

УДК 004.056.5

В. Я. Чечельницький, д-р техн. наук,
М. В. Калашніков, **О. О. Яковенко**,
Н. І. Кушніренко

УРАХУВАННЯ СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ КОНТЕЙНЕРУ ДЛЯ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

***Анотація.** Було досліджено зміну статистичних показників зображення як контейнера при приховуванні інформації з урахуванням цих показників та без їх урахування. Застосування отриманих даних дозволить покращити роботу алгоритму з урахуванням статистичних даних контейнера, зменшити ймовірність виявлення прихованого повідомлення за допомогою статистичного стегааналіза.*

***Ключові слова:** цифрова стеганографія, приховування інформації, частотна область, дискретно-косинусне перетворення, статистичні показники*

V. Ja. Chechel'nickij, ScD.,
N. V. Kalashnikov, **A. A. Jakovenko**,
N. I. Kushnirenko

CONTAINER'S STATISTIC FEATURES CONSIDERING FOR STEGANOGRAPHIC ALGORITHM

***Abstract.** Some image statistics changes for embedding information with container image statistics accounting and without were checked. As a container considered static digital images in JPEG file format, data hiding in least significant bits of container discrete cosine transform coefficients provided. Container distortion parameters were measured and chi-square test was conducted for embedding information with container image statistics accounting and without. Also values distribution for container discrete cosine transform coefficients was checked. Obtained data allow improving algorithm with image statistic features considering. Decreasing image distortions and statistics changes will reduce probability of hidden message detection with histogram-based and statistical steganalysis.*

***Keywords:** digital steganography, data hiding, frequency domain, discrete-cosine transform, statistic features*

В. Я. Чечельницький, д-р техн. наук,
Н. В. Калашніков, **А. А. Яковенко**,
Н. І. Кушніренко

УЧЕТ СТАТИСТИЧЕСКИХ ОСОБЕННОСТЕЙ КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА

***Аннотация.** Было исследовано изменение статистических показателей изображения в качестве контейнера при сокрытии информации с учетом этих показателей и без их учета. Использование полученных данных позволит улучшить работу алгоритма сокрытия информации с учетом статистических данных изображения и уменьшит вероятность выявления скрытого сообщения при помощи статистического стегаанализа.*

***Ключевые слова:** цифровая стеганография, сокрытие информации, частотная область, дискретно-косинусное преобразование, статистические показатели*

Вступ. Стеганографія вирішує задачі приховування факту існування таємних даних при їх передачі, зберіганні або обробці. Повідомлення, яке приховується, вбудовується у певний об'єкт, що не привертає уваги. Такий об'єкт називається контейнером та може вільно передаватися адресату [1]. Значна кількість стеганографічних алгоритмів (СА) використовує у якості контейнера цифрові зображення у форматі JPEG, а також

інших форматах із використанням дискретного косинусного перетворення (ДКП). Такі СА можуть використовувати різницю коефіцієнтів ДКП для кодування бітів стеганографічного повідомлення (СП), наприклад алгоритми Коха-Жао та Хсу і Ву [1], так і модифікацію найменших значущих бітів (НЗБ) коефіцієнтів ДКП, наприклад, програма Jpeg-Jsteg. У роботі [2] було запропоновано новий СА, який змінює значення НЗБ коефіцієнтів ДКП та використовує модифікацію таблиці квантизації JPEG. Для програми Jpeg-Jsteg модифіковано СА з метою зменшення помітності вбудовування повідомлен-

© Чечельницький В.Я., Калашніков М.В., Яковенко О.О., Кушніренко Н.І., 2016

ня шляхом перестановки значень коефіцієнтів ДКП у блоці [3]. У роботі [4] розглянуто методи покращення стійкості для існуючих СА з використанням ДКП.

Існуючі методи стеганографічного аналізу дозволяють виявити наявність прихованого повідомлення у зображенні, у тому числі у НЗБ коефіцієнтів ДКП за статистичними показниками контейнера [5–7]. Таким чином, залишається актуальним пошук нових СА, які забезпечують максимальну подібність порожнього та заповненого контейнерів при приховуванні інформації. Для реалізації подібних алгоритмів є необхідним урахування статистичних показників вихідного зображення, а також їх змін при вбудовуванні СП [8 – 9].

Мета роботи. Метою даної роботи є дослідження зміни статистичних показників контейнера для двох СА – з урахуванням цих показників та без їх урахування, при цьому було вирішено наступні задачі:

1. Здійснено приховування інформації у НЗБ коефіцієнтів двовимірного по-блокового ДКП зображення.
2. Розглянуто методіку оцінювання статистичних показників зображення-контейнеру.
3. Досліджено зміну статистичних показників зображення-контейнеру при приховуванні інформації.

