ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.5:518:512.624.3

М.А. Мельник

МЕТОДИКА СРАВНИТЕЛЬНОЙ ОЦЕНКИ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ К СЖАТИЮ

В работе разработана методика сравнительной оценки устойчивости к сжатию различных стеганоалгоритмов, разных реализаций одного стеганометода на основе достаточных условий устойчивости, полученных ранее. Предложенная методика имеет полиномиальную вычислительную сложность. Определены формальные параметры, описывающие состояние контейнера/стеганосообщения, анализ возмущений которых является наиболее информативным для рассматриваемой проблемы. Приведен пример использования методики для различных реализаций стеганографического метода Коха и Жао.

***Ключевые слова**: устойчивость стеганографического алгоритма, сжатие, сингулярные числа, сингулярные векторы, контейнер, стеганопреобразование, матрица, цифровое изображение.*

У роботі розроблено методику порівняльної оцінки стійкості до стиску різних стеганоалгоритмів, різних реалізацій одного стеганометоду на основі достатніх умов стійкості, отриманих раніше. Запропонована методика має поліноміальну обчислювальну складність. Визначено формальні параметри, що описують стан контейнера/стеганоповідомлення, аналіз збурень яких є найбільш інформативним для розглядуваної проблеми. Наведено приклад використання методики для різних реалізацій стеганографічного методу Коха й Жао.

***Ключові слова**: стійкість стеганографічного алгоритму, стиск, сингулярні числа, сингулярні вектори, контейнер, стеганоповідомлення, матриця, цифрове зображення.*

This paper focuses on the development of a comparative evaluation method of steganographic algorithm stability to the compression. The proposed method has a polynomial computational complexity. Formal parameters describing the state of the container / stegano message, perturbation analysis which is the most informative for the problem are defined. An example of the use of method for different implementations of steganographic method Koch and Zhao is given.

***Keywords:** steganographic algorithm stability, compression, singular value, singular vector, cover, stegano transformation, matrix, digital image.*

Введение

Стеганографические методы наряду с криптографическими сегодня являются обязательной составной частью комплексной системы защиты информации.

В процессе стеганографирования дополнительная информация (ДИ), которая является результатом предварительного кодирования конфиденциального сообщения (КС), встраивается в некоторый объект, или контейнер, в качестве которого в настоящей работе рассматривается цифровое изображение (ЦИ), результатом чего является стеганосообщение (СС), которое передается по каналу общего пользования или хранится в таком виде. Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП).

Эффективность любой стеганографической системы, типичный вид которой представлен на рис. 1, зависит от свойств использованного при ее построении стеганографического алгоритма [1]. Системы скрытой передачи данных подвергаются различным атакам. Одна из самых распространенных на сегодняшний день – атака сжатием относится к атакам против встроенного сообщения, направлена на разрушение ДИ [2]. Популярность этой атаки связана с широким распространением в настоящий момент форматов с потерями для хранения и пересылки информации, что не привлекает внимание к ней адресатов. Эта атака является очень эффективной для многих стеганографических систем [1–3]. До настоящего момента остается актуальной не только проблема разработки новых стеганографических алгоритмов, устойчивых к атаке сжатием, в том числе, со значительными коэффициентами, но и задача оценки упомянутого параметра для уже существующих методов и алгоритмов [1].

