УДК 004.056.5

ЗМІНА СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ КОНТЕЙНЕРУ У ЧАСТОТНІЙ ОБЛАСТІ ДЛЯ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко, Л. В. Нечитайлова
Одеський національний політехнічний університет

Анотація. *У даній роботі було проведено порівняльне дослідження ймовірності виявлення стеганографічного повідомлення за допомогою статистичного аналізу при вбудовуванні із перестановкою коефіцієнтів ДКП у блоці та з урахуванням статистичних властивостей контейнера. Було розраховано ймовірність правильного виявлення стеганографічного повідомлення, ймовірності помилок першого та другого роду, статистичну значущість критерію. У результаті дослідження було виявлено, що подібний аналіз дозволяє виявити повідомлення, вбудоване із перестановкою коефіцієнтів ДКП, а при урахуванні урахуванням статистичних властивостей контейнера ймовірність його виявлення близька до ймовірності при випадковому вгадуванні.*

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

Вступ

Стеганографія вирішує задачі приховування факту існування таємних даних при їх передачі, зберіганні або обробці. Приховане повідомлення, вбудовується у певний контейнер — об'єкт, що не привертає уваги та може вільно передаватися адресату. Стеганографічні алгоритми (СА) набули широкого вжитку для попередження несанкціонованого доступу до інформації, а також вбудовування цифрових водяних знаків у цифрові носії інформації з метою захисту авторських прав [1].

Значна кількість цифрових зображень зберігається на електронних носіях інформації та передається по каналам цифрового зв'язку, у форматі JPEG, а також у інших форматах, що використовують дискретне косинусне перетворення (ДКП). Для приховування інформації у частотній області таких зображень застосовують СА, які можуть використовувати як різницю коефіцієнтів ДКП для кодування бітів стеганографічного повідомлення (СП), наприклад алгоритми Кохa-Жао та Хсу і Ву [1], так і модифікацію найменших значущих бітів (НЗБ) коефіцієнтів ДКП, як у програмі Jpeg-Jsteg. Використання подібних алгоритмів може забезпечити рівень викривлень зображення-контейнера, який є непомітним для людського ока. Разом з тим, приховування СП призводить до зміни статистичних показників зображення-контейнера, що може бути виявлено, наприклад, за зміненням розподілу значень коефіцієнтів ДКП або за зміною співвідношення кількості парних та непарних коефіцієнтів ДКП у зображенні.

1. Аналіз досліджень та публікацій

Питання вбудовування та прихованої передачі інформації з використанням цифрових зображень формату JPEG розглянуто у ряді наукових праць. Наприклад, у [2] запропоновано СА, у якому після вбудовування повідомлення виконується перестановка коефіцієнтів ДКП у блоці для зменшення викривлень у просторовій області. У роботах [3] та [4] розглянуто СА із рівномірним вбудовуванням повідомлення у контейнер, які використовують взаємокореляцію між блоками ДКП для зменшення ймовірності статистичного виявлення СП. У [5] запропоновано алгоритм для медичних зображень формату JPEG, що забезпечує збереження різниці коефіцієнтів ДКП, які знаходяться на однакових позиціях. Для протидії стеганографічному аналізу у декількох областях, запропоновано СА [6], який враховує викривлення блоків пікселів у просторовій області та коефіцієнтів ДКП у частотній. Розроблено стеганографічні алгоритми для вбудовування повідомлення шляхом імітації натурального шуму, який виникає при створенні (зйомці) зображення, з використанням вихідного зображення у форматі RAW [7] та з використанням додаткових зображень одної сцени [8]. Також запропоновано СА, що забезпечує ймовірності виявлення СП статистичним аналізом шляхом вбудовування з використанням обраної моделі статистичних показників контейнера [9].

Також запропоновано методи стеганографічного аналізу на основі зміни окремих особливостей контейнеру [10] та з використанням двови-

мірних фільтрів Габора [11], які забезпечують покращене статистичне виявлення прихованих повідомлень.

2. Мета та задачі роботи

Метою даної роботи є дослідження показників викривлення контейнера та зміни його статистичних показників при вбудовуванні інформації СА з використанням перестановки коефіцієнтів ДКП у блоці [2] та СА з урахуванням статистичних показників контейнера [12]. При цьому було вирішено наступні задачі:

1. Обрано показники (критерії) для чисельної оцінки особливостей розподілу коефіцієнтів ДКП.

