Прохожев Н.Н., Михайличенко О.В.,
Башмаков Д.А., Сивачев А.В., Коробейников А.Г.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СТАТИСТИЧЕСКИХ АЛГОРИТМОВ КОЛИЧЕСТВЕННОГО СТЕГАНОАНАЛИЗА В ЗАДАЧЕ ДЕТЕКТИРОВАНИЯ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

Аннотация: *Противодействие скрытым каналам передачи информации, является актуальной задачей при организации информационной безопасности. Одним из видов пассивного противодействия является обнаружение факта стеганографического воздействия на исследуемый контейнер. Распространенное применение неподвижных цифровых изображений в качестве стеганоконтейнеров, обуславливается их большой долей в общем информационном трафике. Задача пассивного противодействия (стеганоанализа), позволяющая выявить цифровое изображение с встроенной информацией, фактически представляет собой задачу бинарной классификации. В основе классификатора используется статистический алгоритм количественного стеганоанализа, определяющий количество измененных пикселей в предъявляемом контейнере. От точности такого алгоритма напрямую зависит качество классификации и практическая эффективность пассивного противодействия в целом. Под эффективностью противодействия в статье понимается соотношение вероятности истинно положительного результата классификации к вероятности ложной положительной классификации. К настоящему времени разработано значительное количество статистических алгоритмов количественного стаганоанализа. При этом исследования, посвященные их сравнительному анализу, отсутствуют, что затрудняет выбор конкретного алгоритма при решении задачи противодействия стеганографическим каналам утечки информации. Также остается открытым вопрос о практической эффективности пассивного противодействия стеганографическим каналам на основе встраивания в наименее значимые биты (НЗБ) пикселей цифрового изображения.Предметом исследования является эффективность применения современных*

DOI: 10.7256/2305-6061.2015.3.17233

статистических алгоритмов количественного стеганоанализа. На основе результатов построены графики доверительных областей, позволяющие произвести сравнительную оценку эффективности пассивного противодействия НЗБ стеганографии. Для исследований выбраны следующие алгоритмы стеганоанализа: RS- analysis, Sample pair analysis, Difference image histogram, Triples analysis, Weighted stego-image. Из тестового множества изображений выбирается изображение. Проводится оценка его пропускной способности (определяется максимальная полезная нагрузка). В проводимых экспериментах за эту величину принято значение общего количества пикселей в изображении. Стеганографическое воздействие моделируется изменением значения наименьших значащих бит для заданного количества пикселей (полезной нагрузки). Модифицированное изображение подается на вход конкретной реализации алгоритма стеганоанализа. Результатом работы алгоритма является количество измененных пикселей в изображении. Эксперименты проводятся в одинаковых условиях для всех реализаций алгоритмов стеганоанализа. Основными выводами проведенного исследования является, то что на основе современных статистических алгоритмов стеганоанализа можно организовать эффективное пассивное противодействие стеганографическим каналам НЗБ встраивания с полезной нагрузкой контейнера более 5%. Уменьшение полезной нагрузки контейнера менее 5% резко снижает эффективность пассивного противодействия. Небольшое изображение разрешением 600x400 пикселей, преобразованное в стеганограмму с полезной нагрузкой в 1-2% практически не детектируется классификаторами на основе статистических количественных алгоритмов стеганоанализа. С учетом возможности предварительного сжатия скрываемых данных и применения матричного встраивания, рассматриваемые современные алгоритмы стеганоанализа нуждаются в дальнейшем совершенствовании.

Ключевые слова: *статистический стеганоанализ, стеганография НЗБ, регулярно-сингулярный анализ, разностно-гистограммный анализ, анализ триплетов, стеганоанализ алгоритмов, стеганография, цифровые водяные знаки, неподвижные изображения, алгоритмы статистического анализа*

Abstract: *Countering the hidden channels of information transmission is an important task in the organization of information security. One kind of passive physical resistance methods is detection of the steganographic impact on the investigated container. The widespread use of digital still images as stegano-containers is due to their large share in total data traffic. The task of passive counteraction (steganalysis) allowing identifying the digital image with the built-in information is actually a binary classification problem. At the core of the classifier lies statistical algorithm of quantitative steganalysis for determining the amount of modified pixels in the data container. The accuracy of the algorithm directly affects the quality classification and the practical effectiveness of passive physical resistance as a whole. By effective counteraction the article refers to the ratio of probabilities between true positive classification and the probability of a false positive classification. Currently there are many statistical algorithms for quantitative steganalysis. However, there are no studies on their comparative analysis which complicates the selection of an algorithm while*

