The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message

Bobok I., Kobozieva A., Sokalsky S.
Odessa Polytechnic National University
Odessa, Ukraine

Abstract. Steganography is the perspective area of information security. The reliability of the steganographic system, its stability is affected by the carrier – a container, which is considered in the paper as a digital image. The aim of the work is to increase the resistance of a steganographic system to attacks against an embedded message by developing a method for choosing a container from a finite set of available digital images that ensures the transmitted message the minimum (close to the minimum) possible sensitivity of the generated steganographic message to disturbing influences under consideration with the selected steganographic algorithm. The goal was achieved using a theoretical study of perturbations of the formal parameters of the container matrix, as a result of steganographic transformation and active attacks, which made it possible to introduce a new formal representation for information protected from perturbing influence *E*, as the difference of low-rank approximations of container matrices and steganographic messages. The most important result of the work is the development of a container selection method ready for practical implementation. The efficiency of the developed method exceeds the efficiency of analogs, it remains high, regardless of the used steganographic method, which allows increasing the overall resistance of the steganographic system to attacks against the embedded message. The significance of the obtained result lies in the use of the developed method of increasing the stability of the steganographic system to attacks against the embedded message.
Keywords**:** steganographic method, digital message, choice of container, resistance of the stegano system, singular value, singular vector.

DOI: https://doi.org/10.52254/1857-0070.2022.4-56.07
UDC: 004.056

Problema alegerii unui container steganografic în fața atacurilor împotriva unui mesaj încorporat

Boboc I.I., Kobozeva A.A., Sokalsky S.N.
Universitatea Națională ”Odeskaia Politehnika”, Odesa, Ucraina

Rezumat. Astăzi, sarcina de a proteja informațiile de accesul neautorizat, modificările neautorizate devine din ce în ce mai complexă, acoperind toate sferele activității umane. Evident, sectorul energetic, care este parte integrantă a infrastructurii critice a oricărui stat, este deosebit de sensibil la calitatea sistemelor de securitate a informațiilor. Unul dintre cele mai promițătoare domenii în securitatea informațiilor este steganografia.. Scopul lucrării este de a creşte rezistența unui sistem steganografic la atacurile împotriva unui mesaj încorporat prin dezvoltarea unei metode de alegere a unui container dintr-un set finit de imagini digitale disponibile care asigură mesajului transmis minim/aproape de minimum posibil. sensibilitatea mesajului steganografic generat la influențele perturbatoare pentru imaginile E luate în considerare cu algoritmul steganografic selectat. Scopul a fost atins prin: studiul teoretic al perturbațiilor parametrilor formali ai matricei container, obținute folosind descompunerea valorii sale normale singulare şi definirea unică a matricei, ca urmare a stego-transformarii şi a atacurilor active, care a făcut posibilă introducerea unei o nouă reprezentare formală a informațiilor protejate de influența perturbatoare, ca diferența de aproximări de rang scăzut ale matricelor de container şi steganomesaj, unde rangul aproximărilor este determinat de numărul de valori singulare ale matricei de container care au o separare suficientă în ceea ce privește către E. Cel mai important rezultat al lucrării este dezvoltarea unei metode de selecție a containerelor pregătită pentru implementare practică. Eficiența metodei dezvoltate depăşeşte eficiența analogilor şi rămâne ridicată, indiferent de metoda steganografică utilizată pentru steganoconversie. Semnificația rezultatului obținut constă în asigurarea prin utilizarea metodei dezvoltate de creştere a stabilității steganosistemului împotriva atacurilor împotriva mesajului încorporat.
Cuivinte-cheie**:** metoda steganografică, imagine digitală, alegere container, stabilitate steganosistem, valoare singulară, vector singular.

Задача выбора стеганографического контейнера в условиях атак против встроенного сообщения

Бобок И.И., Кобозева А.А., Сокальский С.Н.
Национальный университет «Одесская политехника»
Одесса, Украина

***Аннотация*.** На сегодняшний день задача защиты информации от несанкционированного доступа, несанкционированного изменения становится все более сложной, охватывающей все сферы человеческой деятельности. Очевидно, что энергетическая сфера, являющаяся составной частью критической инфраструктуры любого государства, является особенно чувствительной к качеству систем защиты информации. Одним из наиболее перспективных направлений в обеспечении информационной безопасности является стеганография. Существенное влияние на надежность стеганосистемы, ее устойчивость оказывает носитель – контейнер, в качестве которого в работе рассматривается цифровое изображение. Выбор контейнера позволяет в наибольшей степени обеспечить различные требования, выдвигаемые к получаемому стеганосообщению. Целью работы является повышение устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки метода выбора контейнера из конечной совокупности имеющихся цифровых изображений, обеспечивающего для передаваемого сообщения минимальную/близкую к минимально возможной для рассматриваемых изображений чувствительность формируемого стеганосообщения к возмущающим воздействиям при выбранном стеганографическом алгоритме. Поставленная цель была достигнута путем: теоретического исследования возмущений формальных параметров матрицы контейнера, получаемых при помощи ее нормального сингулярного разложения и однозначно определяющих матрицу, в результате стеганопреобразования и активных атак, что дало возможность для введения нового формального представления для информации, защищенной от возмущающего воздействия E, как разности малоранговых аппроксимаций матриц контейнера и стеганосообщения, где ранг аппроксимаций определяется количеством сингулярных чисел матрицы контейнера, имеющих достаточную отделенность по отношению к E. Наиболее важным результатом работы является разработка метода выбора контейнера, готового к практической реализации. Эффективность разработанного метода превышает эффективность аналогов и остается высокой, независимо от используемого для стеганопреобразования стеганографического метода. Значимость полученного результата заключается в обеспечении за счет использования разработанного метода повышения устойчивости стеганосистемы к атакам против встроенного сообщения.

