УДК 004.056.5

М.А. Мельник, А.С. Головатюк, В.Р. Чабан

Одесский национальный политехнический университет, Одесса

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОАЛГОРИТМА К СЖАТИЮ

В статье рассматриваются разработка теоретических основ обеспечения устойчивости стеганографических методов и алгоритмов к атаке сжатием, в том числе, со значительным коэффициентом. Получены достаточные условия обеспечения устойчивости стеноалгоритма к сжатию с одновременным обеспечением надежности восприятия формируемого стеганосообщения, которые не зависят от используемой для погружения дополнительной информации области контейнера.

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

Введение

Существующие стеганографические методы, являясь одной из основных составных частей современной комплексной системы защиты информации, определяют сегодня одно из наиболее востребованных, перспективных направлений информационной безопасности. В настоящий момент стеганография переживает период своего бурного развития, связанный как с ограничением и даже законодательным запретом шифрования во многих странах мира, так и с возникновением необходимости защиты прав собственности на информацию, представленную в цифровом виде [1 – 4].

Целью статьи является разработка теоретических основ обеспечения устойчивости стеганографических методов и алгоритмов к атаке сжатием

Основная часть

Достижение поставленной цели очевидно позволит повысить эффективность работы организуемого скрытого канала связи в рамках открытого канала в условиях активных атакующих действий, определяемую эффективность соответствующей стеганосистемы. Эффективность стеганосистемы в работе оценивается ее устойчивостью к сжатию, которая определяется устойчивостью к сжатию алгоритма, на основе которого построена стеганосистема, характеризуемой коэффициентом корреляции для цифрового изображения (ЦИ) [1].

Необходимо привести анализ свойств сингулярных чисел блоков, полученных при стандартном разбиении матрицы цифрового изображения.

Пусть $F\ (n \times n)$ – матрица ЦИ. Предварительным шагом при организации сжатия, как правило, является разбиение матрицы изображения на блоки [2]. Обозначим B – матрицу отдельного 8×8 – блока. Для каждого блока строим единственное нормальное сингулярное разложение [2]:

$$B = U\Sigma V^T, \qquad (1)$$

где U, V – ортогональные матрицы размером 8×8, столбцы $u_1,...,u_8$ матрицы U, левые сингулярные векторы (СНВ) B лексикографически положительны [4]; $\Sigma = \mathrm{diag}(\sigma_1(B),...,\sigma_8(B))$, при этом

$$\sigma_1(B) \geq ... \geq \sigma_8(B) \geq 0, \qquad (2)$$

σ – сингулярные числа (СНЧ) B.

Результат стеганопреобразования, как и сжатия формализуем далее в виде совокупностей возмущений СНЧ и СНВ множества блоков [3]. Для достижения цели работы необходимо выделить из СНЧ, СНВ 8×8-блоков наименее чувствительные к сжатию, возмущения которых в результате стеганографического преобразования (СП) обеспечат нечувствительность к сжатию получаемого стеганосообщения (с учетом требования его надежности восприятия). Действительно, если СП будет проводиться таким образом, что его формальным выражением будет возмущение именно этих параметров, то естественно ожидать, что при сжатии стеганосообщения погруженная в него дополнительная информация не пострадает или пострадает незначительно по сравнению с другими вариантами стеганопреобразования, что и является основной идеей для получения последующих результатов. СНЧ B являются хорошо обусловленными в соответствии с соотношением [1]:

$$\max_{1 \leq j \leq 8} \left| \sigma_j(B) - \sigma_j(B + \Delta B) \right| \leq \left\| \Delta B \right\|_2, \qquad (3)$$

где ΔB – матрица возмущающего воздействия для блока B (в частности, матрица возмущения блока B при сжатии), $\left\| \bullet \right\|_2$ - спектральная матричная норма [1], $\sigma_j(B + \Delta B)$, $j = \overline{1,8}$, - СНЧ матрицы $B + \Delta B$. Наиболее ярко особенности возмущений при сжатии проявляются для наименьших СНЧ: их значения становятся сравнимы друг с другом и близки к нулю Кроме того, данная ситуация может значительно затруднить (или даже сделать невозможным) про-

цесс декодирования ДИ, связанный с учетом порядка СНЧ в блоке [3]. Таким образом, процесс стеганопреобразования должен быть проведен так, чтобы при его формальном представлении в виде совокупности возмущений СНЧ блоков матрицы контейнера, значения этих возмущений были таковыми, чтобы не вызывали изменения взаимного порядка СНЧ, т.е. абсолютные значения этих возмущений должны быть меньше отделенностей возмущаемых СНЧ. В то же время эти возмущения должны быть больше, чем возмущения СНЧ при сжатии. Для установления возможности одновременного удовлетворения этим двум требованиям был проведен вычислительный эксперимент, в котором 250 ЦИ в формате без потерь (TIF, BMP) пересохранялись в формат JPEG с потерями с различными коэффициентами качества QF. Затем матрица каждого из пары соответствующих ЦИ (одно – в формате без потерь, другое – в формате с потерями) разбивалась стандартным образом на блоки. Определялось возмущение $\|\Delta B\|_2$ каждого блока при сжатии для каждого конкретного значения QF.

