

И.И. Борисенко, Одесса, Украина

## **ОЦЕНКА ВОЗМУЩЕНИЯ КОНТЕЙНЕРА ПРИ ЕГО СТЕГАНОПРЕОБРАЗОВАНИИ**

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

*Предложен метод количественной оценки возмущений контейнера при его стеганографическом преобразовании, который позволяет построить 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.*

*The method of the quantitative assessment of perturbations of the container in case of its steganographic conversion which allows to create more effective algorithms due to minimization of the impact of the built-in message on the container is offered. The function allowing to make the analysis of the perturbations, arising in case of embedding of messages different steganographic algorithms, that gives the opportunity to compare their efficiency is constructed. The results of numerical experiment confirm the efficiency of the proposed method.*

### **Введение**

Основной целью компьютерной стеганографии является сокрытие сообщения в некотором не привлекающем к себе внимания объекте – контейнере так, чтобы само его присутствие в контейнере не вызывало подозрения. В качестве сообщения может выступать любая конфиденциальная информация – личные или медицинские данные, банковская или коммерческая информация и т.д. Процесс встраивания сообщения в контейнер будем называть стеганографическим преобразованием (СП), а результат СП – стеганографическим сообщением или стеганоконтейнером [1, 2].

Как известно, стеганографическая система является совершенно стойкой (совершенно надежной) [2], если вероятностное распределение контейнера точно соответствует распределению стеганоконтейнера. Теоретически такие стеганосистемы для искусственных источников были построены [3].

Но, невозможно точно определить вероятностные распределения реальных контейнеров, в роли которых выступают цифровые медиа (звук, цифровые изображения, видео кадры) в силу сложности их структуры, поэтому совершенную стеганосистему на базе таких эмпирических источников построить нельзя [4]. В силу сказанного, построение защищенных стеганографических систем с использованием реальных контейнеров является открытым вопросом и требует дальнейшего исследования и развития.

### **Цель статьи и постановка задач**

Целью настоящей работы является разработка на основе ОПАИС [5] метода оценки возмущений матрицы контейнера при его стеганографическом преобразовании, который бы:

- 1) не зависел от используемого стеганографического алгоритма и области погружения сообщения;
- 2) позволял проводить сравнение уровня возмущений, вносимых различными стеганоалгоритмами.

Для достижения цели требуется решить следующие задачи:

- 1) исследовать возмущения, вносимые элементом контейнера при его модификации с целью определения количественной меры для оценки таких возмущений;
- 2) построить функцию для оценки возмущения матрицы контейнера при его стеганопреобразовании;
- 3) провести вычислительный эксперимент с целью проверки эффективности разработанного метода.

### **Основная часть**

В какой бы области (спектральной, пространственной и т.д.) преобразования матрицы контейнера не проводилось стеганопреобразование – это обязательно приведет к изменению значений элементов в пространственной области. В зависимости от того какие элементы подверглись модификации уровень возмущений матрицы контейнера будет неодинаковым. Рассмотрим это утверждение в формальном виде.

В качестве контейнера будем рассматривать цифровое изображение (ЦИ) с матрицей  $C=[c_{ij}]$  размерности  $m \times n$ . Рассмотрим два пикселя со значениями яркости  $K_1$  и  $K_2$  таких, что  $K_1 > K_2$ , изменим эти значения на +1 каждое (придадим элементам минимально возможное возмущение), а значения яркости остальных пикселей оставим без изменения. Может вначале показаться, что поскольку значения пикселей изменились на одну и ту же величину, то их вклад в изменения характеристик контейнера должен быть одинаков, но это не так. Например, как известно [6] одной из важных характеристик цифрового сигнала является его энергия. Для ЦИ энергия в

пространственной области вычисляется по формуле:  $E = \sum_i \sum_j c_{ij}^2$ . Тогда новое

значение энергии  $\bar{E} = E + \Delta E$  будет определяться формулой:  
 $\bar{E} = c_{11}^2 + c_{12}^2 + \dots + K_1^2 + 2K_1 + 1 + \dots + K_2^2 + 2K_2 + 1 + \dots + c_{mm}^2$ .

