УДК 004.056.5

СТАТИСТИЧНЕ ВИЯВЛЕННЯ СТЕГАНОГРАФІЧНИХ ПОВІДОМЛЕНЬ У ЗОБРАЖЕННЯХ ФОРМАТУ JPEG

М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко, В. Я. Чечельницький
Одеський національний політехнічний університет

Анотація. *У даній роботі було досліджено можливість детектування повідомлень, прихованих у коефіцієнтах дискретно-косинусного перетворення зображення контейнера. Було обрано статистичні показники та порогове значення для детектування, а також розраховано ймовірність правильного виявлення стеганографічного повідомлення, ймовірності помилок першого та другого роду, статистичну значущість критерію.*

Ключові слова: *цифрова стеганографія, приховування інформації, дискретно-косинусне перетворення, статистичні показники, статистична значущість.*

Вступ

Методи цифрової стеганографії використовуються для того, щоб приховати сам факт існування певних даних при їх передачі, зберіганні або обробці. Зазвичай, повідомлення, яке необхідно передати, конвертується у бінарний формат та вбудовується у певний об'єкт, який не приверне до себе уваги.. Такий об'єкт називається контейнером та може вільно передаватися адресату [1]. У якості контейнера може використовуватися певний текстовий чи медіа-файл, службовий або прихований файл тощо. Значна кількість стеганографічних алгоритмів (СА) використовує у якості контейнера цифрові зображення у форматі JPEG, а також інших форматах із використанням дискретного косинусного перетворення (ДКП). Значна кількість подібних алгоритмів використовує для вбудовування стеганографічного повідомлення (СП) безпосередньо коефіцієнти ДКП зображення-контейнера. Для кодування бітів повідомлення може використовуватись як різниця значень між певними коефіцієнтами ДКП (алгоритми Коха-Жао та Хсу і Ву [1]), так і модифікація найменших значущих бітів (НЗБ) коефіцієнтів ДКП (наприклад, програма JSTEG). Окрім цього, у роботі [2] було запропоновано новий СА, який, окрім зміни НЗБ коефіцієнтів ДКП модифікує таблицю квантизації JPEG. Також було розроблено модифікацію алгоритму JSTEG з метою зменшення викривлень зображення контейнера при вбудовуванні за допомогою перестановки коефіцієнтів ДКП у блоці [3]. Для підвищення рівня захищеності прихованого повідомлення можливим є одночасне використання двох різних СА, наприклад JSTEG та OutGuess, що розглянуто у роботі [4].

Разом з тим, на сьогоднішній день не вирішеним у повній мірі залишається питання створення стеганографічного алгоритму, який би забезпечував вбудовування СП таким чином, що існуючі методи стеганографічного аналізу не змогли б виявити факт наявності вбудованого повідомлення [5]. Існують методи, які дозволяють виявити наявність прихованого повідомлення у зображенні, використовуючи статистичні показники та залежності коефіцієнтів ДКП зображення [6, 7]. Деякі методи також дозволяють оцінити довжину вбудованого повідомлення [8, 9]. Отже, актуальним є питання розробки нових СА, які забезпечать надійний захист від подібних атак. Для розробки таких алгоритмів є необхідним урахування статистичних показників коефіцієнтів ДКП зображення контейнера, що в свою чергу вимагає наявності надійного статистичного тесту для визначення зміни цих показників при вбудовуванні СП [10].

1. Мета та задачі роботи

Метою даної роботи є дослідження ймовірності виявлення СП за допомогою статистичного аналізу особливостей розподілу значень коефіцієнтів ДКП для двох СА, при цьому було вирішено наступні задачі:

1. Обрано показники (критерії) для чисельної оцінки особливостей розподілу коефіцієнтів ДКП.
2. Проведено дослідження особливостей розподілу коефіцієнтів ДКП з використанням обраних показників на вибірці зображень.
3. Досліджено зміну обраних статистичних показників зображення-контейнеру при приховуванні інформації за допомогою різних СА.
4. За отриманими даними обрано порогове значення обраних параметрів для розрізнення порожніх та заповнених контейнерів та оцінено ймовірність виявлення СП.