2. Проведено вбудовування стеганографічного повідомлення у відібрані зображення-контейнери за допомогою обох СА.

3. Досліджено зміну обраних статистичних показників зображення-контейнеру при приховуванні стеганографічного повідомлення за допомогою різних СА.

4. За отриманими даними обрано порогове значення обраних параметрів для розрізнення порожніх та заповнених контейнерів та оцінено ймовірність виявлення СП.

3. Основна частина

При приховуванні СП у контейнері з використанням алгоритму з урахуванням статистичних показників контейнера, який було розглянуто у роботі [12] або алгоритму з перестановкою коефіцієнтів ДКП, що описано у [4], біти повідомлення вбудовуються у НЗБ коефіцієнтів ДКП контейнера. Тому виглядає доцільним дослідити співвідношення кількості коефіцієнтів ДКП з різними значеннями для кожного з модифікованих зображень. Для цього використаємо такий показник, як *розбаланс парних коефіцієнтів ДКП контейнеру* Δ_k, визначення якого було наведено у роботі [13].

Розрахунок розбалансу парних коефіцієнтів ДКП контейнеру здійснюється наступним чином:

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

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

N – загальна кількість коефіцієнтів ДКП у контейнері.

Для визначення зміни обраного показника при вбудовуванні СП у контейнер було проведено обчислювальний експеримент у середовищі математичних обчислень Matlab. Експеримент виконувався наступним чином:

1. Було створено вибірку із довільних зображень формату JPEG, знайдених у мережі Internet. Розмір вибірки N = 1000 зображень. Для квантування коефіцієнтів ДКП було використано стандартну таблицю IJG [14], показник якості зображення Q = 85.

2. Також було обрано уривок тексту довжиною L = 29559 символів у якості стеганографічного повідомлення. Було вирішено вбудовувати однакове повідомлення в усі контейнери, для того, щоб зміна обраного статистичного показника залежала лише від властивостей зображення-контейнера.

3. Було обчислено значення розбалансу парних коефіцієнтів ДКП для кожного порожнього зображення-контейнера.

4. Було проведено вбудовування обраного повідомлення у кожне зображення-контейнер за допомогою СА з використанням перестановки коефіцієнтів ДКП у блоці та для кожного отриманого зображення обчислено значення розбалансу парних коефіцієнтів ДКП.

5. Аналогічним чином було проведено вбудовування повідомлення за допомогою СА з урахуванням статистичних показників контейнера, для кожного отриманого зображення також обчислено значення розбалансу парних коефіцієнтів ДКП.

Результати виконання пп. 3-5 наведені у графічному вигляді на рис. 1.

З отриманих результатів видно, що вбудовування СП змінює розподіл значень розбалансу парних коефіцієнтів ДКП. Тому стає можливим правильно виявити факт вбудовування СП у довільне зображення із певною ймовірністю P шляхом порівняння значення розбалансу парних коефіцієнтів ДКП Δ_k з обраним пороговим значенням T. Виходячи з рис. 1, у якості вихідної гіпотези H_0 було взято припущення, що у контейнері є приховане повідомлення, якщо $\Delta_k >= T$. Альтернативною гіпотезою H_1 стало припущення, що повідомлення вбудовано при значеннях $\Delta_k < T$. Ймовірність вірності кожної з гіпотез (або похибки) обчислювалась як:

$$P = \frac{N_H}{N}$$

де N_H – кількість зображень у вибірці, для яких виконується (не виконується) обрана для даної гіпотези умова,

N – загальна кількість зображень у вибірці.

З точки зору стеганографічного аналізу довільного зображення, виглядає важливим не лише правильне виявлення вбудованого повідомлення, але й правильне виявлення його відсутності. Тому порогове значення T було розраховане таким чином, щоб ймовірність помилкового виявлення СП у порожньому контейнері (помилка першого роду [15]), що також дорівнює статистичній значущості критерію α, та ймовірність не виявлення вбудованого повідомлення (помилка другого роду [15]) були рівними [13]. Отримане значення $T = 0.005$.

