УДК 004.056.5

И. И. БОБОК, канд. техн. наук,
Одесский национальный политехнический университет;
О. В. КОСТЫРКА, аспирант,
Академия пожарной безопасности им. Героев Чернобыля, Черкассы

АНАЛИЗ УСТОЙЧИВОСТИ НОВОГО СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К СТЕГАНОАНАЛИТИЧЕСКИМ АТАКАМ

Рассмотрена эффективность детектирования нового стеганографического алгоритма, производящего вложение дополнительной информации в пространственной области контейнера-изображения, при помощи современных стеганоаналитических комплексов. Показана устойчивость анализируемого алгоритма к стеганоанализу. Продемонстрирована зависимость эффективности стеганоаналитических программных комплексов от значения показателя качества цифровых изображений. Приведены результаты вычислительных экспериментов.

Ключевые слова: стеганография; стеганоанализ; эффективность детектирования.

Введение

Трагические события 11 сентября 2001 г., повлекшие за собой ограничение, а в некоторых странах, в том числе и в Украине, запрет шифрования на законодательном уровне, привели к значительной активизации разработок в области стеганографии. В свою очередь, на фоне активизации научной деятельности в области стеганографии, многочисленных публикаций новых результатов в открытой печати появились дополнительные возможности использования получаемых разработок различными антигосударственными, террористическими структурами. В силу сказанного симметричным ответом стало развитие разработок в направлении повышения эффективности стеганоанализа.

Сегодня стеганографический алгоритм может позиционироваться как эффективный только в том случае, если он является устойчивым к стеганоанализу. Следовательно, вопрос оценки такой устойчивости актуален для каждого стеганометода и алгоритма.

Постановка задачи

В [1] авторами был предложен новый стеганографический метод, получивший свою реализацию в виде устойчивого к возмущающим воздействиям алгоритма *SA*, который осуществляет погружение дополнительной информации в пространственной области изображения-контейнера и основан на ***достаточном условии*** такой устойчивости, полученном в [2]. Достаточное условие обеспечивается благодаря организации стеганопреобразования корректировкой яркости пикселей $l \times l$-блоков матрицы цифрового изображения-контейнера. Разбиение на блоки осуществляется стандартным образом. Корректировка на значение $\pm\Delta b$ осуществляется при погружении в очередной блок B очередного бита дополнительной информации. При этом Δb должно удовлетворять следующему условию:

$$|\Delta b| = \left|\frac{\Delta\sigma_1}{l}\right| > \frac{\left\|\Delta\overline{B}\right\|_2}{l},$$

где $\Delta\sigma_1$ — возмущение максимального сингулярного числа блока B при стеганопреобразовании; $\left\|\Delta\overline{B}\right\|_2$ — спектральная норма матрицы предполагаемого возмущения блока стеганосообщения.

Декодирование дополнительной информации в *SA* после предварительного разбиения матрицы стеганосообщения и контейнера на $l \times l$-блоки соответственно $\overline{\overline{B}}$ и B сводится к сравнению количества положительных и отрицательных элементов в матрице $\Delta B = \overline{\overline{B}} - B$.

Согласно сказанному ***целью статьи является исследование устойчивости алгоритма SA к стеганоанализу, проводимому современными программными комплексами.***

Для достижения поставленной цели необходимо решить следующие три задачи.

1. Для всестороннего анализа рассматриваемого алгоритма выделить среди современных стеганоаналитических комплексов те, которые имеют разные математические основы, используют разные математические инструменты.

2. Определить слабые места в построении и функционировании современных стеганоаналитических комплексов.

3. Провести вычислительный эксперимент и получить числовые характеристики эффективности стеганоанализа для исследуемого стеганографического алгоритма.

Основная часть

Стеганоанализ сегодня развивается в двух основных направлениях. Во-первых, это создание алгоритмов, позволяющих детектировать результаты работы *конкретных* стеганографических методов, а во-вторых, разработка так называемых *универсальных*, или *слепых* (*blind*), методов, позволяющих на основании выявления или кон-

статации отсутствия определенных характерных признаков в анализируемом контенте делать вывод об осуществленном внедрении конфиденциальной информации или об отсутствии такового, не привязываясь к конкретике использованного стеганографического алгоритма [3].

В процессе достижения поставленной цели первоначально была проведена серия экспериментов с использованием 250 цифровых изображений размером 1000×1000 пикселей (цветовая схема RGB) в формате JPEG из базы изображений NRCS [4], а также фотографий, полученных непрофессиональными фотографами. Погружение дополнительной информации происходило в синюю составляющую изображения-контейнера. С учетом того, что, как показано в [5], алгоритм *SA* является устойчивым к сжатию, стеганосообщения были сохранены в формате JPEG с различными (от 50 до 100 с шагом 10) коэффициентами качества (*quality factor* — QF), после чего подвергались стеганоанализу.

Использованные стеганоаналитические комплексы представлены следующими продуктами:

- CANVASS 1.0 (разработка 2009 г.);
- StegAlyzerSS 3.0 (2007 г.);
- Stegdetect 0.6.3 (2004 г.).

