УДК 004.056.5:518

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 18-27

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К АТАКЕ СЖАТИЕМ

А.А. Кобозева

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

На основе общего подхода к анализу состояния и технологии функционирования информационных систем, разработанного автором ранее, предлагается новый подход к решению проблемы устойчивости стеганографических алгоритмов к атаке сжатием. В работе получены формальные достаточные условия малой чувствительности стеганосообщения к сжатию с одновременным обеспечением его надежности восприятия. Предложенный подход позволит автоматизировать процесс анализа существующих или разрабатываемых стеганографических алгоритмов с точки зрения их устойчивости к сжатию путем оценки возмущений сингулярных чисел матрицы (матриц) контейнера, произошедших в процессе стеганопреобразования, а также даст возможность априорного выбора из множества стеганосообщений наименее чувствительного к сжатию.

Ключевые слова: стеганографический алгоритм, атака сжатием, сингулярные числа

Введение

Надежная защита информации, которая в настоящее время все больше становится товаром, причем одним из наиболее дорогих [1], от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [2-6], особенностью которых является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый объект, не привлекающий внимание, или контейнер, который затем открыто пересылается адресату по каналу связи или хранится в таком виде.

В последнее время создано много методов сокрытия информации в разных типах и форматах данных [4, 7-9], и сейчас этот процесс активно развивается, поскольку, хотя современные компьютерные технологии обработки данных дали возможность широкого использования криптографических методов защиты информации, для ряда прикладных задач информационной безопасности криптографических методов недостаточно [7].

Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС). Для определенности везде ниже как ОС используется монохромное цифровое изображение (ЦИ), а как ДИ – сформированная случайным образом бинарная последовательность.

К любому стеганографическому алгоритму (СА) выдвигается ряд требований, среди которых важную роль играет требование устойчивости к преднамеренным (непреднамеренным) атакам [2, 7, 8]. Согласно [4], СА назовем устойчивым (неустойчивым), если сформированное им СС является нечувствительным (чувствительным) к возмущающим воздействиям.

Созданию устойчивых алгоритмов в современной печати уделено достаточно внимания, однако вопрос создания СА, устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов (в частности ЦИ), остается актуальным и на сегодняшний день. Как правило, все существующие СА такого плана осуществляют погружение ДИ в частотной области контейнера и, при условии обеспечения надежности восприятия СС, выдерживают лишь незначительное сжатие [2, 3, 10, 11]. И хотя в некоторых работах, как, например, в [11], декларируется достижение устойчивости предлагаемого алгоритма к сжатию для любого коэффициента качества, представленные теоретические обоснования и результаты тестирования его работы на 10 ЦИ выглядят неубедительно.

Поскольку атака сжатием на СС является одним из видов возмущающих воздействий, сравнение устойчивости различных СА к атаке сжатием можно проводить, сравнивая чувствительность к возмущающим воздействиям формируемых ими СС, используя подход, предложенный автором ранее в [12], основанный на теории возмущений и матричном анализе. Сложность в использовании данного подхода заключается в том, что он носит преимущественно качественный характер. Его развитием стали последующие работы, в частности, [13], результатом которых явилось создание метода количественной оценки устойчивости СА к произвольным возмущающим воздействиям, основой которого является оценка объема защищенной информации в СС, проводимая с учетом возмущений сингулярных векторов (СНВ) соответствующих матриц ОС при СП. Геометрическая интерпретация процесса СП дана на рис. 1, где $u_i, i=\overline{1,3}$, – СНВ матрицы (подматрицы) ОС, а $\overline{u}_i, i=\overline{1,3}$, – СНВ СС. Однако предложенный подход является «слишком универсальным», он не учитывает особенностей конкретного возмущающего воздействия – сжатия. Кроме того, оценка чувствительности СС через оценку чувствительности возмущенных в ходе СП СНВ вызывает затруднение, поскольку чувствительность СНВ одной и той же матрицы различна и зависит от отделенностей соответствующих сингулярных чисел (СНЧ) [4, 13]. Более предпочтительным и желаемым является сведение оценки устойчивости СА к локализации возмущений только СНЧ, произошедших в ходе СП, в силу их хорошей обусловленности [14].