Ключевые слова: стеганографический метод, цифровое изображение, выбор контейнера, устойчивость стеганосистемы, сингулярное число, сингулярный вектор.

ВВЕДЕНИЕ

В современных условиях бурного развития информационных технологий задача защиты информации от несанкционированного доступа, несанкционированного изменения становится все более сложной и многогранной, требующей системного и комплексного подхода [1-3].

Составной частью любой современной комплексной системы защиты информации является стеганографическая система [4-6], дающая возможность скрыть сам факт наличия секретной информации «под маской» не привлекающего внимание контейнера, в качестве которого при организации скрытого (стеганографического) канала связи в сегодняшней стеганографии используются, как правило, цифровые контенты – изображения (ЦИ), видео, аудио. Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к ней будет только усиливаться [7], основными причинами чего являются: ограничение (вплоть до запрещения) на использование криптосредств в ряде стран мира, проблемы защиты прав собственности на информацию, которая представлена в цифровом виде, объемы и ценность которой непрерывно возрастают.

Стеганография является наиболее перспективным направлением в обеспечении безопасности информации в современных системах и сетях [8].

Процесс стеганографирования в общем случае состоит из нескольких этапов [9]: выбор (если таковой возможен) контейнера, в качестве которого в настоящей работе рассматривается ЦИ, так как существенное влияние на надежность стеганосистемы, возможность обнаружения факта передачи скрытого сообщения, на другие ее характеристики оказывает именно носитель; предварительное кодирование передаваемой информации, в результате которого, как правило, получается бинарная цифровая последовательность – дополнительная информация (ДИ); непосредственное встраивание ДИ в контейнер, результатом чего является стеганосообщение (СС).

Используемые при организации скрытого канала связи контейнеры могут быть трех типов [9]: случайный, навязанный и выбранный. При этом очевидно, что именно выбранный контейнер позволит в наибольшей степени обеспечить требования, выдвигаемые к получаемому СС. Так существует принципиальная возможность подбора контейнера таким образом, чтобы он в своем оригинальном виде уже содержал нужную ДИ в соответствии с используемым секретным ключом, тем самым аннулируя для стеганоаналитика возможность выявления факта наличия ДИ (однако на практике такая возможность используется крайне редко ввиду значительной вычислительной сложности ее реализации).

Единого мнения о том, каким должен быть «идеальный» контейнер, нет [10], да оно и не может быть сформировано, поскольку приоритетные требования, которые ставятся к СС, для различных условий его получения и использования так же различны [9,11]. Задача выбора контейнера всегда решается с учетом приоритетности требований, предъявляемых к СС в конкретных условиях его использования, среди которых: обеспечение надежности восприятия (СС не должно визуально отличаться от контейнера), устойчивость к стеганоанализу, устойчивость к атакам против встроенного сообщения [9,12] и т.д. На взгляд авторов статьи, именно атаки против встроенного сообщения заслуживают на сегодняшний день наибольшего внимания. Действительно, надежность восприятия СС обязан обеспечивать каждый контейнер, входящий в область применимости используемого стеганографического алгоритма. Если это не так, то такой стеганоалгоритм просто не имеет право на существование. Стеганоаналитическая атака (отличная от визуальной) требует от атакующего наличия специфических программных, технических средств выявления (наличия) скрытой информации, а также соответствующей квалификации, что явно сужает круг таких атак. Что же касается атак против встроенного сообщения, то они могут быть проведены без какого-либо специфического оборудования, программного обеспечения, специфической квалификации атакующего, например, атака сжатием с потерями, что делает такие атаки широко распространенными, чрезвычайно актуальными, одними из тех, с которыми надо бороться в первую очередь, в том числе, за счет выбора контейнера, обеспечивающего малую чувствительность СС к возмущающим воздействиям. Под чувствительностью СС здесь и далее понимается чувствительность задачи декодирования ДИ.

Задача выбора контейнера находится в поле зрения многих современных ученых-стеганографов. Так в [13] рассматривается вопрос выбора контейнера для повышения безопасности стеганографической системы. Данные контейнера моделируются как процесс Гаусса-Маркова. Основная цель выбора контейнера – обеспечение/повышение устойчивости стеганосистемы к стеганоанализу. Вопросы устойчивости к атакам против встроенного сообщения в работе не поднимаются, как и в [10], где рассматривается вопрос выбора контейнера из определенного набора ЦИ для заданного секретного сообщения с целью обеспечения высокого качества визуального восприятия СС, а также устойчивости к стеганоанализу. Выбор осуществляется путем двухшаговой процедуры. На первом шаге происходит фильтрация потенциальных контейнеров с учетом их гистограмм. На втором – анализируются характеристики интенсивности пикселей, выделенных предварительно блоков. Для повышения вероятности сохранения надежности восприятия СС при встраивании ДИ проводятся дополнительные геометрические преобразования блоков, что, хотя и обеспечивает эффективный выбор контейнера в соответствии с выдвинутыми авторами требованиями, но никак не гарантирует устойчивости формируемого СС к возмущающим воздействиям.