Данные стеганоаналитические комплексы являются широко используемыми, современными и доступными для свободного (неправительственного) применения, кроме того, как будет показано далее, они отличаются своими математическими основами.

Результаты эксперимента

Наихудшие результаты показал ***StegAlyzerSS*** [6], или *Steganography Analyzer Signature Scanner*. Этот комплекс не смог осуществить детектирование вложений ни в одной из групп изображений с различным QF.

На первый взгляд, результат кажется фантастическим, однако, если разобраться в принципе работы сканера, то можно понять, что объяснение данного факта лежит на поверхности.

Представленный программный продукт является *сигнатурным сканером*. Это означает, что принцип его работы базируется на поиске масок и сигнатур различных известных на данный момент стеганографических методов и алгоритмов. Таким образом, любой новый стеганоалгоритм, не внесенный еще в базы компании-производителя, будет «не замечен» данным программным комплексом.

Этим примером авторы настоящей статьи хотели бы обратить внимание научной общественности на бессмысленность дальнейших разработок сигнатурных сканеров для решения задач стеганоанализа. Будущее стеганоанализа может быть связано только со «слепыми» методами, сигнатурные же методы обречены на вечную роль «догоняющего» в гонке с разработчиками стеганографических алгоритмов.

Следующей была проанализирована работа программного комплекса ***Stegdetect***, разработанного в 2000-х гг. Н. Провосом. Данный комплекс способен обнаруживать скрытую информацию в изображениях JPEG-формата, внедренную различными известными алгоритмами стеганографии (например, jsteg, jphide, F5 и т. д.), а также автоматически обнаруживать новые методы стеганографии при помощи линейного дискриминантного анализа [7].

Результаты работы этого комплекса, как и остальных, приведены в таблице. Эффективность детектирования (здесь и далее под эффективностью детектирования будет пониматься доля в процентах верно детектированных стеганосообщений от общего числа анализируемых) данного комплекса ни в одной из групп не превысила 13%.

Эффективность детектирования нового стеганографического алгоритма современными стеганоаналитическими комплексами

Стеганоаналитический комплекс	Эффективность детектирования, %					
	QF = 50	QF = 60	QF = 70	QF = 80	QF = 90	QF = 100
Canvass	83,6	83,1	72,6	37,2	9,1	1,8
Stegdetect	0	1,6	0,5	13,5	3,1	1
StegAlyzerSS	0					

Низкий уровень детектирования данным стеганоаналитическим комплексом, по-видимому, связан с использованием *линейного дискриминантного анализа* для классификации изображений.

Линейный дискриминантный анализ — методы статистики и машинного обучения, применяемые для нахождения линейных комбинаций признаков, наилучшим образом разделяющих два или более классов объектов или событий. Полученная комбинация может быть использована в качестве линейного классификатора или для сокращения размерности пространства признаков перед последующей классификацией.

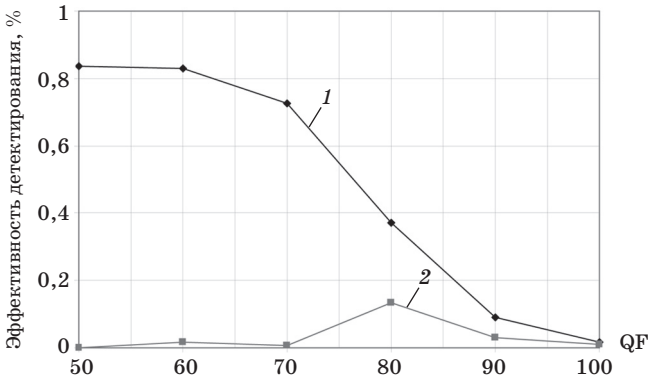
Линейный дискриминантный анализ для случая двух классов (а именно это и ставится в задачу стеганоаналитического комплекса — отделить стеганограммы от пустых контейнеров) осуществляется следующим образом: для каждого образца объекта или события с известным классом *y*

рассматривается набор наблюдений x (называемых еще признаками, переменными или измерениями). Набор таких образцов называется ***обучающей выборкой***. Задача классификации состоит в том, чтобы построить хороший прогноз класса y для всякого так же распределенного объекта (не обязательно содержащегося в обучающей выборке), имея только наблюдения x [8].

Таким образом, чем больше количество наблюдений, тем, вероятно, более эффективной будет работа данного стеганоаналитического программного продукта. Этот факт не может быть оценен нами как достоинство, это скорее — недостаток.

Следующей была проанализирована работа программного комплекса ***Canvass***, основанного на частично упорядоченных марковских моделях, которые использованы для метода опорных векторов [9]. Эффективность упомянутого комплекса самая высокая из всех рассматриваемых в данной работе, однако, как следует из таблицы, максимум эффективности достигается при QF от 50 до 70. При высоком качестве стеганограмм данный программный комплекс не особо выделяется на фоне рассмотренного ранее комплекса Stegdetect (см. рисунок). Эффективность детектирования для группы QF = 75 будет примерно на уровне 50%, что соответствует в бинарном классификаторе случайному отнесению объекта к тому или иному классу.