Таким образом, актуальным остается поиск новых путей и подходов к принципиальному решению проблемы обеспечения для разрабатываемых СА устойчивости к сжатию, которую далее будем называть проблемой сжатия (ПС).

Цель исследования и постановка задачи

В [14] на основе теории возмущений и матричного анализа был разработан общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), в частности, систем защиты информации, основная идея которого заключается в следующем.

Произвольная информационная система, в том числе, стеганографическая система (или отдельно рассматриваемый контейнер, СС), формализуется в виде двумерной матрицы (конечного множества двумерных матриц), что позволяет свести анализ состояния системы к анализу свойств соответствующих матриц. Для простоты изложения, не ограничивая при этом общности рассуждений, в качестве математической модели произвольной информационной системы рассматривается двумерная $m \times n$-матрица F. Результат любых действий, производимых над системой, в общем случае можно представить как возмущение ΔF матрицы F, сами действия – возмущающие воздействия на F, а задача любого преобразования системы, т.е. генерации новой, для которой старая является исходными данными, – это задача получения возмущенной

матрицы для исходной матрицы F, причем результирующая матрица очевидно удовлетворяет соотношению: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы F. Таким образом, в качестве набора формальных параметров, однозначно определяющих и всесторонне характеризующих информационную систему, можно использовать любой из наборов, который однозначно определяет произвольную двумерную матрицу – полных наборов параметров [15]. Одним из таких наборов, преимущества которого подробно обсуждаются в [14], является совокупность СНЧ и СНВ, полученных при помощи нормального спектрального разложения матрицы, отвечающей рассматриваемой системе.