Розрахунок ймовірностей вірності висунутих гіпотез та помилок було проведено для СА з перестановкою коефіцієнтів ДКП та для СА алгоритму з урахуванням статистичних показників контейнеру. Результати наведено у табл. 1 та 2 відповідно.

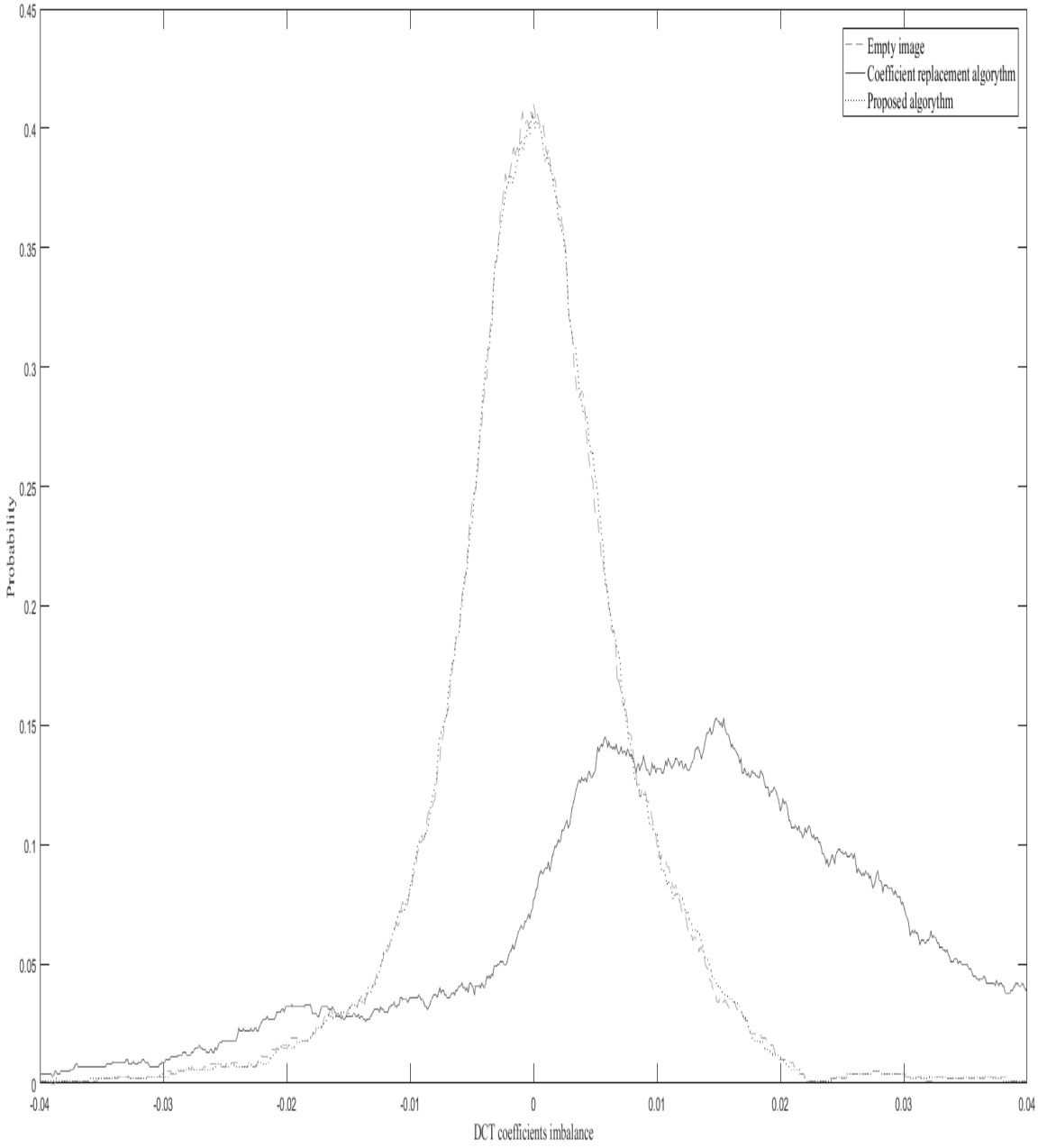


Рис. 1. Розбаланс парних коефіцієнтів ДКП для вихідних зображень та при вбудовуванні СП за допомогою досліджених СА