2. Основна частина

При приховуванні СП у контейнері з використанням алгоритму Jsteg або алгоритму з урахуванням статистичних показників контейнера, який було розглянуто у роботі [11], біти повідомлення вбудовуються у НЗБ коефіцієнтів ДКП контейнера. Отже, вбудовування СП призводить до зміни значень коефіцієнтів ДКП (значення може збільшитись або зменшитись на 1) та їх НЗБ. Тому виявляється доцільним дослідити співвідношення кількості коефіцієнтів ДКП контейнера, які відрізняються лише значеннями НЗБ та співвідношення 0 та 1 у НЗБ коефіцієнтів ДКП.

Для оцінки співвідношення кількості коефіцієнтів ДКП з різними значеннями для всього зображення-контейнера введемо поняття *розбалансу парних коефіцієнтів ДКП контейнеру* Δ_k, де під парними коефіцієнтами маються на увазі коефіцієнти ДКП, що відрізняються лише значенням найменшого значущого біту:

$$\Delta_{\mathrm{k}} = \frac{\sum_{m,n}(k_m - k_n)}{\sum_{i=1}^{N} |k_i|}$$

де *m,n* – відповідні значення парних коефіцієнтів,

N – загальна кількість коефіцієнтів ДКП у контейнері.

Аналогічним чином введемо поняття *розбалансу НЗБ коефіцієнтів ДКП контейнеру* Δ_b, що обчислюється за виразом:

$$\Delta_b = \frac{w^1 - w^0}{N}$$

де w^1 та w^0 – кількість НЗБ коефіцієнтів ДКП, відповідно, зі значеннями «1» і «0»,

N – загальна кількість коефіцієнтів ДКП у контейнері.

З метою визначення зміни розбалансу парних коефіцієнтів ДКП та розбалансу НЗБ коефіцієнтів ДКП контейнеру, було порівняно відповідні показники для вихідних зображень-контейнерів, та заповнених з використанням двох СА – алгоритму JSTEG та алгоритму з урахуванням статистичних показників контейнера, який було розглянуто у роботі [11].

Для дослідження розбалансу парних коефіцієнтів ДКП та розбалансу НЗБ коефіцієнтів ДКП контейнеру, було створено вибірку із довільних зображень формату JPEGзнайдених у мережі Internet. Розмір вибірки N = 1000 зображень. Реалізація обраних СА та визначення обраних статистичних показників здійснювалося у середовищі математичних обчислень Matlab. У якості стеганографічного повідомлення вбудовувався уривок тексту довжиною L = 29559 символів. Для квантування коефіцієнтів ДКП було використано стандартну таблицю IJG [12], показник якості зображення Q = 85. Графічні результати дослідження розбалансу парних коефіцієнтів ДКП та розбалансу НЗБ коефіцієнтів ДКП для вихідних зображень у порівнянні із показниками контейнерів, заповнених з використанням обраних СА, наведені на рис. 1-4.

Виходячи з отриманих графічних результатів, для чисельної оцінки ймовірності наявності СП у зображенні здійснювалось за значенням розбалансу парних коефіцієнтів ДКП контейнеру. Було визначено ймовірність правильного визначення наявності повідомлення *P* для обраного порогового значення *T*. Для цього спочатку дослідили ймовірність помилкового виявлення СП у порожньому контейнері (помилка першого роду [13]), що також дорівнює статистичній значущості критерію α, та ймовірність не виявлення вбудованого повідомлення (помилка другого роду [13]). У якості вихідної гіпотези H_0, виходячи з отриманих графічних результатів, взято припущення, що у зображення вбудовано СП при значеннях $\Delta_k <= T$, а у якості альтернативної гіпотези H_1 – що СП вбудовано при значеннях $\Delta_k > T$. Порогове значення розбалансу парних коефіцієнтів ДКП контейнеру для виявлення СП у зображенні обчислювалося таким чином, щоб ймовірність помилок першого та другого роду була однаковою. Результати дослідження зміни розбалансу парних коефіцієнтів ДКП контейнеру у випадку вбудовування СП за допомогою алгоритму JSTEG та алгоритму з урахуванням статистичних показників наведено відповідно у табл. 1 та 2.