DOI: 10.7256/2305-6061.2015.3.17233

solving the problem of counteraction to steganography channels of information leakage. The practical effectiveness of passive physical resistance to steganography channels by inserting the least significant bits of pixel digital image also remains an open question.The subject of the study is the effectiveness of the application of modern quantitative statistical algorithms steganalysis. Based on the results of the study the authors have formed graphics of trust regions, allowing to make a comparative assessment of the effectiveness of the passive counteraction in LSB-steganography. For the study the authors selected the following steganalysis algorithms: RS- analysis, Sample pair analysis, Difference image histogram, Triples analysis, Weighted stego-image. From the test of multiple images an image is selected. An evaluation of its capacity (defined by the maximum payload) is performed. In the experiments for this value authrs accepted the total number of pixels in the image. Steganographic effects modeled by changing the value of the least significant bit for a predetermined number of pixels (the payload). The modified image used as an input to a particular implementation of the algorithm steganalysis. The result of the algorithm is the number of changed pixels in the image. The experiments were carried out under the same conditions for all implementations of algorithms steganalysis. The main conclusions of the study is the fact that based on modern statistical steganalysis algorithms it is possible to organize an effective opposition to the passive channels with LSB steganography with embedding payload container more than 5%. Reducing the payload container of less than 5% dramatically reduces the effectiveness of the passive counteraction. A small 600x400 pixels image converted to steganography with payload of 1-2% is practically not detected by classifiers based on statistical quantitative algorithms steganalysis. Taking into account the possibility of pre-compression hidden data and matrix embedding, the considered modern algorithms for steganalysis need further improvement.

Keywords: *the steganalysis algorithm, weighted stego-image, difference histogram analysis, simple pair analysis, LSB-based steganography, statistical quantative steganalysis, steganography, digital watermark, still images, statistical analysis algorithms*

Введение

В современном информационном мире стеганографические методы нашли широкое применение в задачах организации скрытых каналов передачи информации [1, 2]. Решая задачи конфиденциальности и защиты передаваемой и хранимой информации, стеганография все чаще применяется для скрытой передачи информации секретными службами [3], криминальными сообществами и террористическими организациями [4, 5]. Одним из распространенных видов контейнеров, в которые производится стеганографическое встраивание скрываемой информации, являются цифровые неподвижные изображения. Большой процент цифровых изображений в информационном трафике позволяет организовать скрытый канал передачи, обладающий значительной пропускной способностью и хорошей скрытностью. Наиболее простыми и доступными среди большого разнообразия стеганографических алгоритмов, являются алгоритмы пространственной области встраивания. В открытом доступе находится значительное количество бесплатного программ-

DOI: 10.7256/2305-6061.2015.3.17233

ного обеспечения, позволяющего осуществлять стеганографическое встраивание в НЗБ пикселей изображения. Противодействовать скрытым каналам передачи информации возможно посредством методов и средств как активного, так и пассивного характера. Активное противодействие предполагает вмешательство в открытый канал передачи и искажение информации контейнера с целью уничтожения скрытого в нем стеганографического канала. Пассивные средства противодействия решают задачу детектирования самого факта наличия стеганографического канала. Задача пассивного противодействия в простейшем случае представляет задачу бинарной классификации. Предъявляемый контейнер необходимо отнести либо к классу оригинальных изображений, либо к классу стеганограмм. Для задач пассивного противодействия разработано большое количество методов и алгоритмов стеганоанализа. Отдельную группу представляют статистические алгоритмы количественного стеганоанализа (statistic quantative steganalysis) (далее – алгоритмы стеганоанализа). Особенностью таких алгоритмов является их ориентация на анализ статистики некоторых характеристик контейнера и оценка количественного показателя стеганографического воздействия в отношении контейнера. Применительно к цифровым изображениям и НЗБ стеганографии, результатом работы алгоритма стеганоанализа будет являться оценка количества пикселей контейнера, измененных в результате стеганографического воздействия. Задача пассивного противодействия усложняется тем фактом, что, как правило, метод стеганографического воздействия заранее неизвестен. Универсальных алгоритмов стеганоанализа к настоящему времени не существует, большинство алгоритмов эффективны в отношении только определенного типа методов стеганографического воздействия. В работе рассматривается задача пассивного противодействия в отношении стеганографических каналов на основе НЗБ методов. К настоящему времени разработано целое семейство статистических алгоритмов стеганоанализа.