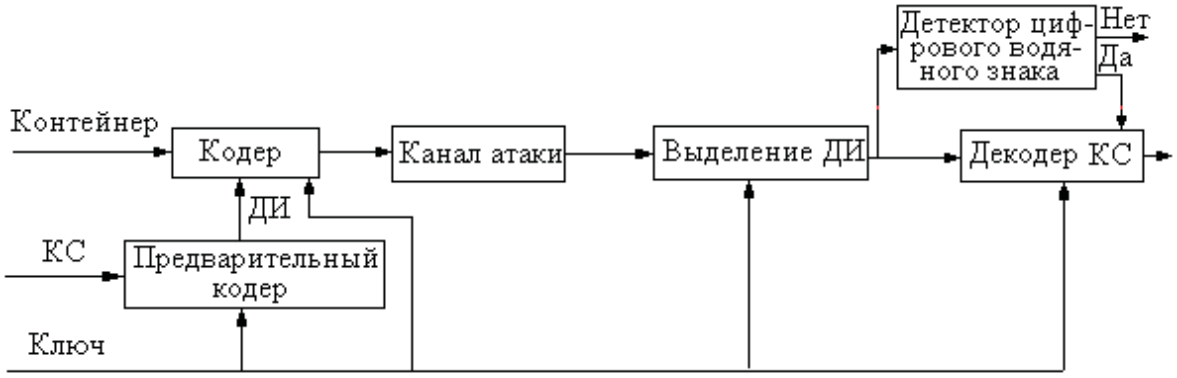

Рис. 1. Основные элементы используемой стеганосистемы

В [4–6] на основе общего подхода к анализу состояния и технологии функционирования информационных систем (ОПАИС) [7] были получены достаточные условия обеспечения устойчивости стеганометода, стеганоалгоритма к сжатию, в том числе, со значительными коэффициентами, в соответствии с которыми эта устойчивость гарантированно обеспечивается тогда, когда процесс СП проводится таким образом, чтобы при формальном представлении его результата в виде совокупности возмущений сингулярных чисел (СНЧ) и/или сингулярных векторов (СНВ) блоков матрицы контейнера, полученных в результате стандартного разбиения [8], эта совокупность содержала возмущения максимальных СНЧ и/или СНВ, отвечающих максимальным СНЧ блоков.

Полученные достаточные условия могут быть использованы как основа для анализа и сравнительной оценки устойчивости к сжатию уже существующих стеганоалгоритмов.

Цель статьи и постановка исследований

Целью настоящей работы является разработка методики сравнительной оценки устойчивости к сжатию различных стеганоалгоритмов, разных реализаций одного стеганометода на основе достаточных условий устойчивости, полученных в [4–6].

Для достижения поставленой цели в работе решаются следующие *задачи*:

1. Определение формальных параметров, описывающих в соответствии с ОПАИС состояние ОС/СС, анализ возмущений которых является наиболее информативным для рассматриваемой проблемы.

2. Обеспечение по возможности малой вычислительной сложности разработанной методики сравнительной оценки устойчивости различных стеганоалгоритмов к сжатию.

Основная часть

Как свидетельствуют результаты вычислительных экспериментов, проводимых для оценки эффективности стеганоалгоритмов, разработанных на основе достаточных условий устойчивости к сжатию [9, 10], наиболее устойчивым к сжатию со значительными коэффициентами является алгоритм, основанный на sign-нечувствительности левых и правых СНВ u_1, v_1, соответственно, блоков матрицы ЦИ, отвечающих максимальным СНЧ [6, 9], а значит, основной при анализе устойчивости стеганоалгоритма будет оценка возмущений именно указанных СНВ.

Методика формальной сравнительной оценки устойчивости стеганоалгоритмов $A_1,...,A_k$ к сжатию.

1. Представить результаты стеганопреобразования ЦИ при помощи алгоритмов $A_1,...,A_k$ в виде совокупности возмущений СНЧ и/или СНВ матриц 8×8 – блоков, полученных в результате стандартного разбиения матрицы контейнера.

2. Для каждого из стеганоалгоритмов A_i, $i = 1,...,k$:

Определить средние значения $U^{(i)}$, $V^{(i)}$ соответственно возмущений левого и правого СНВ $u_1^{(i)}$, $v_1^{(i)}$, отвечающих максимальному СНЧ $\sigma_1^{(i)}$ блока, в процессе СП, выполненного алгоритмом A_i.

3. Определить значения следующих параметров:

$$u = \arg\max_{1\le i\le k} U^{(i)}; \quad (2)$$

$$v = \arg\max_{1\le i\le k} V^{(i)}. \quad (3)$$

4. Если

$\max\limits_{1\le i\le k} U^{(i)} \neq 0$, $\max\limits_{1\le i\le k} V^{(i)} \neq 0$,

то

наиболее устойчивыми к сжатию являются алгоритмы A_u, A_v (если $\max\limits_{1\le i\le k} U^{(i)}$, $\max\limits_{1\le i\le k} V^{(i)}$ в формулах (2), (3) определяются неоднозначно, то в качестве u, v может использоваться любой из возможных вариантов);

иначе

4.1. Для каждого из стеганоалгоритмов A_i, $i = 1,...,k$:

Определить средние значения $S_{\sigma 1}^{(i)}, S_{\sigma 2}^{(i)}$ соответственно возмущений двух наибольших СНЧ $\sigma_1^{(i)}, \sigma_2^{(i)}$ блоков ОС в результате СП, выполненного алгоритмом A_i.