Таблиця 1

Ймовірність вірності висунутих гіпотез для стеганографічного алгоритму з перестановкою коефіцієнтів ДКП

Обрана гіпотеза	Вірна гіпотеза	
	H_0	H_1
H_0	0.749	0.251
H_1	0.251	0.749

Таблиця 2

Ймовірність вірності висунутих гіпотез для стеганографічного алгоритму з урахуванням статистичних показників контейнеру

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

Таким чином, при використанні алгоритму з урахуванням статистичних показників контейнеру [12] ймовірність вірного виявлення вбудованого повідомлення склала 0.5, а отже, практично співпадає з ймовірністю виявлення при випадковому виборі гіпотези. При використанні алгоритму з перестановкою коефіцієнтів ймовірність виявлення СП склала 0.749 при пороговому значенні $T = 0.005$.

Висновки

У даній роботі було проведено порівняльне дослідження особливостей розподілу значень коефіцієнтів ДКП та ймовірності виявлення прихованого повідомлення за зміною розподілу цих значень при вбудовуванні СП у контейнер за допомогою СА з перестановкою коефіцієнтів ДКП та СА з урахуванням статистичних показників зображення. Для цього використано показник розбалансу парних коефіцієнтів ДКП контейнеру, який було введено у роботі [13], проведено обчислення даного показника для порожніх та заповнених контейнерів.

Було висунуто гіпотези стосовно умов, при яких за значенням розбалансу парних коефіцієнтів ДКП контейнеру можливо вірно виявити наявність прихованого повідомлення у зображенні-контейнері, обрано спосіб для розрахунку ймовірності вірності цих гіпотез, та, відповідно, для розрахунку ймовірностей помилок першого та другого роду, обрано порогове значення для порівняння. Порогове значення було обрано таким чином, щоб ймовірність помилок першого та другого роду були однаковими.

За обраним пороговим значенням було розраховано ймовірності цих помилок, ймовірність виявлення СП, прихованого розглянутими СА, статистичну значущість цього критерію, яка дорівнює $\alpha = 0.251$.

З отриманих результатів видно, що при вбудовуванні повідомлення за допомогою СА з перестановкою коефіцієнтів ДКП, використаний показник забезпечує ймовірність успішного виявлення СП $P = 0.749$. Водночас, ймовірність виявлення повідомлень, прихованих за допомогою СА з урахуванням статистичних показників зображення, становить 0.500, тобто практично співпадає з ймовірністю правильного випадкового вибору. Враховуючи [13], видно, що використаний показник забезпечує дещо меншу ймовірність виявлення СП, вбудованого СА з перестановкою коефіцієнтів ДКП у порівнянні із алгоритмом JSTEG, але все одно вищу, ніж при використанні СА з урахуванням статистичних показників зображення. Залишається актуальним питання подальшого покращення алгоритму виявлення СП для урахування більшої кількості статистичних показників зображення-контейнера.

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. Sheisi, H. 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

3. Guo, L. Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited [Text] / Linjie Guo, Jiangqun Ni, Wenkang Su, Chengpei Tang, and Yun-Qing Shi // IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10. — Issue 12 — P. 2669–2680

4. Pan, Y. Improved Uniform Embedding for Efficient JPEG Steganography [Text] / Yuanfeng Pan, Jiangqun Ni, and Wenkang Su // International Conference on Cloud Computing and Security. — 2016. — Vol. 10. — Issue 12 — P. 125–133

5. Liao, X. Medical JPEG image steganography based on preserving inter-block dependencies [Text] / Xin Liao, Jiaojiao Yin, Sujing Guo, Xiong Li, and Arun Kumar Sangaiah // Computers & Electrical Engineering. — 2018. — Vol. 67. — P. 320–329

6. Wang, Z. Hybrid distortion function for JPEG steganography [Text] / Zichi Wang, Xinpeng Zhang and Zhaoxia Yin // Journal of Electronic Imaging. — 2016. — Vol. 25(5).