Авторы, рассматриваемых в статье алгоритмов стеганоанализа, констатируют факт наличия незначительной погрешности при определении количества пикселей, в которых значение НЗБ было изменено в результате стеганографического воздействия на изображение-контейнер. При решении задач пассивного противодействия от выбора конкретного алгоритма стеганоанализа и его погрешности будет зависеть практическая точность классификации предъявляемых изображений. Особо стоит отметить, что при использовании в стеганоанализе количественных алгоритмов большое значение имеет не просто средняя погрешность алгоритма, а погрешность при малых значениях полезной нагрузки (payload) изображения-контейнера.

Существующие работы, посвященные оценке алгоритмов стеганоанализа, не в полной мере отвечают практическим потребностям при решении задач пассивного противодействия. Часть публикаций, предоставляющих обзор современных алгоритмов стеганоанализа, указывает точность определения количества измененных пикселей, заявляемую самими авторами этих алгоритмов, и, как следствие, полученными в разных условиях [6, 7]. Другие работы, содержащие результаты проведенных исследований, содержат данные зависимости погрешности результатов самих алгоритмов от полезной нагрузки изображения-контейнера, но при этом никак не освещается вопрос их практической эффективности в задачах пассивного противодействия [8].

DOI: 10.7256/2305-6061.2015.3.17233

Таким образом, основной целью работы является оценка эффективности современных алгоритмов стеганоанализа в задачах пассивного противодействия НЗБ стеганографии при небольших значениях полезной нагрузки изображения-контейнера. В качестве конечного результата приводятся графики доверительных областей (Region Of Confident curve) для фиксированных значений полезной нагрузки и таблица, дифференцирующая результаты эффективности применения алгоритмов по разным коллекциям изображений.

Научная новизна работы заключается в получении данных для сравнительного анализа эффективности применения современных алгоритмов стеганоанализа в задаче пассивного противодействия при условии малых значений полезной нагрузки для изображений-контейнеров. Также результаты работы иллюстрируют значения полезной нагрузки, при которой точность классификации предъявляемого изображения резко снижается, т.е. значения максимальной пропускной способности стеганоканала, достижимой в условиях пассивного противодействия с использованием алгоритмов статистического стеганоанализа.

Методика эксперимента

Из тестового множества изображений последовательным перебором выбирается конкретное изображение. В изображении инвертируются значения НЗБ для фиксированного количества пикселей, что моделирует стеганографическое воздействие. Количество пикселей (полезная нагрузка) выражается в процентах от максимальной полезной нагрузки конкретного изображения. Под максимальной полезной нагрузкой принимается значение общего количества пикселей изображения. Значения полезной нагрузки выбирались от 1 до 6% исходя из предпосылок заявленной погрешности алгоритмов около 2%. Модифицированное изображение поступает на вход алгоритма стеганоанализа. Результатом работы алгоритма является число, соответствующее количеству пикселей, подвергшихся стеганографическому воздействию. Результаты сохраняются для дальнейшей статистической обработки. Эксперименты проводятся в одинаковых условиях (количество и характеристики изображений, математическая точность преобразований, среда моделирования и т.д.) для всех реализаций алгоритмов стеганоанализа.

В качестве алгоритмов стеганоанализа рассматривались современные алгоритмы, имеющие подробное описание, низкую вычислительную сложность, простоту программной реализации и наиболее часто встречаемые в литературе. Все рассматриваемые в работе алгоритмы, по утверждению их создателей, обладают малой погрешностью определения количества пикселей, подвергшихся стеганографическому воздействию в области НЗБ. При этом результаты их сравнительного анализа в открытых источниках отсутствуют. Таким образом, для исследований были выбраны следующие алгоритмы:

– RS-analysis (RS) [9];
– Sample pair analysis (SP) [10];
– Difference image histogram (DIH) [11];
– Triples analysis (TR) [12];
– Weighted stego-image (WSI) [13].