4.2. Определить значения следующего параметра:

$$m = \arg\max_{1 \le i \le k} S_{\sigma 1}^{(i)}; \qquad (1)$$

4.3. Наиболее устойчивым к сжатию является алгоритм A_m (если $\max\limits_{1 \le i \le k} S_{\sigma 1}^{(i)}$ в формуле (1) определяется неоднозначно, то из всех полученных вариантов нужно выбрать тот, для которого значение $S_{\sigma 2}^{(m)}$ максимально).

Вычислительная сложность T реализации предложенной методики в предположении проведения анализа возмущений как СНЧ, так и СНВ блоков матрицы ЦИ-контейнера будет определяться количеством 8×8 блоков матрицы (матриц) ЦИ-контейнера и количеством анализируемых алгоритмов, и составит

$$T = k \cdot \underline{O}\left(n^2\right)$$

операций, если матрица ОС имеет размеры пикселей.

При оценке возмущений только СНВ блоков матрицы контейнера количество операций будет сравнимо с $\frac{2T}{3}$.

Замечание 1. Как показывает вычислительный эксперимент, сравнительный анализ устойчивости стеганоалгоритмов к сжатию может быть сведен к анализу произошедших в результате СП возмущений только СНЧ (шаг 4), на что, при грубой оценке, пойдет $\frac{T}{3}$ операций.

Замечание 2. Если в качестве контейнера используется цветное ЦИ, то его формальным представлением является не одна, а несколько матриц (например, для формата RGB – 3). Это никоим образом не ограничивает область применения предложенной методики: в этом случае анализу могут подвергаться все матрицы ЦИ. Однако если стеганоалгоритм использует для СП все матрицы ЦИ, то их возмущения качественно происходят одинаково с точки зрения устойчивости получаемого результата СП к сжатию [2, 3]. Поэтому для сокращения вычислительной сложности при анализе возможно использование только одной из матриц и в случае цветного ЦИ.

В качестве иллюстративного примера использования разработанной методики рассмотрим различные реализации метода Коха и Жао, который позиционируется как устойчивый к сжатию и часто используется для сравнения с аналогами [3]. Внедрение ДИ осуществляется здесь за счет модификации коэффициентов дискретного косинусного преобразования блоков матрицы контейнера с индексами $(i_1, j_1), (i_2, j_2)$. Реализация этого метода для случая $(i_1, j_1) = (3,4), (i_2, j_2) = (4,3)$, рекомендуемого в [3], обеспечивающего надежность восприятия формируемого СС, и его тестирование, результаты которого приведены в табл. 1, говорят о его недостаточной устойчивости к сжатию со значительными коэффициентами. При этом тестирование алгоритма включало в себя сохранение получаемого рассматриваемым стеганоалгоритмом СС в формат Jpeg с различными коэффициентами

качества *QF* в общедоступном графическом редакторе IrfanView, а эффективность оценивалась стандартным образом при помощи коэффициента корреляции *NC* для ДИ [11]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t},$$

где $p_1, p_2, ..., p_t$; $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $p_i, \overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, – соотвественно погруженная и декодированная из стеганосообщения ДИ; $p_i' = 1, \overline{p}_i' = 1$, если $p_i = 1, \overline{p}_i = 1$, и $p_i' = -1, \overline{p}_i' = -1$, если $p_i = 0, \overline{p}_i = 0$, т.е. $p_i' \times \overline{p}_i' \in \{1,-1\}$.

Таблица 1

Результаты тестирования метода Коха и Жао для реализации
$(i_1, j_1) = (3,4), (i_2, j_2) = (4,3)$

QF	60	70	80	90
NC	0.70	0.95	0.99	0.99

Полученные результаты легко объяснимы при помощи предложенной методики.

Для анализа результатов стеганопреобразования, произведенного методом Коха и Жао при различных реализациях A_1, A_2, A_3, каждая из которых определяется конкретным выбором пары (i_1, j_1), (i_2, j_2) они представлялись в виде совокупности возмущений только СНЧ блоков матрицы контейнера. Для полученной совокупности оценивались относительные возмущения наибольших СНЧ блоков – σ_1, σ_2. В табл.2 для примера приведены типичные результаты для одного и того же блока тестируемого ЦИ (СС после СП сохранялось без потерь). Результаты для средних значений относительных возмущений σ_1, σ_2 качественно не отличаются от приведенных в табл. 2.