В [14] рассмотрен вопрос выбора контейнера для обеспечения максимально возможной устойчивости стеганосистемы к пасивным атакам, при этом большое внимание уделено форматам, в которых хранятся контейнеры. Вопросы устойчивости к активным атакам вновь игнорируются. При этом какой-либо конкретный метод выбора контейнера в работе не предлагается.

В [15] выбор контейнера делается для одного стеганометода Бенгама-Мемона-Эо-Юнга, который авторы предварительно модифицируют, используя для внедрения информации вместо области дискретного косинусного преобразования область

дискретного вейвлет-преобразования. Выбор контейнера здесь сводится к формулировке требований к ЦИ, т.е. по сути – к получению ограничений на область использования модифицированного метода и не может рассматриваться как вариант решения задачи в целом.

В [16] был предложен метод, позволяющий из имеющегося множества контейнеров выбрать тот, который обеспечит относительную устойчивость получаемого СС к предполагаемым атакам против встроенного сообщения. Значительным преимуществом метода является отсутствие ограничений на область применения не только в смысле используемого стеганографического алгоритма, но и в смысле конкретики атак против встроенного сообщения, в силу чего этот метод заслуживает особого внимания.

Метод основан на возможности формального представления стеганопреобразования контейнера с $n\times n$-матрицей F, независимо от используемого стеганометода и выбранной области для погружения ДИ (пространственной, области преобразования), в виде:

$$\overline{F} = F + \Delta F, \qquad (1)$$

где $\overline{F}$ - $n\times n$-матрица СС, ΔF - $n\times n$-матрица возмущения, произошедшего в результате внедрения ДИ в контейнер. В работе введено понятие объема защищенной от возмущающего воздействия E информации (ЗИ) с использованием понятий защищенного от E собственного вектора (СВ), отвечающего собственному значению (СЗ) с достаточной абсолютной отделенностью, для матрицы рассматриваемого цифрового контента после ее предварительной симметризации. В [16] показано, что, в основном, с ростом величины объема ЗИ возрастает и устойчивость СС к атакам против встроенного сообщения. Однако указанная зависимость не является прямой, здесь возможна ситуация, когда ЦИ-контейнеру с максимальным объемом ЗИ отвечало СС, количественный показатель устойчивости которого, определяемый объемом правильно декодированной информации, был значительно меньше максимально возможного значения этого показателя для рассматриваемого множества контейнеров. Причины этого частично были исследованы в [17], где была предпринята попытка учесть и устранить выявленные недочеты, допущенные в [16], среди которых: необоснованное использование абсолютных отделенностей СЗ матрицы при расчете объема ЗИ; условие выбора защищенных СВ, не использующее индивидуальные характеристики изображения и др. Однако к повышению эффективности процесса выбора контейнера это практически не привело, причиной чего является то, что изменения, внесенные в принцип расчета объема ЗИ касались лишь очень незначительной части СЗ, СВ, которые учитывались при расчетах. При этом СЗ с наибольшей абсолютной отделенностью и соответствующих им СВ, которые являются нечувствительными к любым возмущающим воздействиям, это никак не коснулось. Кроме того, удаление из рассмотрения СЗ в каком бы то ни было качестве, по мнению авторов данной статьи, является «шагом назад» в процессе повышения эффективности выбора контейнера по сравнению с [16], т.к. приводят к игнорированию совокупности параметров, возмущения которых являются составной частью формального представления результата стеганопреобразования [16].

Таким образом, задача выбора из имеющейся совокупности потенциальных ЦИ-контейнеров такого, который для заданной ДИ обеспечит наименьшую чувствительность к возмущающим воздействиям формируемого СС, является такой, которая не имеет окончательного решения, остается актуальной для повышения эффективности стеганосистемы в целом.

Целью работы является повышение устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки метода выбора контейнера из конечной совокупности K имеющихся ЦИ, обеспечивающего для заданной ДИ минимальную/близкую к минимально возможной для ЦИ из K чувствительность формируемого СС к возмущающим воздействиям при выбранном стеганографическом алгоритме. При этом эффективность разработанного метода не должна зависеть от конкретики используемого при формировании СС стеганоалгоритма.

В качестве основного показателя эффективности метода выбора контейнера будем рассматривать отклонение количественного показателя (определяемого ниже) чувствительности СС к возмущающему воздействию, сформированного на основе выбранного

контейнера, от максимально возможного значения этого показателя по всему множеству *K*.