DOI: 10.7256/2305-6061.2015.3.17233

Все алгоритмы реализованы в среде Matlab.

В качестве тестового множества использованы три коллекции полутоновых изображений:

– коллекция 1 – 3126 изображений разрешением от 392x550 до 5184x3456 [14];

– коллекция 2 – 5214 изображений разрешением от 1339x1357 до 5100x4026 [15];

– коллекция 3 – 30682 изображений разрешением от 700x500 до 1300x734 [16].

Коллекции находятся в общем доступе, имеют широкий диапазон характеристик и значительное количество изображений.

Координаты пикселей для изменения значений НЗБ выбирались псевдослучайным образом с равномерным характером распределения.

Методика оценки эффективности алгоритмов стеганоанализа

Как уже отмечалось выше, задача пассивного противодействия стеганографическим каналам сводится к задаче бинарной классификации. Тогда множество классов может быть обозначено как $Y=\{-1,+1\}$, а классификатор может быть представлен в виде:

$$a(x) = sign(f(x,w)-w_0),$$

где x – произвольный объект, $f(x,w)$ – дискриминантная функция (алгоритм стеганоанализа), w – вектор параметров (количество пикселей с измененным значением НЗБ), w_0 – порог.

Таким образом, в основе классификатора применяется алгоритм стеганоанализа и классификация предъявляемого изображения осуществляется путем сравнения результата работы алгоритма с некоторым пороговым значением. Уравнение $f(x,w)=w_0$ определяет разделяющую поверхность.

Если в результате работы алгоритма стеганоанализа получается величина, превышающая пороговое значение, система классифицирует предъявляемое изображение как стеганограмму, в противном случае изображение относится к классу оригинальных изображений без признаков стеганографического воздействия.

Выбор величины порогового значения w_0, задача не тривиальная, поскольку от нее зависят значения вероятностей как положительного (TP), так и ложного положительного (FP) детектирования. Выбор слишком малого значение величины порога приведет к увеличению вероятности, как положительной классификации, так и ложной положительной классификации. Такой выбор на практике приведет к классификации оригинальных изображений как стеганограмм.

Слишком большое значение величины порога увеличит вероятность ложного отрицательного (FN) результата, т.е. когда система не фиксирует факт стеганографического воздействия для предъявляемого изображения, хотя таковое имело место быть.

Вышеописанную проблему хорошо иллюстрирует статистика результатов работы алгоритма RS-analysis, полученная на тестовом множестве изображений (рис. 1). Графики подтверждают утверждения авторов данного алгоритма, что погрешность определения количества пикселей, подвергшихся изменению значений НЗБ, составляет около 2% от общего количества пикселей изображения.

Графики также иллюстрируют, что выбирая величину порогового значения (двигаясь вдоль горизонтальной оси) для классификации на основе алгоритма RS-analysis и при

DOI: 10.7256/2305-6061.2015.3.17233

условии, что полезная нагрузка не превышает 5% при любых значениях порога, неизбежны сценарии ложной положительной или ложной отрицательной классификации.