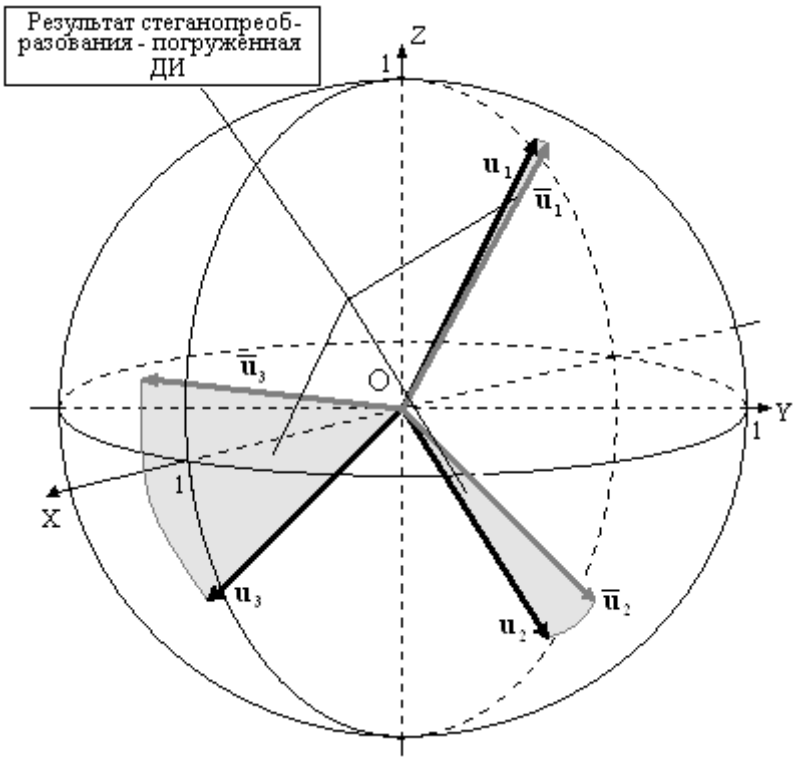

Рис. 1. Формальное представление результата стеганопреобразования

Любое преобразование информационной системы возмутит ее матрицу F, следовательно определенным образом возмутит ее СНЧ и СНВ, а значит любое преобразование, в том числе и СП, представимо в виде совокупности возмущений СНЧ и (или) СНВ соответствующей матрицы (матриц). Это позволяет естественным образом свести задачу анализа процесса стеганопреобразования к анализу возмущений СНЧ и СНВ соответствующей матрицы (матриц) контейнера (СС), независимо от рассматриваемой области сигнала, конкретики используемого СА или предпринятой атаки [4].

Таким образом, о результате преобразования информационной системы (в частности, стеганосистемы), ее свойствах, характеристиках можно судить по характерным особенностям совокупности возмущений однозначно определяющих ее параметров – СНЧ и СНВ соответствующей матрицы (матриц). Это утверждение является краеугольным камнем для разработок, предложенных в настоящей работе.

Целью работы является получение достаточных условий обеспечения устойчивости СА к атаке сжатием с одновременным обеспечением надежности восприятия формируемого СС путем разработки принципиально нового общего подхода к решению ПС на основе адаптации ОПАИС в область стеганографии, что даст возможность автоматизировать процесс анализа существующих или разрабатываемых

СА с точки зрения их устойчивости к сжатию и формально определить необходимые корректировки СА в случае его неустойчивости.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Выделить из совокупности формальных параметров, определяющих результат СП, – СНЧ (СНВ) соответствующих матриц, отвечающих ОС, наименее чувствительные к операции сжатия;

2) Получить формальное представление процесса сжатия в виде совокупности определенных возмущений СНЧ (СНВ) матриц ЦИ.

Основная часть

Конкретизируем понятие СА, устойчивого к атаке сжатием.

Общая схема сжатия (с потерями) для ЦИ, которая использована в наиболее распространенных на сегодня стандартах, в частности, в стандарте JPEG, состоит из трех основных шагов:

- отображение в частотную область после предварительного стандартного разбиения матрицы изображения на 8×8-блоки;
- квантование полученных частотных коэффициентов;
- энтропийное кодирование.

Восстановление включает в себя шаги, обратные к перечисленным выше, в обратном порядке [15].

Независимо от конкретики непосредственной реализации сжатия отметим, что в силу специфики человеческого зрения сжатие происходит таким образом, что его результат приводит к исключению из сигнала его высокочастотных (а возможно, и среднечастотных) составляющих за счет обнуления соответствующих коэффициентов. В силу этого для определенности изложения, никак не ограничивая общности рассуждений, везде ниже атака сжатием, направленная на СС, моделируется путем сохранения этого СС в одном из наиболее распространенных на сегодняшний день форматов – формате JPEG с потерями, основанном на дискретном косинусном преобразовании.

В силу специфики предметной области решаемой задачи не имеет смысла рассматривать сжатие с потенциально произвольным коэффициентом, поскольку после проведенной на СС атаки надежность восприятия этого СС не должна быть нарушена [2].

Учитывая [16], в данной работе рассматриваются варианты JPEG-сжатия ЦИ, которое осуществляется в среде *Adobe* Photoshop с коэффициентами качества $Q\in\{8,9,10,11,12\}$ (для меньших значений Q надежность восприятия, устанавливаемая путем субъективного ранжирования, может нарушаться). Эффективность декодирования СА оценивается величиной объема восстановленной информации (ОВИ), который вычисляется согласно формуле

$$\frac{k-\sum_{i=1}^{k} p_i \oplus \overline{p}_i}{k}\cdot 100\%,$$

где

$p_1, p_2, ..., p_k$, $p_i \in \{0,1\}$, $i = 1,...,k$, – последовательность, которая отвечает встраиваемому секретному сообщению;

$\overline{p}_1, \overline{p}_2, ..., \overline{p}_k$, $\overline{p}_i \in \{0,1\}$, $i = 1,...,k$, – декодированное из СС секретное сообщение;

$\oplus$ – операция логического исключающего ИЛИ.