МЕТОДЫ, РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Цель работы может быть достигнута только при использовании общей формализации процесса стеганопреобразования, никак не связанной со спецификой конкретного стеганографического алгоритма, чему очевидно удовлетворяет (1). Соотношение (1) с учетом того, что для симметричной матрицы она полностью и однозначно определяется набором СЗ и СВ, полученных в результате нормального спектрального разложения [16], позволяет сделать следующий вывод: результат любого стеганопреобразования для контейнера с симметричной матрицей формально может быть представлен в виде совокупности возмущений СЗ и СВ, произошедших при погружении ДИ в контейнер, что используется в [16] при определении понятия ЗИ. Однако, расчет объема ЗИ в соответствии с [16,17] требует предварительной симметризации матрицы ЦИ. Принцип симметризации, предложенный в [16] и сохраненный в [17]:

$$F = \begin{pmatrix} f_{11} \cdots f_{1n} \\ \vdots \quad \vdots \\ f_{n1} \cdots f_{nn} \end{pmatrix} \rightarrow$$

$$A = \begin{pmatrix} f_{11} \cdots f_{n1} \\ \vdots \quad \vdots \\ f_{n1} \cdots f_{nn} \end{pmatrix}, B = \begin{pmatrix} f_{11} \cdots f_{1n} \\ \vdots \quad \vdots \\ f_{1n} \cdots f_{nn} \end{pmatrix}$$

приводит к тому, что в каждой из двух полученных симметричных матриц *A*, *B*, которые ставятся в соответствие квадратной матрице *F* произвольной структуры, вносится лишь половина (верхний/нижний треугольник) оригинальной *F*, что, кроме дополнительной вычислительной работы, приводит к тому, что получаемые путем нормального спектрального разложения СВ и СЗ определяют не оригинальную матрицу, а ее специфическую модификацию, являясь дополнительным источником погрешности метода выбора контейнера как в [16], так и в [17]. В связи с этим, отталкиваясь от (1) и учитывая, что результат любого стеганопреобразования может быть представлен также в виде совокупности возмущений сингулярных чисел (СНЧ) и сингулярных векторов (СНВ), полученных путем нормального сингулярного разложения матрицы контейнера, поскольку для матрицы с различными СНЧ такое разложение всегда существует и единственно [18] (в отличие от «классического» сингулярного разложения), очевидной является целесообразность замены набора формальных параметров, фигурировавших в [16,17] для определения и количественной оценки объема ЗИ, на набор СНЧ и СНВ соответствующей матрицы, в пользу чего так же говорит сравнимость свойств этого набора параметров с набором СЗ и СВ симметричной матрицы с точки зрения чувствительности к возмущающим воздействиям [19].

Построим для произвольной $n \times n$-матрицы *F* нормальное сингулярное разложение:

$$F = U \Sigma V^T, \qquad (2)$$

где *U, V* – ортогональные матрицы, столбцы которых $u_i, v_i, i = \overline{1,n}$, являются левыми и правыми СНВ соответственно, при этом левые СНВ дополнительно являются лексикографически положительными [18]; $\Sigma = diag(\sigma_1, ..., \sigma_n), \sigma_1 \geq ... \geq \sigma_n \geq 0$ – СНЧ *F*. СНЧ произвольной *F*, как и СЗ симметричной матрицы, являются хорошо обусловленными в силу соотношения [19]: $\max_i |\sigma_i(F) - \sigma_i(F+E)| \leq \|E\|_2$, где $\|\cdot\|_2$ – спектральная матричная норма, *E* – $n \times n$-матрица возмущающего воздействия, мерой же чувствительности к возмущающим воздействиям СНВ u_i до сих пор считалась отделенность

$$svdgap(i,F) = \min_{i \neq j} |\sigma_i - \sigma_j| \qquad (3)$$

соответствующего СНЧ σ_i в соответствии с формулой [20]:

$$sin 2\theta_i \leq 2\|E\|_2 / svdgap(i,F), \qquad (4)$$

где θ_i – угол поворота u_i в результате возмущающего воздействия *E*. Очевидно, что соотношение (4) дает оценку сверху для угла θ_i только тогда, когда его правая часть

меньше либо равна 1. В противном случае поведение вектора u_i после атаки непредсказуемо. Возникновение данной ситуации для конкретного СНВ зависит от величины $svdgap(i,F)$ (3). В связи с этим будем говорить, что СНЧ σ_i матрицы F имеет достаточную отделенность по отношению к возмущающему воздействию E, если