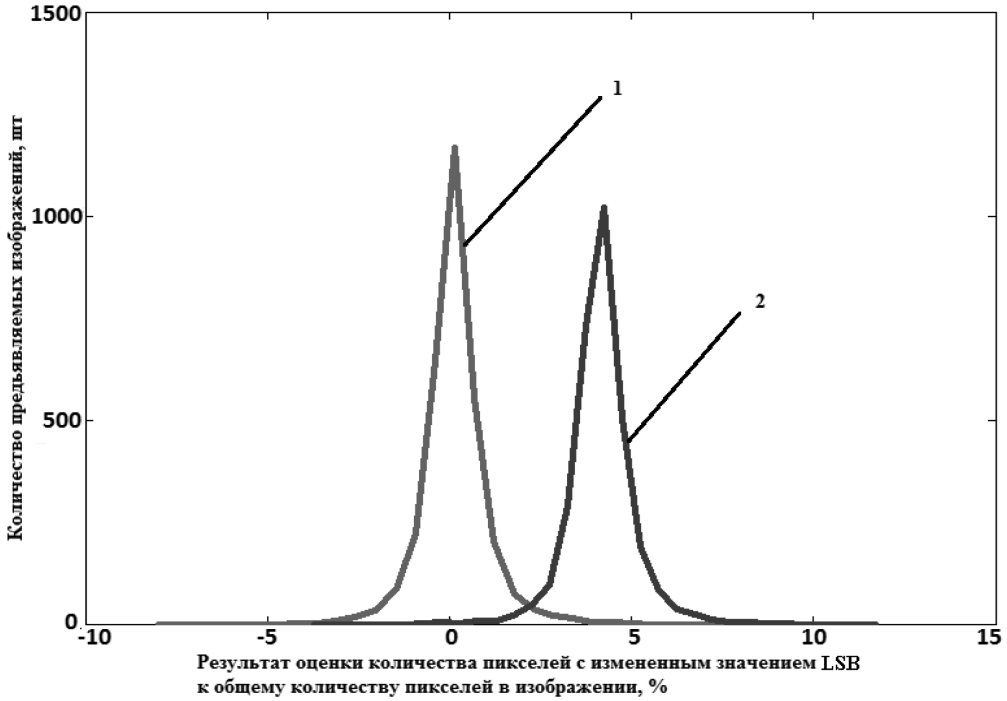

Рис. 1. График распределения результатов работы алгоритма RS-analysis для изображений, не подвергавшихся изменениям (1), и стеганограмм с полезной нагрузкой 5 % (2).

Доля верных положительных классификаций (True Positive Rate, TPR) определяется как:

$$TPR(a, \mathrm{X}^{\mathrm{m}}) = \frac{\sum_{i=1}^{m}[a(x_i) = +1][y_i = +1]}{\sum_{i=1}^{m}[y_i = +1]},$$

где, $X^m = (x_1, \ldots, x_m)$ – выборка объектов, $y_1 \ldots y_m$ классы, к которым принадлежат соответствующие объекты из выборки. Данная характеристика бинарного классификатора называется «точность» (precision) и показывает, сколько из классифицированных стеганограмм оказались действительно стаганограммами.

Доля ложных положительных классификаций (False Positive Rate, FPR) определяется как:

$$FPR(a, \mathrm{X}^{\mathrm{m}}) = \frac{\sum_{i=1}^{m}[a(x_i) = +1][y_i = -1]}{\sum_{i=1}^{m}[y_i = -1]},$$

DOI: 10.7256/2305-6061.2015.3.17233

и показывает, сколько от общего числа оригинальных изображений, оказались классифицированными как стеганограммы.

Очевидно, что изменяя величину порогового значения, будут изменяться FPR и TPR. От соотношения этих величин будет зависеть качество классификации, и, следовательно, практическая эффективность пассивного противодействия. Идеальный классификатор, обеспечивающий абсолютную эффективность пассивного противодействия, имеет долю верной положительной классификации 1 и долю ложной положительной классификации равную 0.

Для большей наглядности этих зависимостей, предлагается воспользоваться графиком доверительных областей (ROC) [17]. Для его построения по вертикальной оси откладывается значение TPR, по горизонтальной значение FPR, полученные при одинаковых значениях порога w_0.

Наличие графиков доверительных областей для различных алгоритмов стеганоанализа, полученных в идентичных условиях, позволяет провести сравнительную оценку анализируемых алгоритмов.

Результаты исследования

По результатам экспериментов были построены графики доверительных областей для всех исследуемых в работе алгоритмов стеганоанализа при разных значениях полезной нагрузки изображения-контейнера. Графики доверительных областей, наиболее наглядно демонстрирующие сравнительные характеристики алгоритмов стеганоанализа и динамику их изменения в зависимости от значения полезной нагрузки, представлены на рисунке 2. Те же результаты, дифференцированные по различным коллекциям изображений, приведены в таблице.