Приращение  $\Delta E = \delta_1 + \delta_2$  составляет сумма величин  $\delta_1 = 2K_1 + 1$  и  $\delta_2 = 2K_2 + 1$ , где  $\delta_1 > \delta_2$ . Следовательно, вклад пикселя со значением яркости  $K_1$  в  $\Delta E$  больше, чем вклад пикселя со значением яркости  $K_2$ .

В наше время активно развиваются методы стеганографии [7, 8] и стеганоанализа [9] базирующиеся на ОПАИС [5], в основу которого положен матричный анализ и теория возмущений. Преобразование контейнера за счет погружения в него сообщения, независимо от способа и области этого погружения, в соответствии с ОПАИС представляется как возмущение  $\Delta C$  матрицы  $C$ :  $\bar{C} = C + \Delta C$ , где  $\bar{C}$  – матрица стеганоконтейнера или в виде совокупности возмущений множества сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) матрицы контейнера, которые ее однозначно определяют [5]. Напомним, что для матрицы  $C$  сингулярное разложение (SVD) имеет вид:  $F = U \Sigma V^T$ , где  $U, V$  – ортогональные матрицы, т.е.  $U^T U = I, V^T V = I$  ( $I$  – единичная матрица) размерности  $m \times n$  и  $n \times n$  соответственно;  $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_n)$ ,  $\sigma_1 \geq \dots \geq \sigma_n \geq 0$ . Столбцы  $u_1, \dots, u_n$  матрицы  $U$  и  $v_1, \dots, v_n$  матрицы  $V$  называют соответственно левыми и правыми сингулярными векторами матрицы  $F$ , величины  $\sigma_1, \dots, \sigma_n$  – сингулярными числами.

Поскольку СНЧ и СНВ являются параметрами, которые однозначно характеризуют матрицу контейнера [5], то в какой бы области преобразования контейнера не произошли изменения, эти изменения обязательно отразятся на СНЧ и СНВ.

В [10] получена формула энергии, выраженная через СНЧ матрицы контейнера, а именно:  $E = \sigma_1^2 + \dots + \sigma_n^2$ , т.е. энергия матрицы контейнера равна сумме квадратов СНЧ. Таким образом, справедлива формула  $E = \sum_i \sum_j c_{ij}^2 = \sigma_1^2 + \sigma_2^2 + \dots + \sigma_n^2$ , а это означает, что  $\delta_1$  и  $\delta_2$  обязательно

отразятся в сингулярном спектре матрицы контейнера. Норма матрицы возмущений  $\|\Delta C\|_2$  не зависит от того, какие именно СНЧ были возмущены при стеганопреобразовании, а зависит только от абсолютных величин этих возмущений, поэтому в дальнейшем будем использовать именно СНЧ.

Как было показано выше, различные элементы вносят различный вклад в общий уровень возмущения контейнера, поэтому предлагается сделать предобработку контейнера с целью определения коэффициента  $\mu_{ij}$  –

количественной оценки вклада каждого конкретного элемента  $C_{ij}$  контейнера в  $\|\Delta C\|_2$  на случай, если элемент будет модифицирован. Возмущения элементов контейнера будем моделировать изменением их значений на наименее возможное, а именно на единицу.

Основные шаги вычисления  $\mu_{ij}$  и его использование:

1) возмутить элемент  $C_{ij}$ ; в результате получаем матрицу  $\bar{C}_{\sim ij}$ , в которой значения всех элементов совпадают со значениями элементов матрицы  $C$ , кроме одного, значение которого изменилось на единицу;

2) для матриц  $C$  и  $\bar{C}_{\sim ij}$  построить сингулярное разложение:  $C = USV^T$ ,  $\bar{C}_{\sim ij} = \bar{U}_{\sim ij} \bar{S}_{\sim ij} \bar{V}_{\sim ij}^T$ ;

3) найти возмущение матрицы СНЧ:  $\Delta S = S - \bar{S}_{\sim ij}$ ;

4) оценить значение  $\mu_{ij}$  по формуле  $\mu_{ij} = \max_i |\Delta S_{ii}|$ , где  $\Delta S_{ii}$  – диагональные элементы матрицы  $\Delta S$ .