Таблиця 1

Ймовірність висунутих гіпотез для JSTEG

Обрана гіпотеза	Вірна гіпотеза	
	H_0	H_1
H_0	0.819	0.180
H_1	0.181	0.820

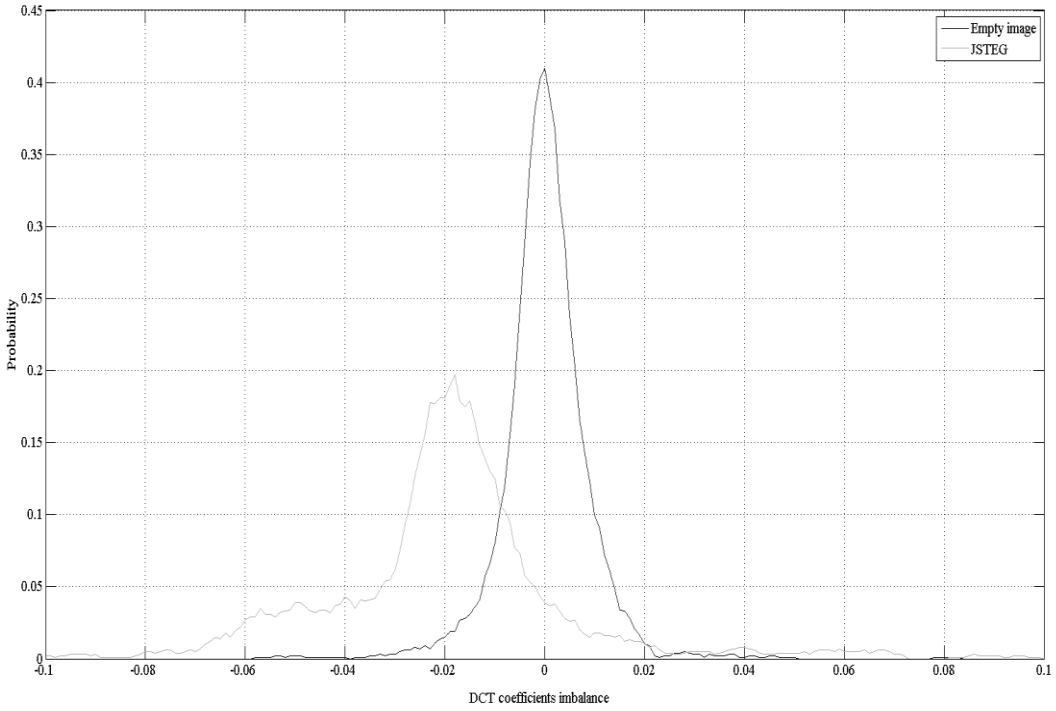


Рис. 1. Розбаланс парних коефіцієнтів ДКП для вихідних зображень та при вбудовуванні СП за допомогою алгоритму JSTEG