$$svdgap(i,F) \geq 2\|E\|_2. \qquad (5)$$

При формальном представлении результата внедрения ДИ в контейнер F в виде совокупности возмущений СНЧ и СНВ актуальным является вопрос, как эти полученные возмущения отреагируют на атаку против встроенного сообщения, формальным представлением которой является матрица E. Очевидно, что декодирование ДИ возможно провести безошибочно только в том случае, когда все возмущения СНЧ и СНВ, полученные ими в процесс стеганопреобразования, не изменились в результате атаки. СНВ, отвечающие СНЧ, для которых (5) не выполняются, на практике могут сильно «пострадать» в результате атаки E, изменив свое направление по сравнению с положением в матрице СС настолько сильно (вплоть до противоположного направления), что часть ДИ, результатом внедрения которой было возмущение этих СНВ, будет искажена вплоть до полного уничтожения. Тут нужно отметить, что все же этот процесс *неконтролируемого случайного* изменения направлений некоторых СНВ в результате атаки E не носит исключительно негативный характер, когда возмущение СНВ будет очень значительным, неадекватным возмущающему воздействию. Действительно, как вытекает из формулы (4), ее правая часть дает лишь верхнюю границу возможных значений для $sin2\theta_i$, что никак не запрещает $sin2\theta_i$ отвечать малому углу поворота u_i даже при малой отделенности соответствующего СНЧ (рис.1). Это частично объясняет наличие устойчивых к атакам против встроенного сообщения стеганометодов, которые позволяют достаточно эффективно декодировать внедренную ДИ в условиях (значительных) возмущающих воздействий, сохраняя при этом надежность восприятия формируемого СС. Однако, отсутствие математического инструмента априорной оценки реального возмущения СНВ, отвечающих СНЧ с недостаточной по отношению к E отделенностью и практическая непредсказуемость их поведения, что иллюстрирует рис.1, заставляет для достижения цели, поставленной в работе, остановиться лишь на тех сингулярных тройках (σ_i,u_i,v_i) матрицы ЦИ, которые отвечают СНЧ с достаточной отделенностью. Назовем эти тройки защищенными по отношению к E. Рассмотрим возможность и способ их использования для определения ЗИ.

В [16] для количественной оценки объема ЗИ рассматривались непосредственные углы поворота выбранных (защищенных от E) СВ, в качестве весового коэффициента - абсолютные отделенности соответствующих СЗ. Однако с учетом абсолютных отделенностей СЗ мы получаем не реальные углы поворота СВ, а лишь верхнюю границу для величины этого угла, аналогично (4): $sin\theta_i \leq 2\|E\|_2 / gap_{abs}(i,F)$, где θ_i - угол поворота СВ u_i в результате возмущающего воздействия E, $gap_{abs}(i,F)$ - абсолютная отделенность СЗ λ_i: $gap_{abs}(i,F) = \min_{i \neq j} \|\lambda_i| - |\lambda_j\|$, что говорит о нецелесообразности использования абсолютной отделенности СЗ в качестве весового коэффициента, более того, ее использование приводит к тому, что количественно объем ЗИ неоправданно увеличивается, давая приоритетные позиции контейнерам, которые на практике не являются таковыми. В силу этого, проводя аналогичные рассуждения для СНЧ, авторы данной работы отказались от идеи использования непосредственно при оценке объема ЗИ отделенностей СНЧ. Однако, учитывая, что, как отмечено выше, результат стеганопреобразования формально представляется в виде возмущений СНЧ и СНВ матрицы контейнера, очевидным является необходимость совокупного учета этих возмущений при определении понятия ЗИ, но не аддитивного, а в виде некоторого интегрального параметра, который бы не искусственным, а естественным путем учитывал взаимосвязь и взаимовлияние возмущений отдельных формальных параметров (СНЧ, СНВ), необходимо присутствующие при любом возмущающем воздействии в силу однозначности нормального сингулярного

разложения матрицы. Действительно, пусть матрица *F* получила возмущение *E*. Построим для $F+E$ нормальное сингулярное разложение (2):

$$F+E=(U+\Delta U)(\Sigma+\Delta\Sigma)(V+\Delta V)^T, \quad (6)$$

где $\Delta U,\Delta\Sigma,\Delta V$ - возмущения соответственно матриц U,Σ,V в результате воздействия *E*, причем:

$$\Delta U\neq 0,\Delta\Sigma\neq 0,\Delta V\neq 0. \quad (7)$$

Действительно, возмущающее воздействие $E\neq 0$ возмущает все/некоторые элементы f_{ij} исходной $n\times n$-матрицы *F*, меняя в общем случае энергию *N*(*F*) соответствующего сигнала. Учитывая, что *N*(*F*) может быть рассчитана в соответствии с формулой: $N(F)=\sum_{i,j=1}^{n} f_{ij}^2=\sum_{i=1}^{n}\sigma_i^2$, изменение f_{ij} приведет к изменению СНЧ *F*, следствием чего является: $\Delta\Sigma\neq 0$. Два других соотношения в (7) объясняются обязательным наличием в пределах матрицы любого ЦИ чувствительных к возмущающим воздействиям СНВ, реагирующих на любое воздействие, вплоть до округлений в ходе вычислений. Из (6) для невырожденной возмущенной матрицы $F+E$ непосредственно вытекает, что $\Delta\Sigma=(U+\Delta U)^T(F+E)(V+\Delta V)-\Sigma$,

$\Delta U=(F+E)(V+\Delta V)(\Sigma+\Delta\Sigma)^{-1}-U$,

$\Delta V=(F+E)^{-1}(U+\Delta U)(\Sigma+\Delta\Sigma)-V$. Такая взаимосвязь подтверждает целесообразность изложенного ниже.

В процессе стеганопреобразования и последующих атак против встроенного сообщения каждая из сингулярных троек (σ_i,u_i,v_i) матрицы контейнера может получить возмущение. Однако, как было отмечено выше, какой-либо «контроль» над искажением внедренной ДИ мы имеем лишь для защищенных троек. Обозначим *M* – множество индексов СНЧ с достаточной по отношению к *E* отделенностью.