7. Denemark, T. Natural Steganography in JPEG Compressed Images [Text] / Tomáš

Denemark, Patrick Bas and Jessica Fridrich // Electronic Imaging, Media Watermarking, Security, and Forensics. — 2018. P. 316–1–316–10(10)

8. Denemark, T. Steganography With Multiple JPEG Images of the Same Scene [Text] / Tomáš Denemark, Jessica Fridrich // IEEE Transactions on Information Forensics and Security. — 2017. — Vol. 12. — Issue 10 — P. 2308–2319

9. Sedighi, V. Content-Adaptive Steganography by Minimizing Statistical Detectability [Text] / Vahid Sedighi, Rémi Cogranne and Jessica Fridrich // IEEE Transactions on Information Forensics and Security. — 2016. — Vol. 11. — Issue 2. — P. 221–234

10. Denemark, T. Steganalysis Features for Content-Adaptive JPEG Steganography [Text] / Tomáš Denemark, Mehdi Boroumand and Jessica Fridrich // IEEE Transactions on Information Forensics and Security. — 2016. — Vol. 11. — Issue 8. — P. 1736–1746

11. Song, X. Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters [Text] / Xiaofeng Song, Fenlin Liu, Chunfang Yang, Xiangyang Luo and Yi Zhang // Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. — 2015. — Vol. 10. — Issue 12 — P. 15–23

12. 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.

13. Калашніков, М. В. Статистичне виявлення стеганографічних повідомлень у зображеннях формату JPEG / М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко, В. Я. Чечельницький // Електротехнічні та комп'ютерні системи. — 2017. — № 25(101). — С. 310–316.

14. 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.

15. 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. 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 (in English)

3. Guo, L., Ni, J., Su, W., Tang, C., and Shi, Y. (2015), Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited, IEEE Transactions on Information Forensics and Security, Vol. 10 Issue 12, pp. 2669–2680 (in English)

4. Pan, Y., Ni, J., and Su, W. (2016), Improved Uniform Embedding for Efficient JPEG Steganography, International Conference on Cloud Computing and Security, Vol. 4 Issue 12, pp. 125–133 (in English)

5. Liao, X., Yin, J., Guo, S., Li, X. and Arun Kumar Sangaiah, (2018), Medical JPEG image steganography based on preserving inter-block dependencies, Computers & Electrical Engineering, Vol. 67, pp. 320–329 (in English)

6. Wang, Z., Zhang, X. and Yin, Z. (2016), Hybrid distortion function for JPEG steganography, Journal of Electronic Imaging, Vol. 25(5) (in English)

7. Denemark, T., Bas, P. and Fridrich, J. (2018), Natural Steganography in JPEG Compressed Images, Electronic Imaging, Media Watermarking, Security, and Forensics, pp. 316–1–316–10(10) (in English)

8. Denemark, T. and Fridrich, J. (2017), Steganography With Multiple JPEG Images of the Same Scene, IEEE Transactions on Information Forensics and Security, Vol. 12. Issue 10, pp. 2308–2319 (in English)

9. Sedighi, V., Cogranne, R. and Fridrich, J. (2016), Content-Adaptive Steganography by Minimizing Statistical Detectability, IEEE Transactions on Information Forensics and Security, Vol. 11 Issue 2, pp. 221–234 (in English)

10. Denemark, T., Boroumand, M. and Fridrich, J. (2016), Steganalysis Features for Content-Adaptive JPEG Steganography, IEEE Transactions on Information Forensics and Security, Vol. 11 Issue 8, pp. 1736–1746 (in English)

11. Song, X., Liu, F., Yang, C., Luo, X. and Zhang, Y. (2015), Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters, International Journal of Computer and Electrical Engineering, Vol. 10 Issue 12, pp. 15–23 (in English)

12. Chechelnytskyi, V., Kalashnikov, M., Iakovenko, O. and Kushnirenko, N. (2016), Container`s statistic features considering for ste-

ganographic algorithm [Urakhuvannya statystychnykh vlastyvostey konteyneru dlya stehanohrafichnoho alhorytmu], Electrotechnic and computer systems, №25(101), pp. 310–316.

13. Kalashnikov, M., Iakovenko, O., Kushnirenko, N. and Chechelnytskyi, V. (2017), JPEG statistical detection of steganographic messages [Statystychne vyiavlennia stehanohrafichnykh povidomlen u zobrazhenniakh formatu JPEG], Electrotechnic and computer systems, №23(99), pp. 83–87.