Основна частина. Узагальнений алгоритм вбудовування інформації у НЗБ частини коефіцієнтів ДКП контейнера з урахуванням їх статистичних показників, який розглядається у даній статті, запропоновано у роботі [10].

Стеганографічне повідомлення у вигляді бітової послідовності може кодуватися асиметричним кодом, наприклад на основі досконалих двійкових решіток [11], для отримання розподілу значень бітів повідомлення максимально наближеного до розподілу НЗБ коефіцієнтів ДКП контейнера.

Для вбудовування інформації без урахування статистичних показників використовуємо СА програми Jpeg-Jsteg [3].

Реалізація розглянутих алгоритмів, та визначення статистичних показників здійснювалось у середовищі математичних обчислень Matlab. Було порівняно зміну статис-

тичних показників контейнера для обох алгоритмів, що досліджуються. У якості контейнера використано зображення у відтінках сірого розміром 256×256. Вбудовувалось таємне повідомлення: «Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.». У якості матриці квантування використано стандартну таблицю JG [12], показник якості зображення $Q = 85$. Зображення-контейнер наведено на рисунку 1.



Рис. 1. Зображення-контейнер

Результати визначення розподілу коефіцієнтів ДКП за їх значеннями для порожнього контейнера та при вбудовуванні розглянутими СА наведено на рисунках 2; 3 та 4.

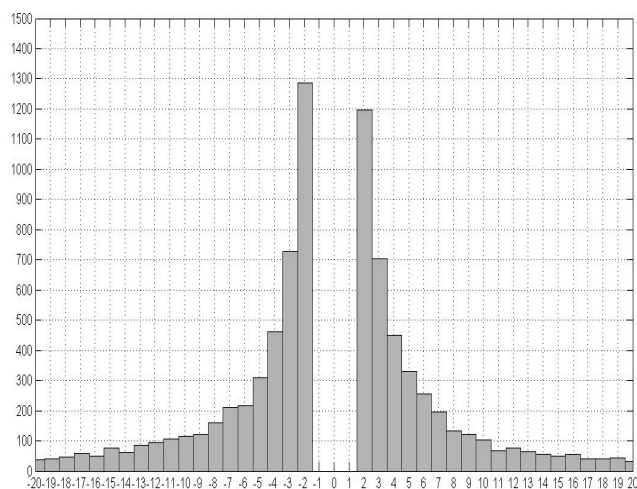


Рис. 2. Розподіл значень коефіцієнтів ДКП для порожнього контейнера

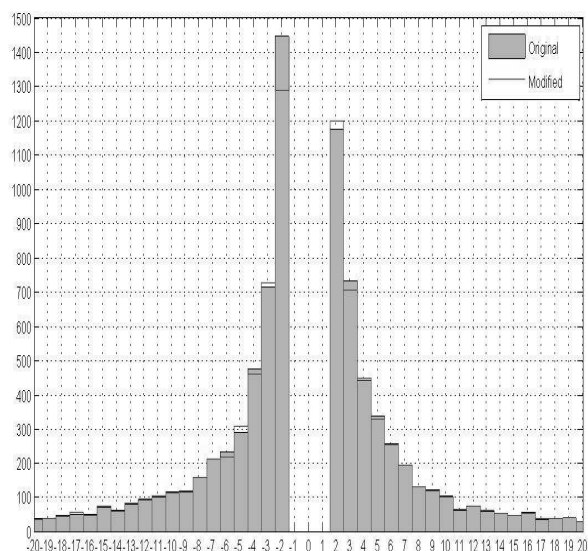


Рис. 3. Порівняння розподілу значень коефіцієнтів ДКП для алгоритму Jpeg-Jsteg

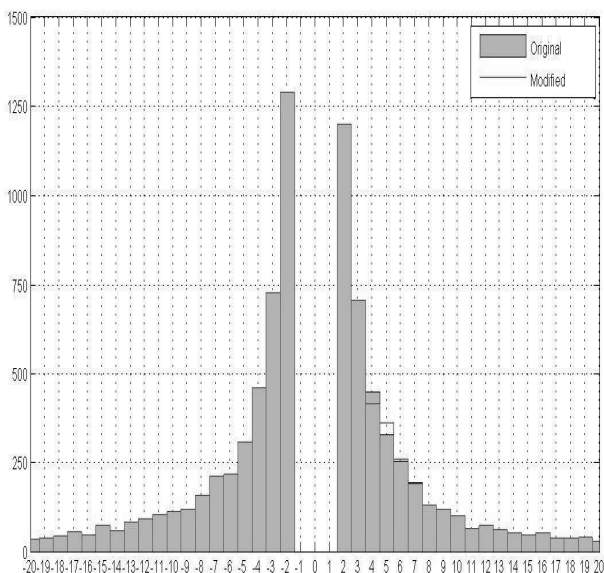


Рис. 4. Порівняння розподілу значень коефіцієнтів ДКП для запропонованого алгоритму

З рис. 3 видно, що при використанні СА Jpeg-Jsteg розподіл значень коефіцієнтів ДКП помітно змінюється. Використання запропонованого алгоритму викликає меншу зміну значень коефіцієнтів ДКП, як показано на рис. 4.

