ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2020.2(61)
Issue 2(61) 2020

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

УДК 004.056.5

Борисенко Ірина Іванівна,
старший викладач Одеського національного політехнічного університету,
м. Одеса, Україна

АНАЛІЗ ЗБУРЕНЬ КОНТЕЙНЕРА ЯК ОСНОВА МЕТОДУ ВБУДОВУВАННЯ ІНФОРМАЦІЇ

Запропоновано метод кількісної оцінки збурень контейнера під час його стеганографічного перетворення, який дозволяє побудову більш ефективних алгоритмів за рахунок мінімізації впливу вбудованого повідомлення на контейнер. Побудовано функцію, яка дозволяє виконати аналіз збурень, що виникають під час вбудовування повідомлень різними стеганографічними алгоритмами, що дає можливість порівнювати їх ефективність. Наведено результати обчислювального експерименту, які підтверджують ефективність запропонованого методу.

Ключові слова: *вбудоване повідомлення, збурення контейнера, стеганографічне перетворення, сингулярне число.*

Предложен метод количественной оценки возмущений контейнера при его стеганографическом преобразовании, который позволяет построение более эффективных алгоритмов за счет минимизации влияния встроенного сообщения на контейнер. Построена функция, позволяющая выполнить анализ возмущений, возникающих при внедрении сообщений различными стеганографическими алгоритмами, что дает возможность сравнивать их эффективность. Приведены результаты вычислительного эксперимента, подтверждающие эффективность предложенного метода.

Ключевые слова: *встроенное сообщение, возмущение контейнера, стеганографическое преобразование, сингулярное число.*

Вступ

Стеганосистема є безумовно досконалою (безумовно надійною) [1], якщо ймовірностний розподіл контейнера точно відповідає розподілу стеганоконтейнера. Теоретично такі стеганосистеми для штучних джерел були побудовані [2]. Проте неможливо точно визначити ймовірностний розподіл реальних контейнерів, роль яких відіграють цифрові медіа (звук, цифрові зображення, відео), через складність їх структури, тому досконалу стеганосистему на базі таких контейнерів побудувати неможливо [3]. Завдяки сказаному побудова захищених стеганографічних систем із використанням реальних

контейнерів наразі залишається відкритим й потребує подальшого дослідження і розвитку.

Вбудовування інформації в контейнер призводить до зміни його характеристик. Ці зміни використовуються методами стеганоаналізу для розпізнавання стеганоконтейнерів. Чим менше збурень зазнає контейнер під час вбудовування інформації, тим важче стеганоаналітичним методам забезпечити низький рівень похибки при розпізнаванні. Останнім часом активно проводяться роботи зі створення стеганографічних методів та алгоритмів, розробники яких намагаються забезпечити найменш можливий вплив на контейнер вбудованої інформації як за рахунок вибору елементів контейнера для вбудовування, так і специфіки самого алгоритму [4–8]. Однак остаточного вирішення це питання не набуло, оскільки методи, які доступні з відкритих джерел, не мають строгого математичного підґрунтя, а отже, не можуть бути універсальними.

Метою роботи є розробка методу оцінки збурень матриці контейнера при його стеганографічному перетворенні, який би не залежав від стеганографічного алгоритму, який використовується й який дозволяв би проводити порівняння збурень контейнера, котрі вносяться різними стеганоалгоритмами.

Основна частина

У якій би області (спектральній, просторовій і т.д.) не проводилося стеганоперетворення (СП) матриці контейнера, це обов'язково призведе до зміни значень елементів у просторовій області. Аналіз збурень контейнера показав, що залежність від того, значення яких елементів були модифіковані, рівень збурення матриці контейнера буде неоднаковим. Розглянемо це ствердження у формальному вигляді.