Таблица 2

Возмущения СНЧ блока ЦИ, хранимого в формате TIF, при СП, осуществляемом различными реализациями метода Кахо и Жао

Реализация	Задействованные в процессе СП коэффициенты ДКП – $(i_1, j_1), (i_2, j_2)$	Относительные возмущения СНЧ (%)	
		σ_1	σ_2
A_1	(5,4), (4,5)	0.0000	0.0166
A_2	(3,4), (4,3)	0.0000	0.6575
A_3	(2,3), (3,2)	0.0014	12.3245

При сравнении результатов для различных $(i_1, j_1), (i_2, j_2)$ с применением разработанной методики получаем: $\arg\max_{1\le i\le 3} S_{\sigma 1}{}^{(i)} = 3$, что говорит о наибольшей устойчивости к сжатию реализации метода Коха и Жао для случая, когда $(i_1, j_1) = (2,3), (i_2, j_2) = (3,2)$, и наименьшей устойчивости для случая $(i_1, j_1) = (4,5), (i_2, j_2) = (5,4)$, что полностью отвечает результатам его работы на практике (табл. 3) и согласуется с невысокими показателями эффективности уже при $QF = 60$, приведенными в табл.1 для пары коэффициентов ДКП с индексами (3,4), (4,3).

Таблица 3

Результаты декодирования дополнительной информации в методе Кахо и Жао при различных значениях коэффициента качества QF, используемого при организации атаки сжатием на стеганосообщение.

$(i_1, j_1), (i_2, j_2)$	*QF*	*NC*	Обеспечение надежности восприятия СС
(5,4), (4,5)	60	0.5316	+
	70	0.9002	+
	80	0.9846	+
	90	0.9901	+
(3,4), (4,3)	60	0.7038	+
	70	0.9512	+
	80	0.9909	+
	90	0.9937	+
(2,3), (3,2)	60	0.9403	–
	70	0.9773	–
	80	0.9929	–
	90	0.9994	–

Необходимо заметить, что использование рассматриваемого метода Коха и Жао в реализации, основанной на возмущении пары коэффициентов дискретного косинусного преобразования с индексами (2,3), (3,2), являющееся наиболее устойчивым к сжатию (табл. 3), невозможно из-за нарушения надежности восприятия формируемого им СС.

Заключение

В работе на основе общего подхода к анализу состояния и технологии функционирования информационных систем предложена методика сравнительной оценки устойчивости стеганоалгоритмов к атаке сжатием, которая нашла подтверждение своей состоятельности при ее использовании на практике для сравнения различных реализаций хорошо известного стеганометода Коха и Жао.

Предложенная методика может быть применена не только в случае использования в качестве контейнера цифрового изображения, но и цифрового видео, с учетом его представления в виде последовательности кадров.

Нет принципиальных возражений против использования методики для цифрового аудио в случае его представления в двумерном матричном виде, однако

здесь требует решения вопрос о наиболее эффективном матричном представлении аудио с учетом рассматриваемой задачи [12].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 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.

2. *Грибунин В.Г.* Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

3. *Конахович Г.Ф.* Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.

4. *Кобозева А.А.* Формальные условия обеспечения устойчивости стеганометода к сжатию / А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. – 2012. – № 4(31). – С. 60–69.

5. *Кобозева А.А.* Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2012. – Вип. 38. – С. 193–203.

6. *Кобозева А.А.* Анализ чувствительности сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / А.А. Кобозева, М.А. Мельник // Захист інформації. – 2013. – Том 15, № 2. – С. 88–96.

7. *Кобозева А.А.* Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. – К. : ГУИКТ, 2009. – 251 с.

8. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс ; пер. с англ. П.А. Чочиа. – М. : Техносфера, 2006. – 1070 с.

9. *Мельник М.А.* Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / М.А. Мельник // Інформатика та математичні методи в моделюванні. – 2013. – Том 3, № 2. – С. 146–155.

10. *Мельник М.А.* Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – № 2(8). – С. 99–106.

11. *Fan, C.-H.* A robust watermarking technique resistant Jpeg compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // Journal of Information Science and Engineering. – 2011. – Vol. 27, Iss. 1. – PP. 163–180.

12. *Кобозева А.А.* Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. В. Даля. – 2008. – № 8(126), Ч. 1. – С. 62–72.

Отримано 19.11.2013.