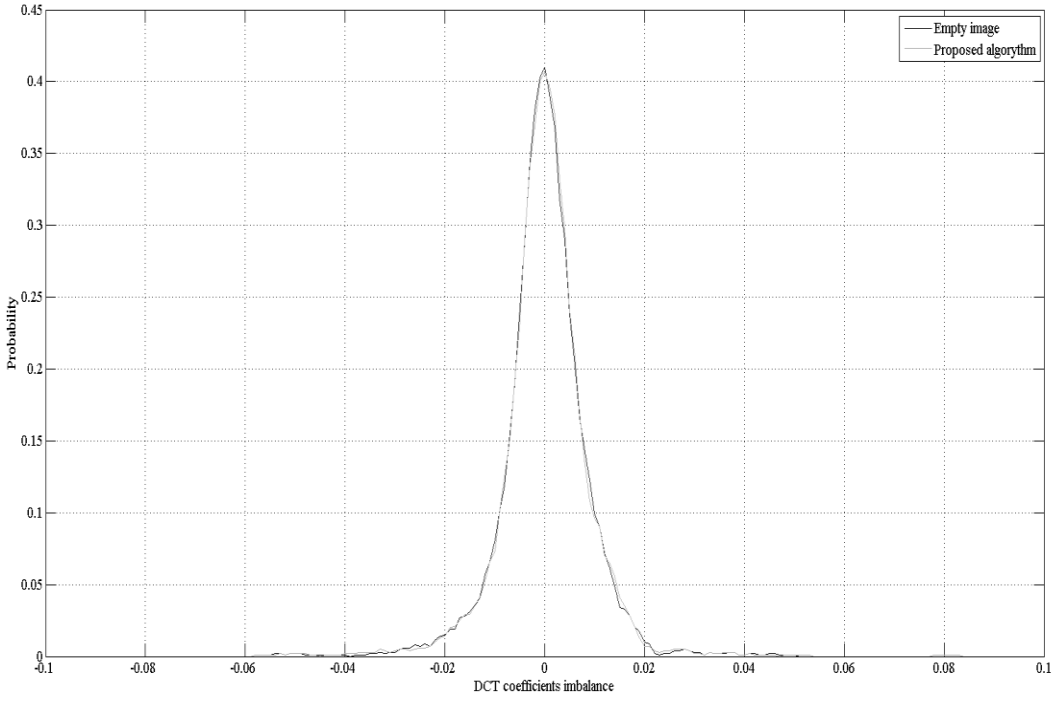


Рис. 2. Розбаланс парних коефіцієнтів ДКП для вихідних зображень та при вбудовуванні СП за допомогою запропонованого алгоритму

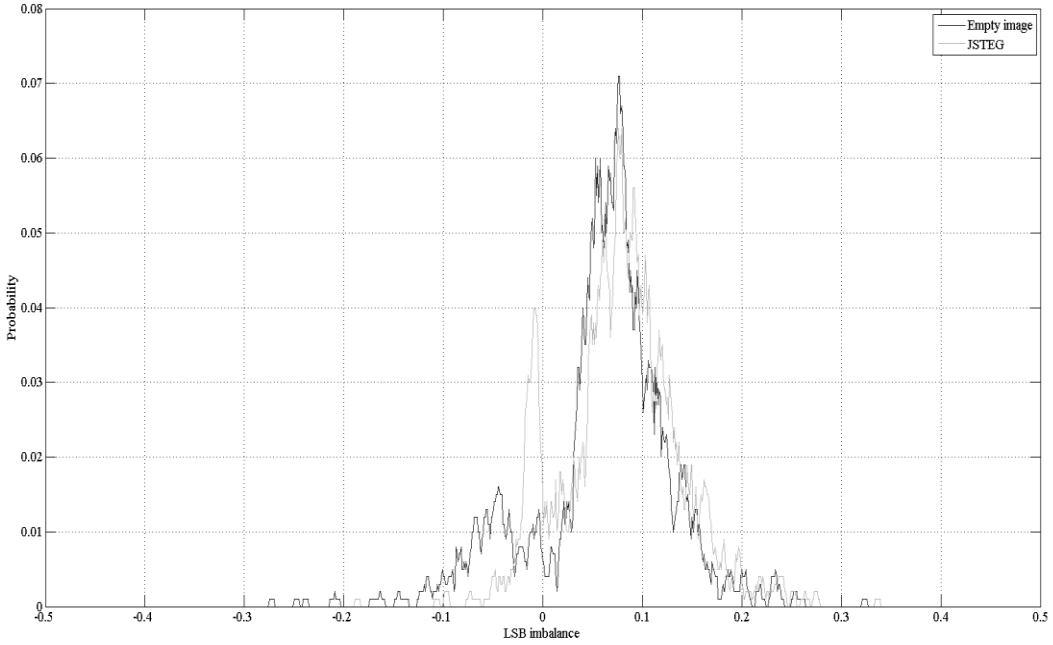


Рис. 3. Розбаланс НЗБ коефіцієнтів ДКП для вихідних зображень та при вбудовуванні СП за допомогою алгоритму JSTEG

