УДК 004.056.5

АНАЛИЗ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА, ОСНОВАННОГО НА ИСПОЛЬЗОВАНИИ ПРЕОБРАЗОВАНИЯ АРНОЛЬДА

Н. В. Калашников, А. А. Яковенко, Н. И. Кушниренко, Е. П. Соколовская

Одесский национальный политехнический университет
Украина, г. Одесса
kalashnikov_n.v@ukr.net

Рассмотрен метод стеганографического сокрытия данных, основанный на использовании преобразования Арнольда и ДКТ-преобразования. Проанализированы некоторые виды атак на изображение-контейнер, а также возможность их предотвращения либо уменьшения вероятности их успешного проведения.

Ключевые слова: стеганография, сокрытие данных, преобразование Арнольда, ДКП.

Метод смешивания коэффициентов ДКП обеспечивает ряд преимуществ по сравнению с иными широко распространенными стеганографическими алгоритмами (Коха—Жао, Куттера—Джордана—Боссена), а именно высокую пропускную способность, относительную простоту реализации. В то же время, данный метод позволяет использовать в качестве секретного сообщения (СС) исключительно изображение, требует наличия у получателя пустого стеганографического контейнера (СК).

Существует стеганографический алгоритм (СА), осуществляющий сокрытие данных путем скремблирования СС с использованием преобразования Арнольда (ПА) [1] и смешивания коэффициентов ДКП и СС после скремблирования. Для считывания СС получателю должны быть известны пустой СК, количество итераций ПА N, коэффициент смешивания коэффициентов ДКП α [2].

Цель работы — анализ данного СА [2], некоторых возможных атак (нарушение передачи СС либо его обнаружение) [3] на данный алгоритм и требуемых модификаций СА для невозможности их успешного проведения.

В данной работе были решены следующие задачи.

1. Произведен анализ алгоритма с целью выявления некоторых возможных атак.
2. Произведено практическое тестирование осуществимости данных атак.
3. Разработаны модификации алгоритма для невозможности успешного проведения данных атак.

Тестирование производится путем моделирования в среде математических вычислений Matlab. В качестве СК и СС используются полутоновые изображения размером 256×256 (рис. 1, *a* и *b*). Коэффициент смешивания коэффициентов ДКП $\alpha = 0{,}85$, количество итераций ПА $N = 37$.

Атака 1. Циклический сдвиг строк либо столбцов СК. При этом СС подвергается значительным искажениям. СС после атаки при количестве сдвигаемых столбцов $M = 10$ показано на рис. 1, *c*.

Модификация 1. Поскольку у получателя имеется пустой СК, возможно восстановление полученного контейнера со сдвигом. Для этого производится итеративный циклический сдвиг строк и столбцов принятого СК с вычислением значения функции взаимной корреляции пустого СК и СК с СС. Корреляционный максимум будет соответствовать отсутствию сдвига СК. Для определения направления сдвига при восстановлении СК возможно использование метода градиентного спуска.

Атака 2. Стеганоанализ СА путем обнаружения и восстановления секретного изображения при помощи обратного ПА, производимого над СК. Поскольку ПА является циклическим, осуществление N итераций модифицированного ПА [1], где N – количество итераций ПА при скремблировании СС отправителем, дескремблирует СС даже без извлечения из контейнера и тем самым проявит СС. Реализуется путем итеративного преобразования Арнольда над контейнером, при каждой итерации выполняется БПФ контейнера. Наличие максимума в НЧ-области будет означать обнаружение скрытого изображения – секретного сообщения (рис. 1, *f*). Для улучшения качества восстанавливаемого изображения может использоваться адаптивное выравнивание гистограммы и фильтрация (рис. 1, *d*).

Модификация 2. Перед ПА к секретному сообщению отправителем прибавляется поэлементное произведение квадратной матрицы констант и матрицы Адамара соответствующей размерности по модулю 255. При этом вносимые искажения незначительны, а успешный анализ СК становится невозможным.

Атака 3. На заполненный СК повторно накладывается заполненный СК, предварительно скремблированный произвольным числом итераций ПА N^*, при помощи смешивания коэффициентов ДКП при коэффициенте смешивания $0{,}8 \le \alpha \le 0{,}85$. Данная атака не приводит к значительным искажениям результирующего СК, однако вызывает неустранимые искажения СС (рис. 1, *e*).

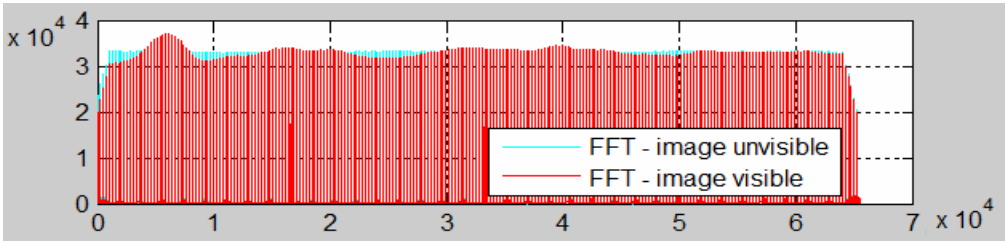
Невозможно предотвращение подобной атаки. Обратное преобразование практически неосуществимо, поскольку параметры N^* и α неизвестны получателю сообщения.

Результаты лабораторного тестирования приведены в таблице и на рис. 1.

Искажения СК и СС при некоторых атаках

Название показателя искажения	СС, атака 1	СС, модификация 2	СК, атака 3	СС, атака 3
Максимальное отношение «сигнал/шум»	14,571	8,245	6,598	3,519
Нормальная среднеквадратическая ошибка	0,034	0,150	0,219	0,445

a). СК b) СС c) СС после атаки 1 d) результат атаки 2 e) СС после атаки 3



f) сравнение коэффициентов FFT до и после модификации 2

Рис. 1. Результаты моделирования атак

Таким образом, в данной работе были рассмотрены некоторые возможные атаки на СА, разработаны соответствующие модификации СА. В то же время, атака повторным наложением не позволяет осуществить восстановление СС.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Min Li, Ting Liang, Yu-jie He. Arnold transform based image scrambling method // 3rd International Conference on Multimedia Technology.— 2013.

2. Jie Yang . Algorithm of image information hiding based on new anti-arnold transform and blending in DCT domain. // IEEE 12th International Conference on Communication Technology.— 2010.

3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография.— Киев: МК-Пресс, 2006.

N. V. Kalashnikov, A. A. Iakovenko, N. I. Kushnirenko

Analysis of steganographic algorithm, based on using Arnold transformation.

A steganography method based on using Arnold transform and DCT transform was considered. Some possible types of attacks on the image container were analyzed, as well as the possibility to prevent the attacks or reduce the likelihood of their success.

Keywords: *steganography, data hiding, Arnold transform, DCT.*