5) элементы контейнера, для которых выполняется условие  $\mu_{ij} \in [(\mu_{ij})_{\min}; P]$ , использовать для встраивания сообщения ( $P$  – некоторое значение  $\mu_{ij}$ , которое определяется исходя, например, из объема сообщения);

6) для оценки возмущений контейнера вследствие стеганопреобразования использовать функцию  $FS = \sum_{\mu_{ij} \in [(\mu_{ij})_{\min}; P]} \mu_{ij}$ .

Рассмотрим несколько приложений использования коэффициентов  $\mu_{ij}$ . Одним из открытых вопросов является сравнение эффективности стеганографических алгоритмов. Для сравнения нескольких стеганографических алгоритмов  $CA_1, \dots, CA_n$  по критерию вносимых возмущений следует выполнить пункты 1) – 4). Далее определить элементы контейнера, в которых локализовано сообщение. Для определенных элементов вычислить  $FS_1 = \sum_{\text{локализ. } CA_1} \mu_{ij}$ , ...,  $FS_n = \sum_{\text{локализ. } CA_n} \mu_{ij}$ . Сравнение  $FS_i$

провести исходя из того, что чем меньшие возмущения были внесены в контейнер вследствие СП, тем  $FS_i$  будут меньше.

Для проверки эффективности предложенного метода алгоритмом  $CA_1$  модифицировались элементы контейнера, которым соответствовали наименьшие  $\mu_{ij}$ , а алгоритмом  $CA_2$  – все остальные. Полученные результаты приведены в табл. 1.

Таблица 1 – Сравнительная характеристика возмущений контейнера

Объем встроенного сообщения	$CA_1$		$CA_2$	
	$FS$	$\ \Delta C\ _2$	$FS$	$\ \Delta C\ _2$
10 битов	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

В [11] был предложен стеганографический алгоритм *GRAPH\_matching*, в основу которого положено построение графовой модели контейнера. Встраивание сообщения происходит за счет обмена элементов контейнера в большей степени, чем за счет их корректировки, что позволяет сохранить статистики первого порядка. Элементы контейнера разбиваются на группы и каждой такой группе ставится в соответствие узел графа. Ребра между узлами создаются только в том случае, если элемент одного узла можно обменять на элемент другого без видимого искажения контейнера. Поскольку узлы – это группы элементов, то ребер между узлами может быть несколько, следовательно, существует несколько пар элементов, которые можно обменять. Эту ситуацию, с учетом изложенного выше метода, будем использовать следующим образом. Выполнить предобработку контейнера, в результате чего получим матрицу  $M$  коэффициентов  $\mu_{ij}$ . Если узлу инцидентно несколько ребер, то для обмена элементов  $C_{ij}$  и  $C_{kl}$  контейнера выбрать ту пару, которой соответствует наименьшая сумма  $\mu_{ij} + \mu_{kl}$ .

Оценка возмущений контейнера, которые вызваны стеганопреобразованием алгоритмом *GRAPH\_matching* и его модифицированной версией *GRAPH\_matching\_1* приведена в табл. 2.

Таблица 2 – Сравнительная характеристика возмущений контейнера  $\|\Delta C\|_2$

Объем встроенного сообщения	<i>GRAPH_matching_1</i>	<i>GRAPH_matching</i>
10 бітів	0,4142	1,9358
1/5 контейнера	32,6878	46,3185
1/2 контейнера	50,5305	68,7341

Полученные результаты свидетельствуют о наличии эффекта от применения предобработки матрицы контейнера.

**Выводы.** В работе предложен метод оценки возмущений контейнера, который позволяет минимизировать эти возмущения за счет определения места локализации встраиваемого сообщения во время стеганопреобразования. Предложенный метод может использоваться при разработке новых стеганографических алгоритмов, а также для сравнения различных стеганоалгоритмов с целью выбора лучшего из них по критерию минимальности вносимых возмущений в контейнер. Предварительная обработка контейнера позволяет выбрать из множества доступных контейнеров тот, количество элементов которого с малыми коэффициентами  $\mu_{ij}$  удовлетворяет желаемому порогу.