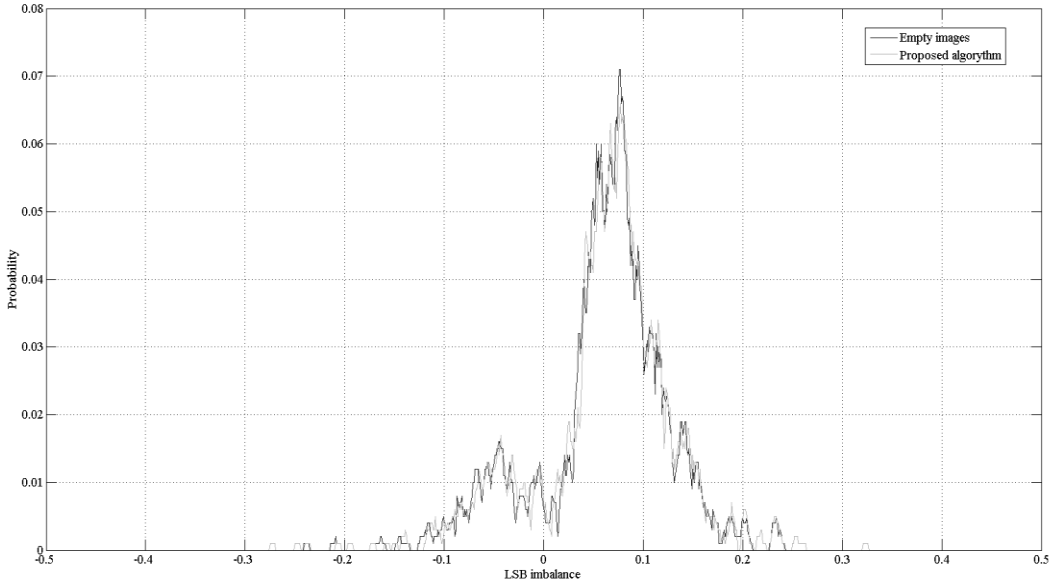


Рис. 4. Розбаланс НЗБ коефіцієнтів ДКП для вихідних зображень та при вбудовуванні СП за допомогою запропонованого алгоритму

Таблиця 2

Ймовірність висунутих гіпотез для запропонованого алгоритму

Обрана гіпотеза	Вірна гіпотеза	
	H_0	H_1
H_0	0.500	0.500
H_1	0.500	0.500

Таким чином, при використанні запропонованого алгоритму [11] ймовірність виявлення вбудованого повідомлення у зображенні склала 0.5, а отже, практично співпадає з ймовірністю виявлення при випадковому виборі гіпотези. При використанні алгоритму JSTEG ймовірність виявлення СП склала 0.819 при пороговому значенні $T = -0.005$.

Висновки

У даній роботі було досліджено особливості розподілу значень коефіцієнтів ДКП та їх НЗБ для зображень формату JPEG, а також можливість виявлення прихованого повідомлення за зміною розподілу цих значень при вбудовуванні СП у контейнер за допомогою СА JSTEG та СА з урахуванням статистичних показників зображення. Для цього було введено поняття розбалансу парних коефіцієнтів ДКП контейнеру та розбалансу НЗБ коефіцієнтів ДКП контейнеру, проведено обчислення даних показників для порожніх та заповнених контейнерів. На основі отриманих результатів для виявлення СП було обрано показник розбалансу парних коефіцієнтів ДКП контейнеру, обрано його порогове значення, таке, що ймовірність помилок першого та другого роду є рівною. За обраним пороговим значенням було розраховано ймовірності цих помилок, ймовірність виявлення СП, прихованого розглянутими СА, статистичну значущість цього критерію, яка дорівнює $\alpha = 0.181$. З отриманих результатів видно, що обраний критерій дозволяє виявляти повідомлення, приховане за допомогою СА JSTEG, з ймовірністю $P = 0.819$. Водночас, ймовірність виявлення повідомлень, прихованих за допомогою СА з урахуванням статистичних показників зображення, становить 0.500, тобто практично співпадає з ймовірністю правильного випадкового вибору. Залишається актуальною задача подальшого удосконалення запропонованого критерію з метою збільшення його статистичної значущості при виявленні повідомлень, прихованих за допомогою СА JSTEG.

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. — 288с., іл.

2. Chang Chin-Chen. A steganographic method based upon JPEG and quantization table [Text] / Chin-Chen Chang, Tung-Shou Chen, Lou-Zo Chung // Information Sciences. — 2002. — № 141 — P. 123–138.

3. Sheisi Hossein. Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm [Text] / Hossein Sheisi, Jafar Mesgarian and Mostafa Rahmani // International Journal of Computer and Electrical Engineering. — 2012. — Vol. 4 № 4 — P. 458–462.

4. Jaheel Hamdan Lateef. A novel approach of combining steganography algorithms [Text] / Hamdan Lateef Jaheel, Zou Beiji // International journal on smart sensing and intelligent systems — 2015 — VOL. 8, №. 1 — P. 90−106.