Поскольку до настоящего момента нигде в открытой печати не была установлена однозначная точная нижняя граница величины, каким-либо образом характеризующей эффективность декодирования СА, для которой алгоритм можно называть устойчивым к операции сжатия (чаще всего такая оценка носит не количественный, а качественный характер), условимся считать СА *устойчивым* к сжатию, если ОВИ после атаки на СС с $Q \in \{8,9,10,11,12\}$, окажется не меньше 75% для $Q = 8$. ОВИ является численной оценкой устойчивости СА.

Последний шаг восстановления ЦИ после сжатия возвращает его из частотной в пространственную область. При этом коэффициенты получаемой матрицы будут иметь вещественные значения, которые могут выходить за границы множества [0,255]. Результат восстановления на этой стадии назовем частичным (ЧВ). Окончательное, или полное, восстановление (ПВ) ЦИ будет получено после округления значений яркости до целых и введения их в границы 0...255.

Процесс квантования приводит к обнулению коэффициентов, отвечающих, как правило, высоким частотам сигнала, за счет чего и происходит сжатие. Но при достаточно большом коэффициенте сжатия возможно обнуление и среднечастотных коэффициентов, поэтому использование для погружения ДИ средней части частотного спектра, о чем говорилось выше, формирует СС, которое принципиально может выдерживать лишь незначительное сжатие.

Пусть F – $m \times n$-матрица контейнера. Для F существует нормальное сингулярное разложение [14]: $F = U\Sigma V^T$, где U, V – ортогональные матрицы размера $m \times n$ и $n \times n$ соответственно, столбцы $u_1,...,u_n$ матрицы U, называемые левыми СНВ, лексикографически положительны [14] (столбцы $v_1,...,v_n$ матрицы V называют правыми СНВ матрицы F); $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ – сингулярные числа (СНЧ); (σ_i, u_i, v_i) называется сингулярной тройкой F. В [14] показано, что невырожденная матрица имеет единственное нормальное сингулярное разложение, если ее СНЧ попарно различны, которое может представляться в форме внешних произведений: $F = \sum_{k=1}^{n} \sigma_k u_k v_k^T$. Матрицу

$$S_k = \sigma_k u_k v_k^T \qquad (1)$$

в соответствии с [17] назовем *k*-й составляющей изображения F.

В [17] в результате представительного вычислительного эксперимента было установлено: *k*-ые составляющие (1) изображения, отвечающие сингулярным тройкам с максимальными СНЧ, соответствуют, главным образом, низкочастотным составляющим сигнала; *k*-ые составляющие ЦИ, отвечающие тройкам с минимальными (средними по величине) СНЧ, несут в себе, в основном, высокочастотные (среднечастотные) составляющие.

Результат сжатия в соответствии с [15] – это обнуление коэффициентов при высоких (и возможно средних) частотных составляющих в частотной области ЦИ. При использовании ОПАИС сжатие, как и любое другое возмущающее воздействие, формально представимо в виде возмущения сингулярных троек, главным результатом которого является обнуление наименьших (и возможно средних) по величине СНЧ, что приведет к удалению из F *k*-х составляющих (1), где k имеет значения равные или близкие к n (вплоть до сравнимых с $n/2$), что подтверждается результатами вычислительного эксперимента [18]. Таким образом, получено решение задачи 2.

Наибольшее СНЧ практически не возмущаются в процессе сжатия. Это не случайно. Сингулярные тройки, отвечающие максимальным СНЧ, соответствуют,

главным образом, низкочастотным составляющим сигнала, а значит являются наименее чувствительными к сжатию, что принципиально решает задачу 1.