**Список использованных источников:** 1. Хорошко В.О., Азаров О.Д и др. Основи комп'ютерної стеганографії : Навчальний посібник для студентів і аспірантів. – Вінниця: ВДТУ, 2003. – 143 с. 2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с. 3. Boris Ryabko, Daniil Ryabko Constructing perfect steganographic systems// Information and Computation 209 (2011) 1223–1230. 4. Böhme R. Advanced statistical steganalysis. Springer-Verlag, Berlin Heidelberg, 2010. 5. Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / А.А. Кобозева // Інформаційні технології та комп'ютерна інженерія. – 2008. – №1 (11). – С.164-171. 6. Гонсалес Р. Цифровая обработка изображений / Р.Гонсалес, Р.Вудс; пер. с англ. под ред. П.А.Чочиа. — М.: Техносфера, 2005. – 1072 с. 7. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень / І.І. Борисенко // Сучасна спеціальна техніка. – 2014. – №2 (37). – С. 110-115. 8. Борисенко І.І. Метод оцінки збурень контейнера внаслідок його стеганографічного перетворення / І.І. Борисенко // 10 МНПК Військова освіта і наука: сьогодні та майбутнє. – 2014. 9. Бобок І.І. Использование метода анализа ROC-кривых для комплексной оценки эффективности стеганоаналитического метода / И.И. Бобок // Информатика и математические методы в моделировании. – 2012. – №3 – С. 221-229. 10. Кобозева А.А. Повышение помехоустойчивости стеганографических методов, использующих сингулярное и спектральное разложение матрицы контейнера/ А.А. Кобозева, И.И. Борисенко // Труды одесского политехнического университета. – 2007. – №2 (28). – С. 192-198. 11. Борисенко І.І. Застосування теорії графів в задачах створення стеганографічних повідомлень / І.І. Борисенко // Сучасна спеціальна техніка. – 2015. – №2.

**Bibliography (transliterated):** 1. Horoshko B.O., Azarov O.D i dr. Osnovi komp'yuternoi steganografii : Navchal'nyj posibnik dlja studentiv i aspirantiv. – Vinnicia: VDTU, 2003. – 143 s. 2. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaja steganografija. – M.: Solon-Press, 2002. – 272 s. 3. Boris Ryabko, Daniil Ryabko Constructing perfect steganographic systems// Information and Computation 209 (2011) 1223–1230. 4. Böhme R. Advanced statistical steganalysis. Springer-Verlag, Berlin Heidelberg, 2010. 5. Kobozeva A.A. Zagal'nij pidhid do ocinki vlastivostej steganografichnogo algoritmu, zasnovanij na teorii zburen' / A.A. Kobozeva // Informacionnye tehnologii i komp'yuternaja inzhenerija. – 2008. – №1 (11). – S.164-171. 6. Gonsales R. Cifrovaja obrabotka izobrazhenij / R.Gonsales, R.Vuds; per. s angl. pod red. P.A.Chochia. — M.: Tehnosfera, 2005. – 1072 s. 7. Borisenko I.I. Zastosuvannja metodiv porivnannja poslidovnostej v steganografichnih peretvorennyah cifrovih zobrazen' / I.I. Borisenko // Suchasna special'na tehnika. – 2014. – №2 (37). – S. 110-115. 8. Borisenko I.I. Metod ocinki zburen' kontejnera vnaslidok jogo steganografichnogo peretvorennja / I.I. Borisenko // 10 MNPK Vijs'kova osvita i nauka: s'ogodennja ta majbutne. – 2014. 9. Bobok I.I. Ispol'zovanie metoda analiza ROC-kryvih dlja kompleksnoj ocenki jeffektivnosti steganoanaliticheskogo metoda / I.I. Bobok // Informatika i matematicheskie metody v modelirovanii. – 2012. – №3 – S. 221-229. 10. Kobozeva A.A. Povyshenie pomehoustojchivosti steganograficheskikh metodov, ispol'zujushih singularnoe i spektral'noe razlozhenie matricy kontejnera/ A.A. Kobozeva, I.I. Borisenko // Trudy odesskogo politehnicheskogo universiteta. – 2007. – №2 (28). – S. 192-198. 11. Borisenko I.I. Zastosuvannja teorii grafiv v zadachah stvorennja steganografichnih povidomlen' / I.I. Borisenko // Suchasna special'na tehnika. – 2015. – №2.