Пусть для (σ_k,u_k,v_k) $k\in M$. Каждая такая тройка определяет матрицу $F_k=\sigma_k u_k v_k^T$, для которой $rank(F_k)=1$.

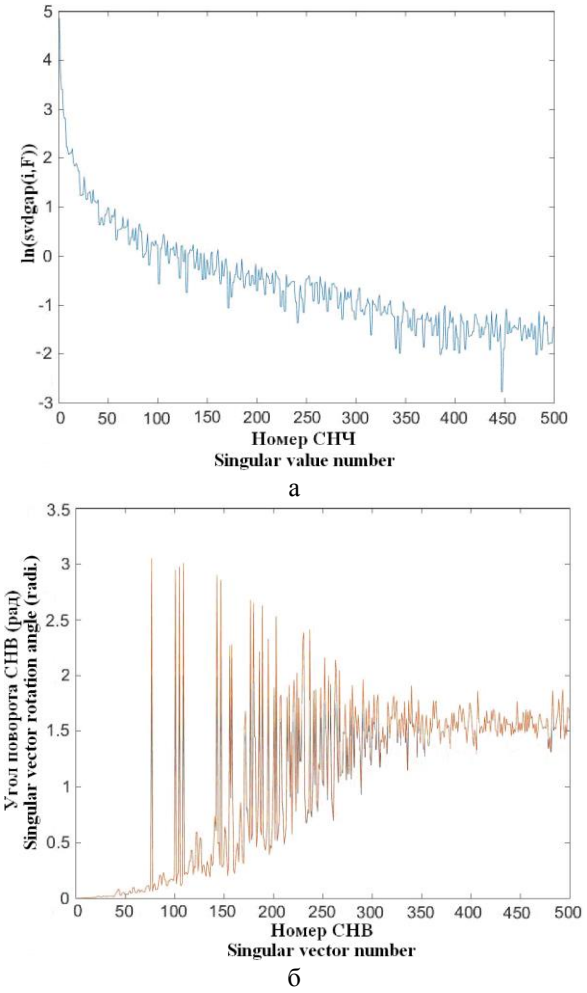

Рис.1. Соответствие возмущений СНВ матрицы ЦИ отделенностям СНЧ: а – график зависимости отделенности СНЧ от его номера; б – график зависимости возмущения СНВ от его номера в условиях *E*, сгенерированной случайным образом.[1]

Поскольку в ЦИ для СНЧ со значительной отделенностью, которая на практике и фигурирует как достаточная, наблюдается ее монотонное убывание с ростом номера СНЧ (рис.1(а)), то совокупность СНЧ с достаточной отделенностью представляет из себя, как правило, множество последовательных СНЧ, а *M* содержит последовательные натуральные числа от 1 до некоторого *m*. Сумма матриц, отвечающих защищенным тройкам, на практике удовлетворяет соотношению

$$\sum_{k\in M}F_k=\sum_{k=1}^{m}F_k=\sum_{k=1}^{m}\sigma_k u_k v_k^T, \quad (8)$$

т.е. является малоранговой аппроксимацией *F* ранга *m* [19]. Именно эта аппроксимация и

[1] Appendix 1

рассматривается как «поле, защищенное от *E*», для внедрения ДИ, причем в силу однозначности нормального сингулярного разложения *F*, это «поле» никак не ограничивает выбор реальной области ЦИ-контейнера, используемой для стеганопреобразования – пространственной, частотной, других областей преобразования.

Формальное определение и количественное выражение для ЗИ получим следующим образом. Пусть F и $\overline{F}$ – матрицы контейнера и СС, $\overline{F} = \overline{U}\overline{\Sigma}\overline{V}^T$ – нормальное сингулярное разложение для $\overline{F}$, в результате которого получены $\overline{\sigma}_i, \overline{u}_i, \overline{v}_i, i = \overline{1,n}$, - СНЧ, левые и правые СНВ СС соответственно. Защищенные от *E* возмущения сингулярных троек, полученные в результате стеганопреобразования, отвечают индексам из *M*.

Определение. Защищенная от возмущающего воздействия *E* ДИ определяется разностью аппроксимаций ранга *m* для матриц F контейнера и $\overline{F}$ СС:

$$S = \sum_{k=1}^{m} \overline{\sigma}_k \overline{u}_k \overline{v}_k^T - \sum_{k=1}^{m} \sigma_k u_k v_k^T, \qquad (9)$$

где *m* – максимальный индекс среди СНЧ F, имеющих достаточную по отношению к *E* отделенность.

Формула (9) определяет искомый интегральный параметр, который позволяет оценить происходящие при стеганопреобразовании возмущения интересующих СНЧ и СНВ в совокупности, учитывая их непосредственную взаимосвязь и взаимовлияние, кроме того, очевидным является здесь отсутствие какой-либо связи с конкретикой используемого для внедрения ДИ стеганометода, что отвечает цели работы.

В качестве количественной характеристики для ЗИ предлагается использовать спектральную матричную норму $\|S\|_2$. Заметим, что здесь не имеет принципиальной разницы, какую именно матричную норму рассматривать, учитывая соотношения, связывающие спектральную норму с нормой Фробениуса $\|S\|_F$, нормами $\|S\|_1$, $\|S\|_\infty$ [19]. Однако с учетом того, что именно спектральная норма фигурирует в оценках чувствительности как СЗ, СВ, так и СНЧ, СНВ, выбор сделан в ее пользу.