Любое СП в соответствии с ОПАИС определяется совокупностью возмущений СНЧ (СНВ) матрицы контейнера F (или ее подматриц). Учитывая, что рассматриваемая в работе задача связана с процессом сжатия, осуществление которого предполагает предварительное разбиение матрицы ЦИ на 8×8-блоки, результат СП формализуем в виде совокупностей возмущений СНЧ (СНВ) блоков [4]. Для достижения цели работы необходимо выделить из СНЧ (СНВ) 8×8-блоков такие, возмущения которых в ходе СП обеспечат нечувствительность получаемого в результате СС к конкретному возмущающему воздействию – сжатию. В соответствии с полученным выше решением задачи 1 результатом СП без учета визуальных искажений, происходящих в СС, должно быть возмущение наибольших СНЧ. Однако, изменение величины максимального СНЧ в блоках всего на 5-8%, возмущение которого в ходе СП очевидно является наиболее желаемым, как показывает вычислительный эксперимент, приводит к появлению явных артефактов на ЦИ. Такой же порядок относительного изменения второго по величине СНЧ, как правило, не приводит к нарушению надежности восприятия СС [4] (рис. 2).

а **б**

в

Рис. 2. Результат возмущения СНЧ блоков матрицы ЦИ: а – исходное ЦИ; б – возмущению подвергнуто максимальное СНЧ блока; в – возмущению подвергнуто второе по величине СНЧ блока

Таким образом, имеет место следующее утверждение.

Утверждение. Для обеспечения устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС

достаточно производить погружение ДИ таким образом, чтобы формальным результатом СП было возмущение второго (и возможно третьего) по значению СНЧ в сингулярных спектрах блоков матрицы контейнера, полученных после ее стандартного разбиения. Если же СП формально выразится в возмущении средних и наименьших по значению СНЧ, то (при большой вероятности обеспечения надежности восприятия СС) такой СА окажется неустойчивым к сжатию.

Замечание 1. Как правило, результат СП существующих СА представляется в виде возмущения практически всех СНЧ соответствующей матрицы (матриц): ДИ «распределяется» по всем составляющим сингулярного спектра. Такая картина будет наблюдаться, если процесс СП не сводится к непосредственному возмущению конкретных СНЧ, как, например, в [19]. При сравнении потенциальной устойчивости различных СА к возможной атаке сжатием предпочтение следует отдать тому, который в ходе СП более остальных СА возмутит максимальные СНЧ.

Для практического подтверждения истинности сформулированного утверждения был рассмотрен один из наиболее широко распространенных СА, который считается устойчивым к атаке сжатием и часто используется для сравнения с подобными вновь создаваемыми или модифицируемыми алгоритмами [10, 11], – метод Коха (E. Koch) и Жао (J. Zhao) (МКЖ) [3]. МКЖ производит внедрение в коэффициенты дискретного косинусного преобразования (ДКП) средней части частотного спектра 8×8-блоков путем их взаимного изменения. Коэффициенты ДКП, выбранные для внедрения ДИ, задаются своими координатами в 8×8-массиве – $(i_1, j_1), (i_2, j_2)$ (рекомендуемые в [3] для внедрения ДИ коэффициенты (5,4) и (4,5)). Вычислительный эксперимент, в котором участвовало более 200 ЦИ в формате TIF, проводился в среде *MathWorks* MATLAB. После СП полученное СС сохранялось в *Adobe* Photoshop с $Q = 8,9,10,11,12$. Результаты эксперимента представлены в табл. 1.

Таблица 1.

Результаты декодирования секретной информации в методе Коха и Жао

$(i_1, j_1), (i_2, j_2)$	Q	ОВИ (%)	Обеспечение надежности восприятия СС
(5,4), (4,5)	8	54.6339	+
	9	91.7782	+
	10	99.1146	+
	11	99.9362	+
	12	99.9947	+
(3,4), (4,3)	8	71.3798	+
	9	94.9230	+
	10	99.0976	+
	11	99.9126	+
	12	99.9782	+
(2,3), (3,2)	8	98.0660	-
	9	99.7319	-
	10	99.8848	-
	11	99.9132	-
	12	99.9392	-