Авторы настоящей статьи считают, что использования JPEG с низким QF является неоправданным. Во-первых, нарушается восприятие даже изображений-контейнеров, а во-вторых, наличие артефактов, особенно на фоновой составляющей, излишне привлекает внимание.



Зависимость эффективности детектирования нового стеганографического алгоритма от показателя качества JPEG для двух комплексов: CANVASS (линия *1*) и Stegdetect (линия *2*)

Выводы

Рассмотрены три программных продукта — стеганоаналитические комплексы, недостатки которых могут быть отнесены к работе и других комплексов, так как принципы их функционирования остаются практически неизменными.

В представленной работе продемонстрирована устойчивость нового стеганографического алгоритма к стеганоаналитическим атакам современными программными комплексами. Полученные результаты свидетельствуют о следующем.

1. Разработанный алгоритм не имеет аналогов в базах сигнатур стеганоаналитических комплексов, осуществляющих определение наличия вложения по маске используемого алгоритма.

2. Обучаемость стеганоаналитических комплексов (что касается как линейного дискриминантного анализа, так и метода опорных векторов) требует для своей реализации наличия постоянно действующего стеганографического канала, что на практике не только часто не реализуемо, но и является малоэффективным с точки зрения поддержания скрытности и безопасности самого канала.

3. Для высококачественных JPEG изображений с QF выше 90 эффективность детектирования не превышает 10%.

Целью дальнейших исследований может стать установление зависимости эффективности детектирования от объема вложенной дополнительной информации, что позволит дать ответ на вопрос о максимальной скрытой пропускной способности нового стеганографического алгоритма.

Литература

1. ***Рудницький, В. М.*** *Стійке стеганоперетворення в просторовій області зображення-контейнера / В. М. Рудницький, О. В. Костирка // Інформатика та математичні методи в моделюванні.— 2013.— Т. 3, № 4.— С. 320–327.*

2. ***Кобозева, А. А.*** *Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А. А. Кобозева, О. В. Костырка // Інформаційна безпека.— 2013.— №4.— С. 57–65.*

3. ***Бобок, И. И.*** *Метод повышения эффективности детектирования вложения конфиденциальной информации: дис. ... канд. техн. наук – 05.13.21 «Системы защиты информации» / И. И. Бобок.— Одесса, 2013.— 136 с.*

4. ***NRCS*** *Photo Gallery [Электронный ресурс] // United States Department of Agriculture. Washington, USA.— Режим доступа:*

http://photogallery.nrcs.usda.gov (Дата обращения: 26.01.2014).

5. ***Рудницкий, В. Н.*** *Стеганопреобразование пространственной области изображения-контейнера, устойчивое к сжатию / В. Н. Рудницкий, М. А. Мельник, О. В. Костырка // Сучасна спеціальна техніка.— 2014.— № 1.— С. 38–44.*

6. ***Steganography*** *Analyzer Signature Scanner (StegAlyzerSS) [Электронный ресурс] // SARC: Steganography Analysis and Research Center. Fairmont, USA.— Режим доступа:*

http://www.sarc-wv.com/products/stegalyzerss/ (Дата обращения: 26.01.2014).

7. Steganography Detection with Stegdetect [Электронный ресурс] // OutGuess org by Niels Provos.— Режим доступа:

http://www.outguess.org/detection.php (Дата обращения: 26.01.2014).

*8. **Линейный** дискриминантный анализ [Электронный ресурс] // MachineLearning.ru — Профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных.— Режим доступа:*

http://www.machinelearning.ru/wiki/index.php?title=Линейный_дискриминантный_анализ (Дата обращения: 26.01.2014).

*9. **Jalan, J.** Feature selection, statistical modeling and its applications to universal JPEG steganalyzer [Электронный ресурс] // Digital Repository @ Iowa State University. USA.— Режим доступа:*

http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2039&context=etd (Дата обращения: 26.01.2014).

І. І. Бобок, О. В. Костирка

АНАЛІЗ СТІЙКОСТІ НОВОГО СТЕГАНОГРАФІЧНОГО МЕТОДУ ДО СТЕГАНОАНАЛІТИЧНИХ АТАК

Розглянуто ефективність детектування нового стеганографічного алгоритму, який здійснює вкладення додаткової інформації у просторовій області контейнера-зображення, за допомогою сучасних стеганоаналітичних комплексів. Продемонстровано стійкість розробленого алгоритму до стеганоаналізу. Наведено залежність ефективності стеганоаналітичних програмних комплексів від значення показника якості цифрових зображень. Наведено результати обчислювальних експериментів.

Ключові слова: стеганографія; стеганоаналіз; ефективність детектування.

I. I. Bobok, O. V. Kostyrka

ROBUSTNESS OF NOVEL STEGANOGRAPHY ALGORITHM AGAINST STEGANALYSIS

In this article was examined the effectiveness of detection of the new steganography algorithm which provides an additional investment in spatial information domain of cover — image with modern facilities of steganalysis. The robustnes of novel steganography algorithm against steganalysis was shown. Testing of dependencies between detection of efficiency of steganalytics of bundled software and quality factor of digital images are adduced. Results of computable experiments are given.

Keywords: steganography; steganalysis; detection efficiency.