Як контейнер будемо використовувати цифрове зображення (ЦЗ) з матрицею $C=[c_{ij}]$ розмірності mґn, $c_{ij} \in [0;255]$. Розглянемо два пікселі зі значеннями K_1 і K_2, таких, що $K_1 > K_2$. Змінимо ці значення на +1 кожне (тобто надамо елементам мінімально можливе збурення), а значення інших пікселів залишимо без змін. Оскільки значення пікселів змінилися на однакову величину, то може видатися, що їх внесок у зміну характеристик контейнера повинен бути однаковим, але це не так. Так, наприклад, однією з важливих характеристик цифрового сигналу є його енергія [9]. Для ЦЗ енергія в просторовій області обчислюється за формулою: $E = \sum_i \sum_j c_{ij}^2$.

Тоді нове значення енергії $\overline{E} = E + \Delta E$ буде визначатися формулою: $\overline{E} = c_{11}^2 + c_{12}^2 + ... + K_1^2 + 2K_1 + 1 + ... + K_2^2 + 2K_2 + 1 + ... + c_{mn}^2$.

Приріст функції DE=d_1+d_2 складає сума величин d_1=2K_1+1 і d_2=2K_2+1, де d_1>d_2. Отже, внесок пікселя із значенням K_1 в DE більший, ніж внесок пікселя зі значенням K_2.

У наш час активно розвиваються методи стеганографії [10,11 та інші, які ґрунтуються на загальному підході до аналізу стану й технології функціонування інформаційних систем (ЗПАІС) [12], у основу якого покладено матричний аналіз і теорію збурень. Перетворення контейнера за рахунок вкладення в нього повідомлення незалежно від способу і області цього вкладення, відповідно до ЗПАІС

представляється як збурення DC матриці C: $\overline{C} = C + \Delta C$, де $\overline{C}$ – матриця стеганоконтейнера або у вигляді сукупності збурень множини сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці контейнера, які її однозначно визначають [12]. Нагадаємо, що для матриці C сингулярне перетворення (SVD) має вигляд: $F = USV^T$, де U, V – ортогональні матриці, (тобто $U^TU = I$, $V^TV = I$, I– одинична матриця) розмірності $m \times n$ и $n \times n$ відповідно; $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$. Стовпці $u_1,...,u_n$ матриці U і $v_1,...,v_n$ матриці V називають відповідно лівими і правими сингулярними векторами матриці F, величины $\sigma_1,...,\sigma_n$ – сингулярними числами.

Оскільки СНЧ і СНВ є параметрами, які однозначно характеризують матрицю контейнера [12], то в якій би області перетворення контейнера не відбулися зміни, ці зміни позначаться на СНЧ и СНВ.

У [13] одержана формула енергії, яка виражається через СНЧ матриці контейнера, а саме: $E = \sigma_1^2 + ... + \sigma_n^2$, тобто енергія матриці контейнера дорівнює сумі квадратів СНЧ. Таким чином, справедлива рівність $E = \sum\sum c_{ij}^2 = \sigma_1^2 + \sigma_2^2 + ... + \sigma_n^2$, а це означає, що δ_1 і δ_2 обов'язково позначаться на сингулярному спектрі матриці контейнера. Норма матриці збурень $\|\Delta C\|_2$ не залежить від того, які саме СНЧ були збурені при СП, а залежить тільки від абсолютних величин цих збурень, тому в подальшому будемо використовувати саме СНЧ.

Як було показано вище, різні елементи роблять різний внесок у загальний рівень збурень контейнера, тому пропонується зробити попередню обробку контейнера з метою визначення коефіцієнтів μ_{ij} – кількісної оцінки внеску кожного елемента c_{ij} контейнера в $\|\Delta C\|_2$. Збурення елементів контейнера будемо моделювати зміною їх значень на найменш можливе, а саме на одиницю.