5. Lyu Siwei. 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, 2005. — 102 p.

6. Weiwei Quan. JPEG Quantization-Distribution Steganalytic Method Attacking Jsteg [Text] / Quan Weiwei, Guo Yanqing, Kong Xiangwei // IJCSNS International Journal of Computer Science and Network Security. — 2006. — VOL.6 No.7B. — P. 192−195.

7. Fu D. JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain [Text] / Dongdong Fu, Yun Q. Shi, Dekun Zou, Guorong Xuan // IEEE: 8th Workshop on Multimedia Signal Processing. — 2006. — P. 310−313.

8. Yu Xiaoyi. On Estimation of Secret Message Length in JSteg-like Steganography [Text] / Xiaoyi Yu, Yunhong Wang, Tieniu Tan // In: Proceedings of the 17th International Conference on Pattern Recognition. — 2004. — P. 673−676.

9. Zhang Tao. A Fast and Effective Steganalytic Technique against JSteg-like Algorithms [Text] / Tao Zhang, Xijian Ping // In: SAC '03 Proceedings of the 2003 ACM symposium on Applied computing — 2003 — P. 307−311.

10. Hyvärinen A. Natural Image Statistics [Text] / Aapo Hyvärinen, Jarmo Hurri, Patrik O. Hoyer. — Springer, 2009. — 467 p.

11. Чечельницький, В. Я. Урахування статистичних властивостей контейнеру для стеганографічного алгоритму [Текст] / В. Я. Чечельницький, М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко // Електротехнічні та комп'ютерні системи. — 2016. — № 23(99) .— С. 83−87.

12. Independent JPEG Group [Electronic resource] // Independent JPEG Group. — Mode of access: WWW.URL: http://www.ijg.org/ — Last access: 10.04.2017. — Title from the screen.

13. Ошибки I и II рода при проверке гипотез, мощность [Electronic resource] // Портал знаний. — Mode of access: WWW.URL: http://statistica.ru/theory/oshibki-pri-proverke-gipotez-moshchnost/ — Last access: 10.04.2017. — Title from the screen.

References

1. Konahovich, G. F. and Puzyrenko, A. Ju. (2006). *Computer steganography. Theory and practice* [Komp'juternaja steganografija. Teorija i praktika], Kyiv: «MK-Press», 288p.

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

3. Sheisi, H., Mesgarian, J. and Rahmani, M. (2012), Steganography: DCT Coefficient Replacement Method and Compare With JSteg Algorithm, *International Journal of Computer and Electrical Engineering*, Vol. 4 № 4, pp. 458–462.

4. Jaheel, Hamdan Lateef and Beiji, Zou (2015), A novel approach of combining steganography algorithms, *International journal on smart sensing and intelligent systems*, VOL. 8, №. 1 pp. 90−106.

5. Siwei Lyu. Natural Image Statistics for Digital Image Forensics. (2003), a Thesis Submitted to the Faculty in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science, Hanover, USA, 102 pp.

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

7. Fu, Dongdong, Shi, Yun Q., Zou, Dekun and Xuan, Guorong (2006), JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain, *IEEE: 8th Workshop on Multimedia Signal Processing*, pp. 673−676.

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

9. Zhang, Tao and Ping, Xijian (2003), A Fast and Effective Steganalytic Technique against JSteg-like Algorithms, *SAC '03 Proceedings of the 2003 ACM symposium on Applied computing*, pp. 307−311.

10. Hyvärinen, A., Hurri J. and Hoyer, P. O. (2009). *Natural Image Statistics*. Springer, 467 p.

11. Chechelnytskyi, V., Kalashnikov, M., Iakovenko, O. and Kushnirenko, N. (2016), Container`s statistic features considering for steganographic algorithm [Urakhuvannya statystychnykh vlastyvostey konteyneru dlya stehanohrafichnoho alhorytmu], *Electrotechnic and computer systems*, № 23(99), pp. 83−87.

12. Ijg.org, (1991). Independent JPEG Group. [online] Available at: http://www.ijg.org/ [Accessed 10 Apr. 2017].

13. Statistica.ru, (2010). Knowledge portal [Portal znaniy]. [online] Available at: http://www.ijg.org/ [Accessed 10 Apr. 2017].