Очевидно, чем больше $\|S\|_2$, тем большее совокупное возмущение защищенных сингулярных троек, произошедшее в результате стеганопреобразования, будет относительно «защищено» от *E*, тем больший объем ДИ, формальным представлением внедрения которой явилось это возмущение, будет сохранен, а чувствительность СС будет меньше, что и учитывается ниже в предлагаемом методе выбора контейнера.

Учитывая резкое уменьшение отделенности при переходе от СНЧ с максимальными значениями к СНЧ с меньшими значениями (рис.1(а)), соотношение (5) и принятое определение для ЗИ, можно теоретически предположить, что получаемая оценка объема ЗИ $\|S\|_2$ может оказаться недостаточно эффективной в случае, если ЦИ будет иметь лишь одно СНЧ (очевидно - σ_1) с достаточной по отношению к *E* отделенностью. Действительно, поскольку для σ_1 в оригинальных ЦИ имеем: $\sigma_1 >> \sigma_i, i = \overline{2,n}$, типичная иллюстрация чего представлена на рис.2 для ЦИ размером 50×50 пикселей, а $svdgap(1,F) >> svdgap(i,F), \quad i = \overline{2,n}$ (рис.1(а)), это приводит к тому, что первые СНВ u_1, v_1 в соответствии с (4) практически не возмущаются под воздействием *E* [21] (угол поворота такого вектора от первоначального положения сравним с нулем), следствием чего является: $\|S\|_2 \approx 0$ для любого из таких ЦИ.

Однако такая ситуация (рис.3 (*NC* отвечает формуле (10)) может иметь место только в том случае, когда предполагается, что СС будет подвергаться значительному возмущающему воздействию *E*, вплоть до нарушения его надежности восприятия. Визуализация величины возмущающего воздействия, фиксирующая нарушение надежности восприятия СС, приведена на примере (рис.4). Однако даже в этом случае отклонение параметра *NC*, характеризующего чувствительность СС к воздействию *E*, для СС, построенного на основе контейнера с максимальным объемом ЗИ, от максимально возможного значения *NC* для всех рассмотренных изображений составило лишь 5.5%. (рис.3). Заметим, что на практике такое

ограничение не является критическим, поскольку при применении атак против встроенного сообщение, учитывая незаинтересованность нарушителя в том, чтобы его действия незамедлительно были обнаружены, атака будет происходить с сохранением надежности восприятия возмущенного СС, т.е. не может иметь значительную $\|E\|_2$.

С учетом всего вышеизложенного, основные шаги предлагаемого метода выбора контейнера из имеющегося множества для заданного секретного сообщения, дающего максимально возможную/близкую к максимально возможной устойчивость по отношению к возмущающему воздействию *E*, следующие.

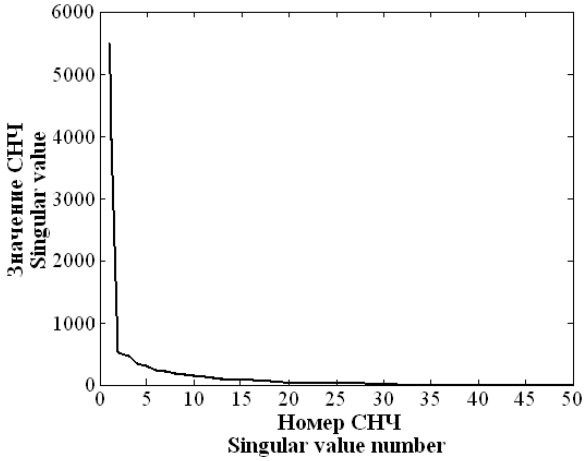

Рис.2. График зависимости величины СНЧ от его номера для оригинального ЦИ.[2]

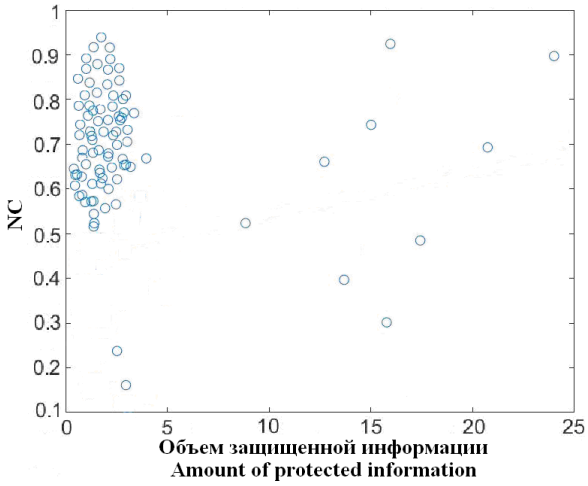

Рис.3. Зависимость коэффициента *NC* от объема ЗИ при использовании стеганометода [22] в условиях мультипликативного шума с *D*=0.004.[3]

а **б**

Рис.4. Иллюстрация возможного нарушения надежности восприятия ЦИ при рассмотренном возмущающем воздействии: а – оригинальное ЦИ; б – ЦИ, которое было подвержено наложению мультипликативного шума с *D*=0.004.[4]

Пусть K – множество ЦИ-контейнеров, из которых происходит выбор, $p_1, p_2, ..., p_l$ - бинарная последовательность – результат предварительного кодирования пересылаемого сообщения, M_S - рассматриваемый для внедрения ДИ стеганометод, E – формальное представление предполагаемой атаки против встроенного сообщения.