Основні кроки обчислення μ_{ij} і його використання:

1) збурити елемент c_{ij}, у результаті одержуємо матрицю $\overline{C}_{\sim ij}$, у якій значення усіх елементів збігається зі значеннями елементів матриці C, окрім одного, значення якого змінилося на одиницю;

2) для матриць C и $\overline{C}_{\sim ij}$ побудувати сингулярний розклад: $C = USV^T$, $\overline{C}_{\sim ij} = \overline{U}_{\sim ij}\overline{S}_{\sim ij}\overline{V}_{\sim ij}^T$;

3) знайти збурення матриці СНЧ: $\Delta S = S - \overline{S}_{\sim ij}$;

4) оцінити значення μ_{ij} за формулою $\mu_{ij} = \max_i |\Delta S_{ii}|$, де ΔS_{ij} – діагональні елементи матриці ΔS.

5) елементи контейнера, для яких виконується умова $\mu_{ij} \in [(\mu_{ij})_{\min}; P]$, використовувати для вбудовування повідомлення (P – деяке значення μ_{ij}, яке визначається з огляду на об'єм повідомлення);

6) для оцінки збурень контейнера внаслідок СП використовувати функцію $FS = \sum_{\mu_{ij} \in [(\mu_{ij})_{\min}; P]} \mu_{ij}$.

Розглянемо декілька додатків використання коефіцієнтів μ_{ij}. Одним з відкритих питань є порівняння ефективності стеганографічних алгоритмів. Для

порівняння декількох стеганографічних алгоритмів $CA_1,...,CA_n$ за критерієм збурень, потрібно визначити елементи, у яких локалізовано повідомлення для кожного, та виконати пункти 1) – 4). Для кожного з CA_i обчислити $FS_1 = \sum_{локализ.CA1} \mu_{ij}$,..., $FS_n = \sum_{локализ.CAn} \mu_{ij}$. Порівняння FS_i провести з огляду на те, що чим менші збурення були внесені в контейнер внаслідок СП, тим FS_i будуть меншими.

Для перевірки ефективності запропонованого методу алгоритмом CA_i модифікувалися елементи контейнера, яким відповідали найменші μ_{ij}, а алгоритмом CA_2 – усі інші. Одержані результати наведені в таблиці 1.

Таблиця 1

Порівняльна характеристика збурень контейнера

Об'єм вбудованого повідомлення	CA_1		CA_2	
	FS	$\|\Delta C\|_2$	FS	$\|\Delta C\|_2$
10 бітів	0,1903	1,4142	1,3362	2,1358
1/5 контейнера	32,4363	34,6888	85,9742	45,3085
1/2 контейнера	160,9376	49,3305	212,4801	65,8341

У [14] був запропонований стеганографічний алгоритм GRAPH_*matching*, у основу якого покладено побудову графової моделі контейнера. Вбудовування повідомлення відбувається за рахунок обміну елементів контейнера більшою мірою, ніж за рахунок їх модифікації, що дозволяє зберегти статистики першого порядку. Елементи контейнера розбиваються на групи, і кожній такій групі ставиться у відповідність вузол графа. Ребра між вузлами створюються тільки в тому випадку, якщо елемент одного вузла можна обміняти на елемент іншого без помітного спотворення контейнера. Оскільки вузли – це групи елементів, то ребер між вузлами може бути декілька, отже, може існувати декілька пар елементів, які можна обміняти. Цю ситуацію, із урахуванням описаного вище метода, будемо використовувати таким чином. Виконати попередню обробку контейнера, у результаті чого одержимо матрицю M коефіцієнтів μ_{ij}. Якщо вузлу інцидентно декілька ребер, то для обміну елементів c_{ij} і c_{kl} контейнера вибрати ту пару, якій відповідає найменша сума $\mu_{ij}+\mu_{kl}$.

Оцінка збурень контейнера, які відбулися внаслідок СП алгоритмом GRAPH_*matching* і його модифікованою версією GRAPH_*matching_1,* наведено в таблиці 2.