JPEG STATISTICAL DETECTION OF STEGANOGRAPHIC MESSAGES

M. V. Kalashnikov, O. O. Iakovenko, N. I. Kushnirenko, V. Ja. Chechelnytskyi
Odessa National Polytechnic University

Abstract. *The subject of this work done is digital steganography field, namely hidden messages detection in statical digital pictures problem. In this paper probability of hidden messages detection using statistical features distribution of discrete cosine transform coefficients for two steganographic algorithms was checked. This data allow detecting JSTEG hidden messages and improving algorithm with image statistic features considering. For this purpose two novel parameters: imbalance of container`s paired discrete cosine transform coefficients and imbalance of container`s discrete cosine transform coefficients least significant bits were determined. As steganographic containers, JPEG images were considered. These parameters were measured for one thousand of empty containers samples and for equal quantity of containers with messages, hidden by JSTEG algorithm and by early proposed steganographic algorithm with container image statistics accounting. Based on the received results, imbalance of container`s paired discrete cosine transform coefficients was chosen as a measured parameter for embedded message detection. Also measured parameter threshold was chosen on condition, that probability of type I and type II errors is equal. With this parameter threshold value probability of type I and type II errors, probability of hidden messages detection and statistical significance of chosen parameter α was calculated. Based on the received results, only JSTEG hidden messages can be definitely detected by chosen parameter measurement. In considered publications, histogram detection of hidden messages was principally described, so this work can offer alternate different numerical parameter for JPEG steganalisys.*

Key words: *digital steganography, data hiding, discrete-cosine transform, statistic features, statistical significance.*

СТАТИСТИЧЕСКОЕ ВЫЯВЛЕНИЕ СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ В ИЗОБРАЖЕНИЯХ ФОРМАТА JPEG

Н. В. Калашников, А. А. Яковенко, Н. И. Кушниренко, В. Я. Чечельницкий

Одесский национальный политехнический университет

Аннотация. *В данной работе было исследовано возможность детектирования сообщений, скрытых в коэффициентах дискретно-косинусного преобразования изображения-контейнера. Были выбраны статистические показатели и пороговое значение для детектирования, а также вычислено вероятность правильного выявления стеганографического сообщения, вероятности ошибок первого и второго рода, статистическую значимость критерия.*

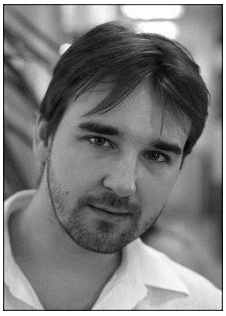
Ключевые слова: *цифровая стеганография, сокрытие информации, дискретно-косинусное преобразование, статистические показатели, статистическая значимость.*

Получено 17.04.2017

Калашніков Микола Вячеславович, аспірант кафедри інформаційної безпеки Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: kalashnikov_n.v@ukr.net, тел. +38-048-705-84-41

Kalashnikov Nikolay, Graduate student, Department of information security, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine

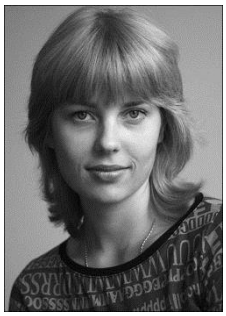
ORCID ID: 0000-0002-4286-1162



Яковенко Олександр Олександрович, старший викладач кафедри інформаційної безпеки Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: iakovenko.oleksandr@gmail.com, тел. +38-050-960-25-65

Iakovenko Oleksandr, Senior lecturer, Department of information security, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine

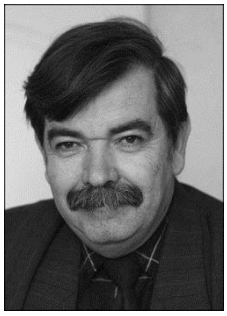
ORCID ID: 0000-0003-1013-9463



Кушніренко Наталія Ігорівна, старший викладач кафедри інформаційної безпеки Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: infsec2011@gmail.com, тел. +38-093-560-88-63

Kushnirenko Nataliia, Senior lecturer, Department of information security, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine

ORCID ID: 0000-0003-3722-0229



Чечельницький Віктор Якович, доктор технічних наук, завідуючий кафедрою інформаційної безпеки Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: cvjonpu@ukr.net, тел. +38-067-731-44-04

Chechelnytskyi Victor, Dr. of Science, Head of the Department of information security, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine

ORCID ID: 0000-0002-8155-5109