Також для обох СА були визначені середньоквадратичне відхилення для порожнього і заповненого контейнерів (MSE), пікове співвідношення сигналу до шуму (PSNR) та проведено тест χ^2 (хі-квадрат). Результати тестів наведено у таблиці.

Показники викривлення зображення

Показник	Вбудовування без урахування статистики	Вбудовування з урахуванням статистики
MSE	0,349	0,199
PSNR	52,707	55,135
Тест χ^2	0,050	0,021

Висновки. У даній роботі було розглянуто зміну статистичних показників зображення-контейнера при приховуванні СП. При вбудовуванні інформації запропонованим СА зміни цих показників дещо менші, ніж при використанні алгоритму Jpeg-Jsteg, але необхідне подальше покращення алгоритму з метою забезпечення максимальної подібності порожнього та заповненого контейнерів. Оскільки розподіл значень бітів у повідомленні повинен бути нерівномірним, для кодування стеганографічного повідомлення бажано використовувати асиметричні коди. Також залишається актуальною оцінка імовірності виявлення прихованого повідомлення, у тому числі з використанням тесту χ^2 , для запропонованого СА.

Список використаної літератури

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко; ред. Ю. А. Шпак. – К. : «МК-Пресс», 2006. – 288 с., іл.
2. Chin-Chen Chang, Tung-Shou Chen, and Lou-Zo Chung, (2002), A Steganographic Method Based upon JPEG and Quantization Table [Text], *Information Sciences*, No. 141, pp. 123 – 138.
3. Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, (2012), Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm [Text], *International Journal of Computer and Electrical Engineering*, Vol. 4, No. 4, pp. 458 – 462.
4. Прохожев Н. Н. Повышение устойчивости стеганоалгоритмов частотной области на основе дискретно-косинусного преобразования к внешним воздействиям [Текст] / Н. Н. Прохожев, О. В. Михайличенко, А. Г. Коробейников // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий,

механики и оптики. – 2009. – № 2(60). – С. 102 – 106.

5. Siwei Lyu, (2005), Natural Image Statistics for Digital Image Forensics [Text]: A Thesis Submitted to the Faculty in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science, *Siwei Lyu*, Hanover, USA, 102 p.

6. Quan Weiwei, Guo Yanqing, and Kong Xiangwei, (2006), JPEG Quantization-Distribution Steganalytic Method Attacking Jsteg [Text], *IJCSNS International Journal of Computer Science and Network Security*, 2006, Vol. 6, No. 7B, pp. 192 – 195.

7. Xiaoyi Yu, Yunhong Wang, and Tieniu Tan, (2004), On Estimation of Secret Message Length in JSteg-like Steganography [Text], *In: Proceedings of the 17th International Conference on Pattern Recognition*, pp. 673 – 676.

8. Aapo Hyvärinen, Jarmo Hurri, and Patrik O. Hoyer, (2009), Natural Image Statistics [Text], *Aapo Hyvärinen*, Springer, 467 p.

9. Zontak M., and Irani M. Internal, (2011), Statistics of a Single Natural Image [Text], *In: Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition*, pp. 977 – 984.

10. Калашніков М. Розробка стеганографічного алгоритму із урахуванням статистики зображення-контейнера [Текст] / М. Калашніков, О. Яковенко, Н. Кушніренко, В. Чечельницький // Матеріали IV-ї міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів : 4-5 червня 2015. – С. 129 – 131.

11. Кушніренко Н. І. Метод криптографічної передачі інформації на базі еквівалентного класу досконалих двійкових решіток [Текст] / Н. І. Кушніренко, В. Я. Чечельницький // Інформатика та математичні методи в моделюванні. – Одеса : – 2014. – № 3. – С. 210 – 218.

12. Independent JPEG Group [Electronic Resource], Independent JPEG Group, (In English), Mode of access: www. Url: <http://www.ijg.org>. (accessed 27.05.2016). – Title from the screen.