Таблиця 2

Порівняльна характеристика збурень контейнера $\|\Delta C\|_2$

Об'єм вбудованого повідомлення	GRAPH_*matching_1*	GRAPH_*matching*
10 бітів	0,4142	1,9358
1/5 контейнера	32,6878	46,3185
1/2 контейнера	50,5305	68,7341

Висновки

У роботі запропоновано метод оцінки збурень контейнера, який дозволяє мінімізувати ці збурення за рахунок визначення місця локалізації повідомлення, що вбудовується. Запропонований метод може використовуватися під час розробки нових стеганографічних алгоритмів, а також для порівняння різних стеганоалгоритмів з метою вибору кращого з них за критерієм мінімальності збурень, які вносяться у контейнер. Попередня обробка контейнера дозволяє вибрати із множини доступних контейнерів той, кількість елементів якого з малими коефіцієнтами μ_{ij} відповідають бажаному порогу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.

2. *Boris Ryabko, Daniil Ryabko.* Constructing perfect steganographic systems. Information and Computation 209 (2011). Pp. 1223–1230.

3. *Bohme R.* Advanced statistical steganalysis. Springer-Verlag, Berlin Heidelberg, 2010.

4. *T. Filler, J. Judas, J.* Fridrich Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. Forensics and Security, vol. 6(1). Pp. 920–935, 2011.

5. *J. Kodovskə, J. Fridrich, V.* Holub On Dangers of Overtraining Steganography to an Incomplete Cover Model. Proc. ACM Multimedia & Security Workshop, Niagara Falls, New York, September 29–30. Pp. 69–76, 2011.

6. *T. Filler, J.* Fridrich Gibbs construction in Steganography. Forensics and Security, 5(4). Pp. 705–720, 2010.

7. *Fridrich J., Filler T.* Practical methods for minimizing embedding impact in steganography. Proceedings SPIE, Electronic Imaging, Steganography, and Watermarking of Multimedia Contents IX. 2007. 6505. Pp. 2–3.

8 *Hetzl S., Mutzel P.* A graph-theoretic approach to steganography. Proc. Communication and Multimedia security. 2005. Pp. 119–128.

9. *Гонсалес Р.* Цифровая обработка изображений / пер. с англ. под ред. П.А. Чочиа. М.: Техносфера, 2006. 1070 с.

10. *Борисенко І.І.* Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. Сучасна спеціальна техніка. 2014. № 2(37). С. 110–115.

11. *Борисенко І.І.* Метод оцінки збурень контейнера внаслідок його стеганографічного перетворення. 10 МНПК Військова освіта і наука: сьогодення та майбутнє. 2014.

12. *Кобозева А.А.* Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. Информационные технологии и компьютерная инженерия. 2008. № 1 (11). С. 164–171.

13. *Кобозева А.А., Борисенко И.И.* Повышение помехоустойчивости стеганографических методов, использующих сингулярное и спектральное разложение матрицы контейнера. Труды Одесского политехнического университета. 2007. № 2(28). С. 192–198.

14. *Борисенко І.І.* Застосування теорії графів в задачах створення стеганографічних повідомлень. Сучасна спеціальна техніка. 2015. № 2. С. 26–33.