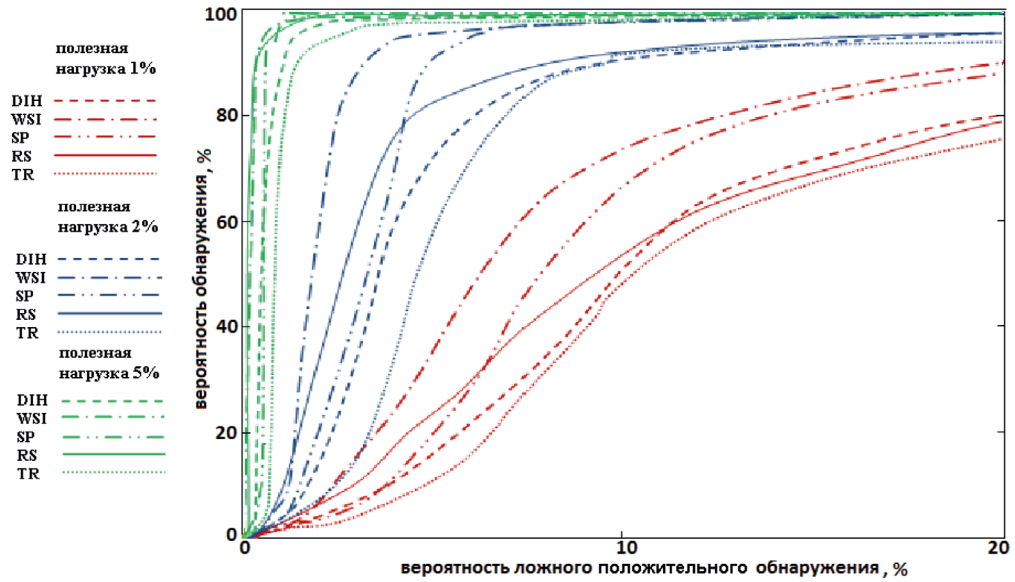

Рис. 2 – Графики доверительных областей для алгоритмов стеганоанализа при разных значениях полезной нагрузки изображения-контейнера

DOI: 10.7256/2305-6061.2015.3.17233

Алгоритм, используемый в системе стеганоанализа	Номер коллекции	Количество пикселей, с изменениями в области НЗБ (полезная нагрузка), %				
		1	2	3	4	5
RS-analysis	1	48,1	30,0	7,1	2,1	0,7
	2	3,6	1,5	1,0	0,6	0,3
	3	49,7	32,7	8,3	3,6	1,9
Difference image histogram	1	42,4	33,4	8,0	2,9	1,5
	2	5,8	2,2	1,2	0,8	0,5
	3	44,9	23,5	18,2	7,8	4,6
Sample pair analysis	1	43,9	9,6	2,1	1,1	0,5
	2	5,2	1,8	1,1	0,7	0,3
	3	44,6	12,8	4,8	2,2	1,3
Triples analysis	1	62,7	37,5	8,3	2,7	1,7
	2	4,4	1,9	1,4	1,0	0,7
	3	64,4	36,7	9,4	3,9	1,9
Weighted stego-image	1	36,7	7,1	1,8	0,7	0,5
	2	2,6	0,9	0,5	0,4	0,1
	3	38,3	8,8	2,4	1,1	0,7

Таблица. Значения ложной положительной классификации (%) для значения доли положительной классификации 97,5%

Выводы

Современные статистические алгоритмы количественного стеганоанализа близки по характеристикам точности определения количества измененных пикселей, что делает классификаторы на их основе также близкими по качеству.

С уменьшением полезной нагрузки контейнеров от 5% и менее качество классификации существенно снижается.

Существенное влияние на качество классификации оказывает разрешение изображения-контейнера. Так для коллекции тестовых изображений № 2, размеры изображений в которой не менее 1339x1357, доля ложной классификации почти на порядок меньше, чем для коллекций №1 и №3, где минимальные размеры изображений 392x550 и 700x500 соответственно (см. таблицу).

Заключение

На основе современных статистических алгоритмов стеганоанализа можно организовать эффективное пассивное противодействие стеганографическим каналам НЗБ встраивания с полезной нагрузкой контейнера более 5%. Уменьшение полезной нагрузки

DOI: 10.7256/2305-6061.2015.3.17233

контейнера менее 5% резко снижает эффективность пассивного противодействия. Для стеганографического встраивания, выполненного в НЗБ область изображений, размер которых не превышает разрешение современных мониторов, а также и значением полезной нагрузки в 1% и менее, пассивное противодействие малоэффективно.