Проанализируем результаты СП, произведенного МКЖ, с точки зрения их представления в виде совокупности возмущений СНЧ блоков матрицы контейнера и соответствия их сформулированному выше утверждению. В табл. 2 для примера

приведены типичные результаты для одного и того же блока тестируемого ЦИ. Эти результаты полностью соответствуют утверждению. Так МКЖ, использующий для СП коэффициенты ДКП с индексами (4,5) и (5,4) принципиально не мог оказаться устойчивым к сжатию с малым коэффициентом качества, что и было получено ранее при тестировании его работы (табл. 1), т.к. такое СП практически не возмутило наибольшие СНЧ. В соответствии с результатами табл. 2 и утверждением, устойчивым к сжатию должен оказаться МКЖ, использующий коэффициенты ДКП с индексами (2,3) и (3,2), что полностью отвечает результатам его работы на практике (табл. 1) (хотя такой вариант МКЖ не обеспечивает надежность восприятия, а значит является неприемлемым).

Таблица 2.

Возмущения СНЧ блока ЦИ, хранимого в формате TIF, при СП методом Коха и Жао (СС после СП сохраняется без потерь)

$(i_1, j_1), (i_2, j_2)$	Характер восстановления ЦИ при обратном ДКП	Относительные погрешности СНЧ в порядке, отвечающем $\sigma_1, \sigma_2, ..., \sigma_8$ (%)
(5,4), (4,5)	ЧВ	0.0000, 0.0899, 3.7185, 32.0837, 93.2585, 0.0623, 265.5867, 82.1709
	ПВ	0.0000, 0.0362, 3.3645, 27.8843, 97.7085, 0.0402, 258.8111, 93.8611
(3,4), (4,3)	ЧВ	0.0000, 0.3338, 14.9730, 0.5167, 17.2428, 3.2857, 125.4383, 62.1174
	ПВ	0.0000, 0.4575, 14.7477, 0.4936, 11.3472, 1.9157, 148.5082, 62.6708
(2,3), (3,2)	ЧВ	0.0013, 11.4289, 3.2428, 1.3678, 8.1935, 12.7950, 0.2274, 24.0782
	ПВ	0.0013, 11.4957, 2.8944, 1.5089, 2.2150, 13.7399, 7.9410, 25.0259

Заключение

В работе предложен новый подход к решению проблемы обеспечения СА устойчивости к атаке сжатием при его разработке, основанный на ОПАИС, в соответствии с которым любое возмущающее воздействие, направленное на ОС, в частности СП, а также возмущение СС, в частности, его сжатие, рассматривается как возмущение соответствующей матрицы (матриц) контейнера (СС).

Разработанный подход:

- позволил получить достаточное условие обеспечения устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС, которое никак не зависит от используемой для погружения ДИ области контейнера (пространственной или частотной) и конкретики СА, и определяется лишь локализацией и относительной величиной возмущений СНЧ соответствующих матриц ОС, произошедших в ходе СП;
- дал возможность для проведения выбора СС, наименее чувствительного к сжатию: чем большему возмущению в процесс СП подверглись максимальные СНЧ блоков матрицы контейнера, тем менее чувствительно к сжатию полученное СС;
- позволит автоматизировать процесс анализа существующих или разрабатываемых СА с точки зрения их устойчивости к сжатию путем оценки

возмущений различных СНЧ в процессе СП: если СП формально выразится в возмущении максимальных (средних и наименьших) по значению СНЧ блоков матрицы ОС, то соответствующий СА будет устойчивым (неустойчивым) к сжатию.