REFERENCES

1. *Gribunin, V.G., Okov, I.N., Turintsev, I.V.* (2002) Tsyfrovaia Steganografiia. "Digital Steganography". M.: Solon-Press. 272 p. [in Russian].
2. *Boris Ryabko, Daniil Ryabko* (2011) Constructing perfect steganographic systems. Information and Computation 209, Pp. 1223–1230 [in English].
3. *Bohme R.* (2010) Advanced statistical steganalysis. Springer-Verlag, Berlin Heidelberg [in English].
4. *T. Filler, J. Judas. J. Fridrich.* (2011) Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. Forensics and Security. Vol. 6(1). P. 920–935 [in English].
5. *J. Kodovskэ, J. Fridrich, V. Holub* (2011) On Dangers of Overtraining Steganography to an Incomplete Cover Model. Proc. ACM Multimedia & Security Workshop, Niagara Falls, New York, September 29–30. P. 69–76 [in English].
6. *T. Filler, J. Fridrich* (2010) Gibbs construction in Steganography. Forensics and Security 5*(4), 705–720* [in English].
7. *Fridrich, J., Filler, T.* (2007) Practical methods for minimizing embedding impact in steganography. Proceedings SPIE, Electronic Imaging, Steganography, and Watermarking of Multimedia Contents IX. 6505. P. 2–3 [in English].
8. *Hetzl, S., Mutzel, P.* (2005) A graph-theoretic approach to steganography. Proc. Communication and Multimedia security. P. 119–128 [in English].
9. *Gonsales, R., Vuds, R.* (2006) Tsifrovaia obrabotka izobrazhenii. "Didgital Processing of Inventions" / transl. P.A. Chochia. M.: Tekhnosfera. 1070 p. [in Russian].
10. *Borysenko, I.I.* (2014) Zastosuvannia metodiv porivniannia poslidovnostei v steganografichnykh peretvorenniakh tsyfrovykh zobrazhen. "Application of Sequence Comparison Methods in Steganographic Transformations of Digital Images". Modern Special Technics 2(37), 110 –115 [in Ukrainian].
11. *Borysenko, I.I.* (2014) Metod otsinky zburen konteinera vnaslidok yogo steganografichnogo peretvorennia. "Method for Estimating Container Perturbations due to Its Steganographic Transformation". 10 MNPK Military Education and Science: Present and Future [in Ukrainian].
12. *Kobozieva, A.A.* (2008) Zagalnyi pidkhid do otsinky vlastyvostei steganografichnogo algorytmu, zasnovanogo na teorii zburen. "A General Approach to Evaluating the Properties of a Steganographic Algorithm Based on Perturbation Theory". Information Technology and Computer Engineering 1 (11), 164–171 [in Ukrainian].
13. *Kobozeva, A.A,. Borysenko, I.I.* (2007) Povysheniie pomekhoustoichivosti steganograficheskikh metodov, ispolzuiushchikh singuliarnoie i spektralnoie razlozheniie matritsi konteinera. "Improvement of the Noise Immunity of Steganographic Methods Using Singular and Spectral Decomposition of the Container Matrix". Proceedings of the Odesa Polytechnic University 2 (28), 192–198 [in Russian] .
14. *Borysenko, I.I.* (2015) Zastosuvannia teorii grafiv v zadachakh stvorennia steganografichnykh povidomlen. "Application of Graph Theory in Problems of Creating Steganographic Messages". Modern Special Technics 2, 26–33 [in Ukrainian].

UDC 004.056.5

Borysenko Iryna,
Senior Lecturer, Odesa National Polytechnic University,
Odesa, Ukraine

ANALYSIS OF PERTURBATIONS OF THE CONTAINER AS THE BASIS OF THE METHOD OF EMBEDDING INFORMATION

The method of the quantitative assessment of perturbations of the container in case of its steganografic conversion which allows to create of more effective algorithms due to minimization of the impact of the built-in message on the container is offered.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.2(61).1
Issue 2(61) 2020 http://suchasnaspetstehnika.com/

First, container pre-processing is carried out in order to determine the coefficient - a quantitative assessment of the contribution of each specific element of the container in case the element is modified.

Finally, the coefficient of the container element is determined based on the singular numbers of the SVD container and stegocontainer.

The function allowing to make the analysis of the perturbations, arising in case of embedding of messages with different steganografic algorithms, that gives the opportunity to compare their efficiency is constructed.

Several applications of using the obtained container element coefficients are considered.

To test the effectiveness of the proposed method, the container elements, which correspond to the lowest coefficients, were modified by algorithm A1, and all the others were modified by algorithm A2. The results of a comparative analysis of container disturbances were in favor of algorithm A1.

The proposed method can be used in the development of new steganographic algorithms, as well as for comparing various steganoalgorithms in order to select the best of them according to the criterion of the minimum introduced disturbances in the container. Pre-processing of the container allows you to choose from the set of available containers the one, whose number of elements with small coefficients satisfies the desired threshold.

Keywords: embedded message, container perturbation, steganographic transformation, singular value.

Отримано 18.05.2020