Исходя из результатов возможных возмущений при сжатии с учетом соотношения (3), можно сделать вывод, что при формализации процесса СП в виде возмущений СНЧ блоков для обеспечения устойчивости стеганоалгоритма к сжатию при $QF \geq 60$, эти возмущения должны превосходить 72, чтобы существовала принципиальная возможность для осуществления эффективного декодирования ДИ. Таким образом, чтобы избежать нарушения первоначального порядка СНЧ, процесс СП (с учетом возможности сжатия стеганосообщения с малыми коэффициентами качества) достаточно проводить таким образом, чтобы при формальном представлении результатов стеганопреобразования в виде совокупности возмущений СНЧ блоков матрицы ОС требуемые для «перекрытия сжатия» значительные возмущения претерпевали только максимальные СНЧ блоков $\sigma_1(B)$ (и возможно $\sigma_2(B)$), поскольку за счет величин их значений и значений их отделенностей изменение их взаимного порядка после СП можно легко избежать: для $\sigma_1(B)$ никаких ограничений не выдвигается, а возмущение $\sigma_2(B)$ желательно проводить в сторону увеличения его значения. Допустимая величина возмущений максимальных СНЧ, происходящих в результате погружения ДИ, должна быть установлена с учетом требования соблюдения надежности восприятия формируемого стеганосообщения [4]. Проверим принципиальную возможность проводить возмущения максимальных СНЧ блоков так, чтобы «перекрыть возмущения сжатия» и обеспечить надежность восприятия СС.

Исходя из вычислений и экспериментальным путём было для того, чтобы стеганографический алгоритм был устойчивым к сжатию, достаточно производить стеганопреобразование так, чтобы его формальным представлением была совокупность возмущений СНВ блоков ЦИ-контейнера, отвечающих максимальным СНЧ этих блоков [5].

Процесс СП должен строиться таким образом, чтобы для СС обеспечивалась надежность восприятия. В силу этого необходимо получить, в первую очередь, качественные оценки возможного возмущения u_1 при организации процесса погружения ДИ.

Для того, чтобы стеганосообщение было нечувствительным (малочувствительным) к сжатию достаточно, чтобы процесс стеганопреобразования был организован таким образом, чтобы формальным представлением его являлась совокупность возмущений левых и/или правых сингулярных векторов блоков матрицы контейнера, отвечающих максимальным сингулярным числам (σ_1) блоков, при этом возмущения сингулярных векторов, происходящие в результате погружения ДИ, должны оставлять их в малой окрестности n-оптимального вектора, что обеспечит надежность восприятия сформированного стеганосообщения. Если же при формальном представлении стеганопреобразования в виде совокупности возмущений СНВ блоков матрицы контейнера, эти возмущения будут отвечать СНВ для которых сингулярные числа имеют малую отделенность, то сформированное стеганосообщение окажется чувствительным, а соответствующий стеганоалгоритм неустойчивым к сжатию.

Выводы

Получены оценки возмущений сингулярных чисел и сингулярных векторов блоком матрицы цифрового изображения при атаке сжатием на стеганосообщение при различных коэффициентах качества, используемых при сжатии. Эти оценки дают принципиальную возможность организации процесса стеганопреобразования за счет бóльших возмущений сингулярных чисел и сингулярных векторов, обеспечивающего надежность восприятия стеганосообщения.

Из совокупности формальных параметров, возмущения которых определяют результат стеганопреобразования, - сингулярных чисел и сингулярных векторов соответствующих матриц, отвечающих контейнеру, выделены наименее чувствительные к операции сжатия (наиболее пригодные для возмущений в процессе стеганопреобразования) – максимальные сингулярные числа, сингулярные векторы, отвечающие максимальным сингулярным числам блоков контейнера.

Получена возможность для формального анализа уже существующих (определения необходимых корректировок стеганоалгоритма в случае его неустойчивости к сжатию), а также разрабатываемых алгоритмов с точки зрения их устойчивости к сжатию путем оценки возмущений различных сингу-

лярных чисел, сингулярных векторов в процессе стеганопреобразования: если погружение дополнительной информации формально выразится в возмущении максимальных (средних и наименьших) по значению сингулярных чисел блоков матрицы контейнера и/или сингулярных векторов, отвечающих максимальным (наименьшим (средним по значению)) сингулярным числам блоков, то соответствующий стеганографический алгоритм будет устойчивым (неустойчивым) к сжатию.

Список литературы

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

2. 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 імені Т. Шевченка. – 2012. – Вип. 38. — С. 193-203.

3. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99-106.

4. Мельник М.А. Методика сравнительной оценки устойчивости стеганографических алгоритмов к сжатию / М.А. Мельник // Сучасна спеціальна техніка. – 2013. – №4. – С. 67-74.

Поступила в редколегию 29.02.2016

Рецензент: д-р техн. наук, проф. В.В. Скачков, Военная академия, Одесса.

ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГАНОАЛГОРИТМА ДО СТИСНЕННЯ

М.О. Мельник, Г.С. Головатюк, В.Р. Чабан

У статті розглядаються розробка теоретичних основ для забезпечення стійкості стеганографічних методів і алгоритмів до атаки стисненням, в тому числі, зі значним коефіцієнтом. Отримано достатні умови забезпечення стійкості стеноалгорітма до стиснення з одночасним забезпеченням надійності сприйняття формованого стеганосообщенія, які не залежать від використовуваної для занурення додаткової інформації області контейнера.

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

THEORETICAL THROUGH BASICS WHICH PROVIDE THE STEGANOGRAPHY ALGORITHM TO COMPRESSION

M.O. Melnyk, A.S. Golovatyuk, V.R. Chaban

Abstract This paper focuses on development of the theoretical foundations of sustainability steganographic methods and algorithms for compression of the attack, including a significant factor. Sufficient conditions to ensure stability of the wall of the algorithm to compress while ensuring the reliability of perception formed by quilted messages that do not depend on your dive details area of the container

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