховування повідомлень в просторовій області зображення-контейнеру (ЗК) були засновані на заміні значень найменш значущого біту (НЗБ) (анлійською LSB – Least Significant Bits) яскравості пікселів зображення-контейнеру $I_{x,y}$ розмірами M x N пікселів, на біти стегоданих [4]:

$$S_{x_i y_i}[n] = d_i, i \in [1; L_M], n \in [1; C_1],$$
$$S_{x_i y_i} = \sum_{k=1}^{C_1} S_{x_i y_i}[k] \times 2^{C_1 - k}, \quad (1)$$

де d_i – i-тий біт приховуваного повідомлення D довжиною L_D (біт); C_1 – розрядність бітового представлення яскравості пікселів ЗК; $S_{x_i y_i}[n]$ – значення n –го біту двійкового представлення яскравості i-го пікселю ЗК, використаного при вбудовуванні стегоданих; $S_{x_i y_i}$ – десяткове представлення яскравості i-го пікселя сформованої стеганограми.

Вестфельдом (Westfeld) та Пфіцманом (Pfitzman) був запропонований перший ефективний метод виявлення факту використання LSB-методів - Pairs- of-Value (PoV) аналіз [3]. Метод заснований на аналізі виду гістограм розподілу значень яскравості пікселів зображень, що містили стегодані. Суттєвим обмеженням практичного застосування PoV-аналізу є те, що виявлення з високою імовірністю стеганограм можливо лише у випадку сильного заповнення ЗК стегоданими (більше 50%). Для підвищення імовірності виявлення стеганограм у випадку слабкого заповнення ЗК стегоданими (менше 10%) було запропоновано використовувати χ^2 —тест [2] та RS-аналіз [4].

Метод χ^2 є універсальним, оскільки підходить для аналізу зображень, створених різними програмами приховування. Проте результати роботи χ^2 —тесту значною мірою залежить від способу приховування даних. При послідовному записі в НЗБ елементів контейнера метод забезпечує хороші результати, а при псевдовипадковому виборі молодших біт та розсіювання повідомлення по всій довжині контейнера метод не спрацьовує.

При RS-аналізі відмінностей у НЗБ-площини і зсунутої НЗБ-площини стего-образу дозволяє надійно виявляти повідомлення розміром від 1 % і більше від загальної кількості пікселів (1 біт на відлік). Крім того, для RS-аналізу можна побудувати швидкий алгоритм. Проте для дуже зашумлених і дрібнотекстурованих зображень різниця між кількістю регулярних і сингулярних груп контейнера мала. Відповідно, лінії в RS-діаграмі перетнуться під малим кутом і точність зменшиться.

Виявлення стеганограм з даними, вбудованими у цифрові зображення є досить складним процесом. Таким чином, на сьогодні актуальною задачею є удосконалення існуючих і створення нових методів стегоаналізу, а також розробка на їх основі програмного комплексу, за допомогою якого підвищиться ймовірність виявлення повідомлень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Прогонов Д.О,, “ Структурні методи пасивного стегоаналізу цифрових зображень”,дис. канд. техн. наук: 05.13.21. Київ, 2016.

2. Швидченко І.В. Методи стеганоанализу для графічних файлів / Швидченко І.В. // Штучний інтелект. – 2010. –№4. – с. 697-705;

3. Westfeld A. F5 – A steganographicalgorithm: HighcapacitydespitebetterSteganalysis / WestfeldAndreas. – Proceedingsof 4th InternationalWorkshoponInformationHiding, LectureNotesinComputerScience. – Ed. Moskowitz I.S. – Pittsburgh, USA, 2001. – pp. 289-302;

4. Fridrich J. Detecting LSB steganographyincolor, andgray-scaleimages / 164 Fridrich J., Goljan M., RuiDu // IEEE MultimediaMagaz., SpecialIssueonSecurity. – 2001. – Vol. 8, Iss. 4. – pp. 22-28. – DOI 10.1109/93.959097;

Чистов Валерій Ігорович **—** ад’юнкт, Харківський національний університет Повітряних Сил, Харків, e-mail: valera.chistov43@gmail.com

Васюта Костянтин Станіславович **—** доктор технічних наук, професор, заступник начальника університету з наукової роботи, Харківський національний університет Повітряних Сил, Харків

ChystovValerii I. **—** adjunct, IvanKozhedubKharkivNationalUniversityoftheAirForce, Kharkivemail : valera.chistov43@gmail.com

VasiutaKonstantyn S .— Doctor of Engineering Science, Professor, Deputy Head of the University for scientific, Ivan Kozhedub Kharkiv National University of the Air Force, Kharkiv