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

15. Statistica.ru, (2010). Knowledge portal [Portal znaniy]. [online] Available at: http://www.ijg.org/ [Accessed 10 Apr. 2017]. http://statistica.ru/theory/oshibki-pri-proverke-gipotez-moshchnost/

CONTAINER`S STATISTIC FEATURES CHANGES FOR STEGANOGRAPHIC ALGORITHM IN FREQUENCY DOMAIN

M. V. Kalashnikov, O. O. Iakovenko, N. I. Kushnirenko, L. V. Nechitaylova
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 messages hidden by steganographic algorithm with DCT coefficient replacement and improving algorithm with image statistic features considering. For this purpose was used early proposed parameter: imbalance of container`s paired discrete cosine transform coefficients. As steganographic containers, JPEG images were considered. For image DCT coefficients quantization, standard IJG matrix was used. These parameters were measured for one thousand of empty containers samples and for equal quantity of containers with messages, hidden by algorithm with DCT coefficients replacement and by early proposed steganographic algorithm with container image statistics accounting. For all steganographic containers same text message was embedded that container`s statistic changes depend only on its own characteristics. Imbalance of container`s paired discrete cosine transform coefficients was used as a measured parameter for embedded message detection. Based on the obtained experimental results, the initial and alternative hypotheses about message presence in container were considered. 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 messages hidden by steganographic algorithm with DCT coefficient replacement can be definitely detected by chosen parameter measurement. For embedding with image statistic features considering probability of message detecting nearly equal to random guessing results.*

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

ИЗМЕНЕНИЕ СТАТИСТИЧЕСКИХ СВОЙСТВ КОНТЕЙНЕРА В ЧАСТОТНОЙ ОБЛАСТИ ДЛЯ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА

Н. В. Калашников, А. А. Яковенко, Н. И. Кушниренко, Л. В. Нечитайлова
Одесский национальный политехнический университет

Аннотация. *В данной работе было проведено сравнительное исследование вероятности обнаружения стеганографического сообщения при помощи статистического анализа при встраивании с перестановкой коэффициентов ДКП внутри блока и с учетом статистических особенностей контейнера. Было рассчитано вероятность правильного обнаружения стеганографического сообщения, вероятность ошибок первого и второго рода, статистическую значимость критерия. В результате исследования было выявлено, что подобный анализ позволяет выявить сообщение, встроенное с перестановкой коэффициентов ДКП, а при учете статистических особенностей контейнера вероятность его обнаружения близка к вероятности при случайном угадывании.*

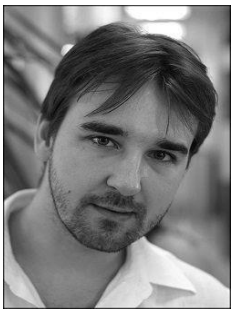
Ключевые слова: *цифровая стеганография, сокрытие информации, дискретно-косинусное преобразование, статистические показатели, статистическая значимость.*

Отримано 15.02.2019

Калашніков Микола Вячеславович, аспірант кафедри радіотехнічних пристроїв 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 radioengineering equipment, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: kalashnikov_n.v@ukr.net

ORCID ID: 0000-0002-4286-1162



Яковенко Олександр Олександрович, старший викладач кафедри радіотехнічних пристроїв 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, Radioengineering Equipment Department, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: iakovenko.oleksandr@gmail.com

ORCID ID: 0000-0003-1013-9463

Кушніренко Наталія Ігорівна, к.т.н., доцент кафедри інформатики та управління захистом інформаційних систем Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: infsec2011@gmail.com, тел. +38-093-560-88-63

Kushnirenko Nataliia, Candidate of Technical Sciences, Associate Professor of Department of informatics and control of information systems protection of Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: infsec2011@gmail.com

ORCID ID: 0000-0003-3722-0229

Нечитайлова Любов Володимирівна, студентка кафедри інформатики та управління захистом інформаційних систем Одеського національного політехнічного університету. Просп. Шевченко, 1, Одеса, Україна, E-mail: lyubanechitaylova@gmail.com, тел. +38-066-644-46-20

Nechitaylova Lyubov, student of the Department of informatics and control of information systems protection, Shevchenko ave, 1, Odessa, Ukraine, E-mail: lyubanechitaylova@gmail.com

ORCID ID: 0000-0001-9714-4243