Державний університет телекомунікацій

СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ

СОВРЕМЕННАЯ
ЗАЩИТА ИНФОРМАЦИИ

MODERN INFORMATION
SECURITY

№2, 2014

Україна, 03110, Київ,
вул. Солом'янська, 7

Тел. +38 (044) 248-86-07
+38 (044) 249-29-27
www.dut.edu.ua

Засновник: Державний університет телекомунікацій
Зареєстровано Міністерством юстиції України
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 20254-10654 ПР від 10 червня 2014 р.

Постановою Президії ВАК України від 1 липня 2010 р. № 1-05/5
Журнал включено до Переліку наукових фахових видань України,
В яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора та кандидата наук в галузі технічних наук
(*Бюлетень ВАК України, №2, 2010*)

РЕДАКЦІЙНА КОЛЕГІЯ

СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ
№2, 2014 р.
Науково-технічний журнал
Засновано у 2010 році
Виходить чотири рази на рік

Рекомендовано до друку Вченою радою Державного університету телекомунікацій (*протокол №12 від 28 травня 2014 р*)
Адреса редакційної колегії: 03110 м. Київ-110, вул. Солом'янська, 7, ДУТ,
Тел. 248-85-79, 248-86-07, 249-29-27.

Видавництво Державного університету телекомунікацій
03110, Київ, вул. Солом'янська, 7.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру.
Серія ДК № 2539 від 26.06.2006 р.
Підписано до друку *30.05.2014 р.* Формат 64Ч90[1]/8. Замовл. № 126

ЗМІСТ

УДК 004.056.5
Бобок И.И., Костырка О.В.

АНАЛИЗ УСТОЙЧИВОСТИ НОВОГО СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К СТЕГАНОАНАЛИТИЧЕСКИМ АТАКАМ

В статье рассмотрена эффективность детектирования нового стеганографического алгоритма, производящего вложение дополнительной информации в пространственной области контейнера-изображения, современными стеганоаналитическими комплексами. 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, активизация научной деятельности в области стеганографии, публикации новых результатов в открытой печати привели к росту возможностей использования получаемых разработок различными антигосударственными, террористическими структурами. В силу вышесказанного симметричным ответом стало развитие разработок в направлении повышение эффективности стеганоанализа.

На сегодняшний день стеганографический алгоритм может позиционироваться как эффективный только в том случае, если он является устойчивым к стеганоанализу. В силу этого вопрос оценки такой устойчивости является *актуальным* для каждого стеганометода и алгоритма.

Постановка цели

В [1] авторами был предложен новый стеганографический метод, получивший свою реализацию в виде алгоритма *SA*, устойчивого к возмущающим воздействиям, осуществляющего погружение дополнительной информации в пространственной области изображения-контейнера, основанного на достаточном условии такой устойчивости, полученном в [2]. Достаточное условие обеспечивается организацией стеганопреобразования путем корректировки яркости пикселей $l \times l -$блоков матрицы цифрового изображения-контейнера. Разбиение на блоки осуществляется стандартным образом. Корректировка на значение $\pm \Delta b$ производится 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, а $\left\| \Delta \overline{B} \right\|_2$ - спектральная норма матрицы предполагаемого возмущения блока стеганосообщения.

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

С учетом вышесказанного *целью* настоящей статьи является исследование устойчивости алгоритма *SA* к стеганоанализу, проводимому современными программными комплексами.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Для всестороннего анализа рассматриваемого алгоритма выделить среди современных стеганоаналитических комплексов такие, 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: разработка алгоритмов, позволяющих детектировать результаты работы конкретных стеганографических методов, и так называемых, универсальных, или слепых (*blind*), методов, позволяющих путем выявления или констатации отсутствия определенных характерных признаков в анализируемом контенте делать вывод о произведенном внедрении конфиденциальной информации или 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 состаляющую изображения-контейнера. С учетом того, что в работе [5] было показано, что алгоритм *SA* является устойчивым к сжатию, стеганосообщения были сохранены в формате JPEG с различными коэффициентами качества (QF, *quality factor*) – от 50 до 100 с шагом 10, после чего подвергались стеганоанализу.

Использованные стеганоаналитические комплексы представлены следующими продуктами:

1. CANVASS 1.0 (разработка 2009 г.)
2. StegAlyzerSS 3.0 (2007 г.)
3. Stegdetect 0.6.3 (2004 г.)

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

Результаты эксперимента

Наихудшие результаты показал StegAlyzerSS [6], или Steganography Analyzer Signature Scanner, – данный 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, что значит, 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 ещё в базы компании-производителя, будет «не замечен» данным программным комплексом.

Этим примером авторы настоящей работы 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, продемонстрированы в табл. 1. Эффективность детектирования (здесь и далее под эффективностью детектирования будет пониматься процент верно детектированных стеганосообщений от общего числа анализируемых) данного комплекса ни в одной из групп не превысила 13%.