Небольшое изображение разрешением 600x400 пикселей, преобразованное в стеганограмму с полезной нагрузкой в 1-2% практически не детектируется классификаторами на основе статистических количественных алгоритмов стеганоанализа. При этом величина полезной нагрузки позволяет встроить информацию объемом 5-10 кбит. С учетом возможности предварительного сжатия скрываемых данных и применения матричного встраивания [18, 19], рассматриваемые современные алгоритмы стеганоанализа нуждаются в дальнейшем совершенствовании.

Библиография :

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография // В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика //Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
3. S. Fox FBI: Russian spies hid codes in online photos [Электронный ресурс] // NBC News, New York, USA. Режим доступа: http://www.nbcnews.com/id/38028696/ns/technology_and_science/t/fbi-russian-spies-hid-codes-online-photos (Дата обращения: 30.05.2014)
4. J. Kelley Terrorist instructions hidden online [Электронный ресурс] / USA TODAY, Virginia, USA. Режим доступа: http://usatoday30.usatoday.com/tech/news/2001-02-05-binladen-side.htm (Дата обращения: 30.05.2014)
5. S. Gallagher Steganography: how al-Qaeda hid secret documents in a porn video [Электронный ресурс] / Ars Technica, Boston, USA. Режим доступа: http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video (Дата обращения: 30.05.2014)
6. L. Singh, R. Chhikara A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted, ITM University, Gurgaon, Haryana, India. International Journal of Engineering and Innovative Technology (IJEIT)Volume 3, Issue 4, October 2013
7. A. Nissar, A.H. Mir Classification of steganalysis techniques, Digital Signal Processing 20 (2010) pp. 1758–1770
8. J. Fridrich, M. Goljana, D. Soukalb Higher-order statistical steganalysis of palette images, Department of Electrical and Computer Engineering, Department of Computer Science, SUNY Binghamton, Binghamton, NY 13902-6000
9. J.Fridrich, M.Goljan, R.Du Reliable Detection of LSB Steganography in Color and Grayscale Images, State Univ. of New York, Binghamton, NY, USA.
10. Lu, P., X. Luo et. al.// An improved sample pairs method for detection of LSB embedding, Proc. of the 6th Information Hiding Workshop, Springer LNCS, vol.3200, pp.116-128, 2004
11. Zhang, T. and X. Ping // Reliable detection of LSB steganography based on the difference image histogram, Proc. of the IEEE ICSAAP 2003, Part III, pp. 545-548, 2003.

DOI: 10.7256/2305-6061.2015.3.17233

12. A.D. Ker: A general framework for structural steganalysis of LSB Replacement // Proc. of the Information Hiding, pp.296-311, 2005.
13. Mao Ye, Fenlin Liu, Chunfang Yang, Xiongfei He Steganalysis Based on Weighted Stego-Image for LSB Replacement Steganography// Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. pp. 945-948
14. Фотографии грибов [Электронный ресурс] / Список форумов rutracker.org Режим доступа: http://rutracker.org/forum/viewtopic.php?t=3705334 (Дата обращения: 30.05.2014)
15. Коллекция Фотографии Америки 20-го века [Электронный ресурс] / Список форумов rutracker.org Режим доступа: http://rutracker.org/forum/viewtopic.php?t=3501973 (Дата обращения: 30.05.2014)
16. Коллекция "World in photo" [Электронный ресурс] / Список форумов rutracker.org Режим доступа: http://rutracker.org/forum/viewtopic.php?t=2272897 (Дата обращения: 30.05.2014)
17. H.G. Schaathun. Machine learning in image steganalysis // Alesund University College, pp 164-167 , 2012
18. Y. Kim, Z. Duric, D. Richards, Modified matrix encoding technique for minimal distortion steganography// in Proc. 8th Int. Workshop Information Hiding. Jul. 10-12, 2006, vol. 4437, pp. 314-327
19. Коробейников А.Г., Кутузов И.М. Алгоритм обфускации // Кибернетика и программирование. - 2013. - 3. - С. 1 - 8. DOI: 10.7256/2306-4196.2013.3.9356. URL: http://www.e-notabene.ru/kp/article_9356.html

References:

1. Gribunin, V.G. Tsifrovaya steganografiya [Tekst] : monografiya // V.G. Gribunin, I.N. Okov, I.V. Turintsev. — M. : SOLON-Press, 2002. — 272 s.
2. Konakhovich, G.F. Komp'yuternaya steganografiya [Tekst]: teoriya i praktika //G.F. Konakhovich, A.Yu. Puzyrenko. — Kiev : MK-Press, 2006. — 288 s.
3. S. Fox FBI: Russian spies hid codes in online photos [Elektronnyi resurs] // NBC News, New York, USA. Rezhim dostupa: http://www.nbcnews.com/id/38028696/ns/technology_and_science/t/fbi-russian-spies-hid-codes-online-photos (Data obrashcheniya: 30.05.2014)
4. J. Kelley Terrorist instructions hidden online [Elektronnyi resurs] / USA TODAY, Virginia, USA. Rezhim dostupa: http://usatoday30.usatoday.com/tech/news/2001-02-05-binladen-side.htm (Data obrashcheniya: 30.05.2014)
5. S. Gallagher Steganography: how al-Qaeda hid secret documents in a porn video [Elektronnyi resurs] / Ars Technica, Boston, USA. Rezhim dostupa: http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video (Data obrashcheniya: 30.05.2014)
6. L. Singh, R. Chhikara A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted, ITM University, Gurgaon, Haryana, India. International Journal of Engineering and Innovative Technology (IJEIT)Volume 3, Issue 4, October 2013
7. A. Nissar, A.H. Mir Classification of steganalysis techniques, Digital Signal Processing 20 (2010) pp. 1758–1770
8. J. Fridrich, M. Goljana, D. Soukalb Higher-order statistical steganalysis of palette images, Department of Electrical and Computer Engineering, Department of Computer Science, SUNY Binghamton, Binghamton, NY 13902-6000
9. J.Fridrich, M.Goljan, R.Du Reliable Detection of LSB Steganography in Color and Grayscale Images, State Univ. of New York, Binghamton, NY, USA.

10. Lu, P., X. Luo et. al.// An improved sample pairs method for detection of LSB embedding, Proc. of the 6th Information Hiding Workshop, Springer LNCS, vol.3200, pp.116-128, 2004
11. Zhang, T. and X. Ping // Reliable detection of LSB steganography based on the difference image histogram, Proc. of the IEEE ICSAAP 2003, Part III, pp. 545-548, 2003.
12. A.D. Ker: A general framework for structural steganalysis of LSB Replacement // Proc. of the Information Hiding, pp.296-311, 2005.
13. Mao Ye, Fenlin Liu, Chunfang Yang, Xiongfei He Steganalysis Based on Weighted Stego-Image for LSB Replacement Steganography// Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. pp. 945-948
14. Fotografii gribov [Elektronnyi resurs] / Spisok forumov rutracker.org Rezhim dostupa: http://rutracker.org/forum/viewtopic.php?t=3705334 (Data obrashcheniya: 30.05.2014)
15. Kollektsiya Fotografii Ameriki 20-go veka [Elektronnyi resurs] / Spisok forumov rutracker.org Rezhim dostupa: http://rutracker.org/forum/viewtopic.php?t=3501973 (Data obrashcheniya: 30.05.2014)
16. Kollektsiya "World in photo" [Elektronnyi resurs] / Spisok forumov rutracker.org Rezhim dostupa: http://rutracker.org/forum/viewtopic.php?t=2272897 (Data obrashcheniya: 30.05.2014)
17. H.G. Schaathun. Machine learning in image steganalysis // Alesund University College, pp 164-167 , 2012
18. Y. Kim, Z. Duric, D. Richards, Modified matrix encoding technique for minimal distortion steganography// in Proc. 8th Int. Workshop Information Hiding. Jul. 10-12, 2006, vol. 4437, pp. 314-327
19. Korobeinikov A.G., Kutuzov I.M. Algoritm obfuskatsii // Kibernetika i programmirovanie. - 2013. - 3. - C. 1 - 8. DOI: 10.7256/2306-4196.2013.3.9356. URL: http://www.e-notabene.ru/kp/article_9356.html

DOI: 10.7256/2305-6061.2015.3.17233