References

1. Konahovich G.F., and Puzyrenko A. Ju., *Komp'yuternaja ste-ganografija. Teoriya i praktika* [Computer Steganography. Theory and Practice], (2006), Kiev, Ukraine, “MK-Press”, 288 p. (In Russian).

2. Chin-Chen Chang, Tung-Shou Chen, and Lou-Zo Chung, (2002), A steganographic Method based upon JPEG and Quantization table, *Information Sciences*, Vol.141 pp. 123 –138 (in English).

3. Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, 2012, Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm *International Journal of Computer and Electrical Engineering*, Vol. 4, No. 4, pp. 458 – 462 (In English).

4. Prokhozhev N.N., Mikhailichenko O. V., Korobeinikov A.G. Povyshenie ustoichivosti steganoalgoritmov chastotnoi oblasti na osnove diskretno-kosinusnogo preobrazovaniya k vneshnim vozdeistviyam [Improving Robustness for Frequency domain Steganographic Algorithms based on Discrete cosine Transform], (2009), *Nauchno-tekhnicheskii Vestnik Sankt-Peterburgskogo Gosudarstvennogo Universiteta Informatsionnykh Tekhnologii, Mekhaniki i Optiki*, Vol.2(60), pp. 102 – 106 (In Russian).

5. Siwei Lyu, (2005), Natural Image Statistics for Digital Image Forensics, a Thesis Submitted to the Faculty in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Computer Science, *Siwei Lyu*, Hanover, USA, 102 p.

6. Quan Weiwei, Guo Yanqing, and Kong Xiangwei, (2006), JPEG Quantization-Distribution Steganalytic Method Attacking Jsteg, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 6, No.7 B, pp. 192 – 195 (In English).

7. Xiaoyi Yu, Yunhong Wang, and Tieniu Tan, (2004), On Estimation of Secret Message Length in JSteg-like Steganography, *Proceedings of the 17th International Conference on Pattern Recognition*, pp. 673 –676 (In English).

8. Aapo Hyvärinen, Jarmo Hurri, and Patrik O. Hoyer, (2009), Natural Image Statistics, *Aapo Hyvärinen*, Springer, 467 p.

9. Zontak M., and Irani M., (2011), Internal Statistics of a Single Natural Image, *Pro-*

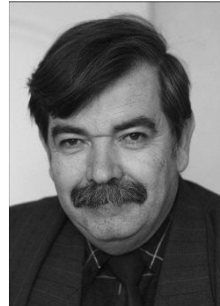
Отримано 06.06.2016

ceedings of the IEEE International Conference on Computer Vision and Pattern Recognition, pp. 977 – 984 (In English).

10. Kalashnikov M., Jakovenko O., Kushnirenko N., and Chechel'nic'kij V., Rozrobka steganografichnogo algoritmu iz urahuvannjam statistiki zobrazhennja-kontejnera [A Development of Steganographic Algorithm Considering Container image Statistic], (2015), *Materiali IV mizhnarodnoï Naukovo-tehnichnoï Konfe-rencii "Zahist Informacii i Bezpeka Informacijnih Sistem"*, Lviv, Ukraine, pp. 129 – 131 (In Ukrainian).

11. Kushnirenko N.I., Chechel'nic'kij V. Ja., Metod kriptografichnoï peredachi informacii na bazi ekvivalentnogo klasu doskonalih dvijkovih reshitok [Method of Cryptographic data Transfer based on Equivalent class of Perfect Binary Lattices], (2014), *Informatika ta Matematichni Metodi v Modeljuvanni*, Odessa, Ukraine, Vol. 3, pp. 210 – 218 (in Russian).

12. Independent JPEG Group [Electronic resource], Independent JPEG Group, (In English), Mode of access: www. Url: <http://www.ijg.org.>, (accessed 27.05.2016). – Title from the screen.



Чечельницький

Віктор Якович, д-р техн. наук, доцент, директор Інст-ту інформаційної безпеки, радіоелектроніки та телекомунікацій Одеського нац. політехнічного ун-ту. Тел.: +38-067-731-44-0
E-mail: cvjonpu@ukr.net



Калашніков

Микола Вячеславович, студент каф. Інформаційної безпеки Одеського нац. політехнічного університету. Тел.: +38(093)7838259.
E-mail: kalashnikov_n.v@ukr.net



Яковенко

Олександр Олександрович, ст. викладач каф. Інформаційної безпеки Одеського нац. політехнічного університету. Тел.: +38-050-960-25-65.
E-mail: iakovenko.oleksandr@gmail.com



Кушніренко

Наталія Ігорівна, ст. викладач каф. Інформаційної безпеки Одеського нац. політехнічного університету. Тел.: +38-093-560-88-63.
E-mail: infsec2011@gmail.com