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 ещё признаками, переменными или измерениями). Набор таких образцов называется обучающей выборкой. Задачи классификации состоит в том, чтобы построить хороший прогноз класса y для всякого так же распределённого 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. Данный факт никак 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 данного комплекса максимальная из всех рассматриваемых в данной работе, однако стоит отметить, что как видно из табл. 1, максимум эффективности достигается при QF от 50 до 70. При высоком качестве стеганограмм данный программный комплекс не особо выделяется на фоне выше рассмотренного stegdetect'a. Эффективность детектирования для группы QF = 75 будет примерно на уровне 50%, что соответствует в бинарном классификаторе случайному отнесению объекта к классу.

Авторы настоящей статьи считают, что использования JPEG с низким QF является неоправданным, ввиду нарушения восприятия даже изображений-контейнеров, а так же излишне привлекающим внимание наличием артефактов особенно на фоновой составляющей.

Таблица 1. 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

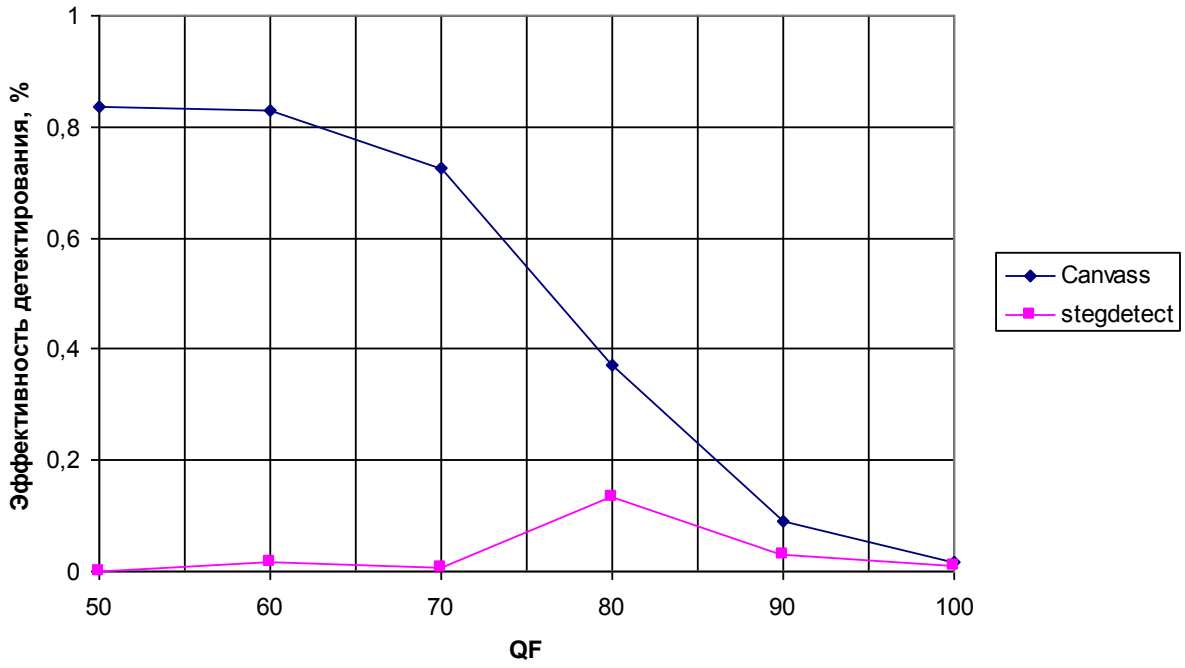

Рис. 1. Зависимость эффективности детектирования нового стеганографического алгоритма от показателя качества JPEG

Выводы

В настоящей статье рассмотрено три стеганоаналитических комплекса, однако недостатки этих программных продуктов могут быть отнесены к работе и других комплексов, ввиду того, что принципы функционирования остаются практически неизменными.

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

1. Разработанный алгоритм не имеет аналогов в базах сигнатур стеганоаналитических комплексов, осуществляющих определение наличия вложения по маске используемого алгоритма;
2. Обучаемость стеганоаналитических комплексов (будь то линейный дискриминантный анализ, или же метод 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 исследование 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 : диссертация … 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).

АНАЛІЗ СТІЙКОСТІ НОВОГО СТЕГАНОГРАФІЧНОГО МЕТОДУ ДО СТЕГАНОАНАЛІТИЧНИХ АТАК

Бобок І.І., Костирка О.В.

У статті розглянуто ефективність детектування нового стеганографічного алгоритму сучасними стеганоаналітичними комплексами. Продемонстровано залежність ефективності детектування від значення показника якості цифрових зображень.

Ключові слова: стеганографія, стеганоаналіз, ефективність детектування

ROBUSTNESS OF NOVEL STEGANOGRAPHY ALGORITHM AGAINST STEGANALYSIS

Bobok I.I., Kostyrka O.V.

The paper focuses on robustness of novel steganography algorithm against steganalysis. Testing of dependencies between detection efficiency and quality factor of digital images.

Keywords: steganography, steganalysis, detection efficiency