Список литературы

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 с.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.
3. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 249 с.
4. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.
5. Böhme R. Advanced Statistical Steganalysis. – Berlin: Springer-Verlag, 2010. – 300 p.
6. Ленков С.В. Методы и средства защиты информации [Текст]: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – . –
Т.2: Информационная безопасность. – 2008. – 344 с.
7. Корольов В.Ю. Планування досліджень методів стеганографії та стеганоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького національного університету. Технічні науки. – 2011. – №4. – С. 187-196.
8. Королев В.Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В.Ю. Королев, В.В. Полиновский, В.А. Герасименко // Управляющие системы и машины. – 2011. – №1(231). – С. 79-87.
9. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.
10. Прохожев Н.Н. Влияние внешних воздействий на DC-коэффициент матрицы дискретно-косинусного преобразования в полутоновых изображениях / Н.Н. Прохожев, О.В. Михайличенко, А.Г. Коробейников // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2008. – Вып.56. – С. 57-62.
11. Михайличенко О.В. Алгоритм встраивания цифровых водяных знаков в единичный коэффициент матрицы дискретно-косинусного преобразования / О.В. Михайличенко, Н.Н. Прохожев // Сборник трудов VI Всероссийской конференции молодых ученых. Выпуск 6. Информационные технологии. – СПб. : СПбГУ ИТМО, 2009. – С. 644-648.
12. Кобозєва А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / Інформаційні технології та комп'ютерна інженерія. – 2008. – №1(11). – С. 164-171.
13. Кобозева А.А. Оценка чувствительности стегосообщения к возмущающим воздействиям / А.А. Кобозева, Е.В. Нариманова // Системні дослідження та інформаційні технології. – 2008. – №3. – С. 52-65.
14. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К. : Изд. ГУИКТ, 2009. – 251 с.
15. Гонсалес Р. Цифровая обработка изображений [Текст] : пер. с англ. / Р.С. Гонсалес, Р.Э. Вудс ; ред. пер. ЧоП. А. Чочиа. – М. : Техносфера, 2006. – 1070 с.
16. Кобозева А.А. Метод выявления результатов размытия цифрового изображения / А.А. Кобозева, В.В. Зорило // Сучасна спеціальна техніка. – 2010. – №3(22). – С. 52-63.
17. Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А. Кобозева // Искусственный интеллект. – 2007. – №4. – С. 531-538.
18. Кобозева А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник Национального технического университета «Харьковский политехнический институт»: Сборник научных трудов. Тематический выпуск «Системный анализ, управление и информационные технологии». – 2007. – №18. – С. 81-93.
19. Кобозева А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А. Кобозева // Праці УНДІРТ. – 2006. – №4(48). – С. 44-52.

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ ДО АТАК СТИСКОМ

А.А. Кобозєва

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

На основі загального підходу до аналізу стану й технології функціонування інформаційних систем, розробленого автором раніше, пропонується новий підхід до рішення проблеми стійкості стеганографічних алгоритмів до атаки стиском. В роботі отримані формальні достатні умови малої чутливості стеганоповідомлення до стиску з одночасним забезпеченням його надійності сприйняття. Запропонований підхід дозволить автоматизувати процес аналізу існуючих або розроблювальних стеганографічних алгоритмів з погляду їхньої стійкості до стиску шляхом оцінки збурень сингулярних чисел матриці (матриць) контейнера, що відбулися в процесі стеганоперетворення, а також дасть можливість апріорного вибору з множини стеганоповідомлень найменш чутливого до стиску.
Ключові слова: стеганографічний алгоритм, атака стиском, сингулярні числа

THE PROBLEM OF STEGANOGRAPHIC ALGORITHM STABILITY TO THE COMPRESSION ATTACKS

Alla A. Kobozeva

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

In this paper, 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 which was previously developed by the author. Consequently, we obtain the sufficient conditions for low-sensitivity of stegano message to compression while ensuring the reliability of perception. The proposed approach automates the process of analyzing the existing or emerging steganography algorithms from viewpoint of its resistance to compression. This became possible due to estimation of singular values perturbation of cover's matrix during the stegano transformation process. Additionally the proposed algorithm allows a priori selection of less sensitive to compression stegano messages from their variety.
Keywords: steganography algorithm, compression attacks, singular values