**УДК 004.056.5**

# СТЕГАНОГРАФИЧЕСКИЙ АЛГОРИТМ ДЛЯ КОНТЕЙНЕРОВ-ИЗОБРАЖЕНИЙ, УСТОЙЧИВЫЙ К АТАКЕ СЖАТИЕМ

М. А. Мельник

Одесский национальный политехнический университет
Украина, г. Одесса
RITOCHEK@yandex.ua

*На основе формального представления стеганопреобразования как совокупности возмущений сингулярных чисел матриц, отвечающих контейнеру, разработан стеганографический алгоритм, устойчивый к сжатию с большими коэффициентами. В качестве контейнера рассматривается цифровое изображение.*

*Ключевые слова: стеганографический алгоритм, атака сжатием, цифровое изображение, сингулярное число, матрица.*

Проблема создания стеганографических алгоритмов (СА), устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов, является актуальной, но не решенной на сегодняшний день. Чаще всего существующие СА такого плана осуществляют погружение дополнительной информации (ДИ), результатом чего является стеганосообщение (СС), в частотной области контейнера и, при условии обеспечения надежности восприятия СС, выдерживают лишь незначительное сжатие [1]. Таким образом, актуальным остается поиск новых путей для разработки СА, устойчивых к сжатию со значительными коэффициентами.

Основным математическим инструментом, используемым в работе, является общий подход к анализу состояния и технологии функционирования произвольной информационной системы (ОПАИС) [2]. В качестве контейнера рассматривается цифровое изображение (ЦИ).

Цель работы – разработка нового СА, устойчивого к сжатию со значительными коэффициентами, на основе формального представления стеганопреобразования (СП) как совокупности возмущений сингулярных чисел (СНЧ) матриц, отвечающих контейнеру, обеспечивающих нечувствительность (малую чувствительность) формируемого СС к сжатию.

Для достижения поставленной цели в работе были решены следующие задачи.

1. Проведен анализ поведения СНЧ-матриц, отвечающих ЦИ, в процессе его сжатия с различными коэффициентами качества с целью выделения подмножества СНЧ, возмущения которых, рассматриваемые как результат процесса СП, принципиально могут привести к СС, нечувствительному к сжатию.

2. Получены формальные достаточные условия устойчивости СА к сжатию со значительными коэффициентами путем адаптации ОПАИС в область стеганографии.

3. Разработан СА, удовлетворяющий достаточным условиям устойчивости к сжатию.

Тестирование разработанного СА проводится путем вычислительного эксперимента в среде Matlab, при этом атака сжатием моделируется путем пересохранения СС в Adobe Photoshop в формат JPEG с различными коэффициентами качества $Q$. В качестве ДИ рассматривается последовательность $p_1, p_2, \ldots, p_t$, где $p_i \in \{0,1\}$, $i = 1,2, \ldots t$. В работе установлено пороговое значение вариации возмущений максимальных СНЧ $K = 200$. Основные шаги алгоритма выглядят следующим образом.

*Шаг 1*. Матрица $F$ контейнера разбивается стандартным образом на блоки $B$ размером $8 \times 8$.

*Шаг 2*. Погружение бита ДИ. $B$ — очередной блок контейнера, $p_i$ — очередной бит ДИ.

2.2. Строится сингулярное разложение $B = U\Sigma V^T$, где $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_8)$;

2.3. *Если* $p_i = 0$, *то* $\sigma_1$ корректируется так, чтобы разность между $\sigma_1$ и $\sigma_2$ при делении

на $K$ давала остаток $K/4$. Результат корректировки – возмущенное максимальное СНЧ $\overline{\sigma}_1$; иначе — $\sigma_1$ корректируется так, чтобы разность между $\sigma_1$ и $\sigma_2$ при делении на $K$ давала остаток $3K/4$. Результат — $\overline{\sigma}_1$.

*Шаг 3*. Формирование блока СС $\overline{F}$. Блок СС $\overline{B}$: $\overline{B} = U\overline{\Sigma}V^T$, где $\overline{\Sigma} = diag\left(\overline{\sigma}_1, \sigma_2, \ldots, \sigma_8\right)$.

Алгоритм для декодирования ДИ выглядит следующим образом.

*Шаг 1*. Матрица $\overline{F}$ СС разбивается стандартным образом на блоки $\overline{B}$ размером $8 \times 8$.

*Шаг 2*. Декодирование бита ДИ. $\overline{B}$ — очередной блок, из которого извлекается бит $p_i$ ДИ.

2.2. Строится сингулярное разложение $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$, где $\overline{\Sigma} = diag\left(\overline{\sigma}_1, \overline{\sigma}_2, ..., \overline{\sigma}_8\right)$;

2.3. Если разность $\overline{\sigma}_1 - \overline{\sigma}_2$ при делении на $K$ дает остаток меньше $K/2$, *то* $p_i = 0$; иначе — $p_i = 1$.

Результаты лабораторного тестирования разработанного алгоритма приведены в табл.1.

Зависимость объема восстановленной ДИ от значения $Q$ при сжатии СС

| Формат хранения ЦИ | Среднее значение объема восстановленной при декодировании ДИ, % | | |
|---|---|---|---|
| | $Q = 12$ | $Q = 7$ | $Q = 3$ |
| Tif | 98,97 | 98,07 | 92,13 |
| JPEG | 98,54 | 98,11 | 91,06 |

Таким образом, в работе предложен новый подход к проблеме обеспечения СА устойчивости к атаке сжатием, основанный на ОПАИС. Установлено, что СП достаточно проводить таким образом, чтобы его формальным представлением была совокупность $S$ возмущений СНЧ-блоков матрицы контейнера, удовлетворяющая условиям: если для сжатия СС предполагается использование высоких коэффициентов качества, то $S$ не должна содержать возмущений наименьших СНЧ; если для СС предполагается использование сжатия с низким коэффициентом качества, то $S$ должна содержать возмущения только максимальных СНЧ-блоков. Полученные достаточные условия не зависят от используемой для погружения ДИ области контейнера и конкретики СА, а определяются лишь локализацией и относительной величиной возмущений СНЧ соответствующих матриц контейнера, произошедших в ходе СП. На основе полученных достаточных условий в работе разработан новый СА, устойчивый к сжатию даже с малыми коэффициентами качества: для $Q = 3$ среднее значение объема восстановленной информации составило $91{,}5\%$, что говорит о перспективности использования предложенного нового подхода, основанного на ОПАИС.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стеганоанализ.— Москва: Вузовская книга, 2009.

2. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности.— Киев: Изд. ГУИКТ, 2009.

---

M. A. Melnyk

**Compressive-stable steganoalgorithm for digital images.**

A new approach to solving a problem of steganography algorithm stability to cover-attack is proposed. The algorithm is based on the general approach to analysis of state and functioning of information system. The proposed approach automates the process of analyzing the existing or emerging steganography algorithms from the viewpoint of its resistance to compression.

Keywords: *steganoalgorithm, compression attacks, digital image, singular value, matrix.*