Шаг 1. Для каждого ЦИ $F \in K$:

1.1. Построить нормальное сингулярное разложение (2) для F ;
1.2. Определить отделенности (3) полученных СНЧ;
1.3. Определить множество M индексов СНЧ с достаточной отделенностью по отношению к возмущению E. Пусть m – максимальный индекс;
1.4. Построить для F аппроксимацию (8) ранга m.
1.5. Произвести внедрение ДИ $p_1, p_2, ..., p_l$ выбранным стеганометодом M_S в контейнер F. Результат – СС с матрицей $\overline{F}$;
1.6. Построить нормальное сингулярное разложение (2) для $\overline{F}$;
1.7. Построить для $\overline{F}$ аппроксимацию (8) ранга m.
1.8. Построить матрицу ЗИ S (9);
1.9. Определить $\|S\|_2$.

[2,3,4] Appendix 1

Шаг 2. Среди всех ЦИ множества K определить такое F_V, для которого матрица S_V (9) удовлетворяет соотношению:

$$\|S_V\|_2 = \max_{F \in K} \|S\|_2 .$$

ЦИ F_V - искомый контейнер.

Некоторые результаты вычислительного эксперимента по тестированию разработанного метода в условиях различных атак против встроенного сообщения, различных используемых для внедрения ДИ стеганометодов, а также результаты сравнительного анализа с методом [16] приведены на рис.5, где отражена зависимость между объемом ЗИ и чувствительностью СС к возмущающим воздействиям, количественным показателем которой взят коэффициент корреляции *NC* между погруженной ДИ $p_1, p_2, ..., p_t, p_i \in \{0,1\}, \ i = \overline{1,t}$, и декодированной $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t, \ \overline{p}_i \in \{0,1\}, \ i = \overline{1,t}$, ДИ [23]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t}, \qquad (10)$$

где $p_i' = 1, \overline{p}_i' = 1$, если $p_i = 1, \overline{p}_i = 1$, и $p_i' = -1, \overline{p}_i' = -1$, если $p_i = 0, \overline{p}_i = 0$.

На полученных графиках (рис.5(а,в,д)) для разработанного метода для любых стеганометодов, любых возмущающих воздействий можно заметить некоторый «разброс»: для ЦИ-контейнеров, имеющих близкие или даже равные значения объема ЗИ значения параметра *NC* отличаются между собой. Это связано со следующим. Очевидно, что не все СНВ из тех, которые отвечают СНЧ с достаточной отделенностью, являются нечувствительными к возмущающему воздействию. Более того, авторы, на основании имеющегося опыта, не согласны с тем, что отделенуость СНЧ является мерой чувствительности соответствующего СНВ к возмущающим воздействиям даже в случае (5) [20]. Очевидно, это можно утверждать лишь для тех СНВ, СНЧ которых имеют очень значительную отделенность, превращая правую часть (4) практически в ноль:

$$2\|E\|_2 / svdgap(i,F) \approx 0 . \qquad (11)$$

В таком случае соответствующий СНВ без вариантов будет нечувствителен к возмущающему воздействию E (в предположении, что угол θ_i поворота СНВ острый). Однако даже если выполняется (5), это не гарантирует адекватный ответ СНВ на возмущение: при малом возмущающем воздействии угол его поворота θ_i может быть далек от нуля, а величина угла будет определяться не только внедрением ДИ, но и возмущениями, не связанными напрямую со стеганопреобразованием, например, погрешностями округлений. Такие возмущения защищенных векторов дают иллюзию значительного объема ЗИ, что не отвечает действительности. Все вышесказанное объясняет и то, что при максимальном объеме ЗИ соответствующий контейнер может давать СС, устойчивость которого не является максимальной из возможных для множества *K* (хотя она очевидно будет близка к максимальной).

Для улучшения результатов работы метода, уменьшения разброса значений *NC* при близких значениях объема ЗИ очевидно следовало бы использовать при анализе сингулярные тройки (σ_i, u_i, v_i), в которых все входящие параметры являются гарантировано нечувствительными к возмущающим воздействиям. Для обеспечения нечувствительности выбранных для анализа сингулярных троек нужно было бы ужесточить условие достаточности отделенности СНЧ:

$$svdgap(i,F) >> 2\|E\|_2 , \qquad (12)$$

однако на практике использование (12) приведет к тому, что в процессе анализа будет систематически задействоваться лишь очень малое (вплоть до одного) количество СНЧ, что, как указывалось выше, является нежелательным.

Однако необходимо заметить, что хотя на практике разброс и имеет место, но при наибольшем объеме ЗИ метод всегда выбирает контейнер, который обеспечивает малую/близкую к наименьшей чувствительность СС к атакам против встроенного сообщения (рис.5, табл.1).

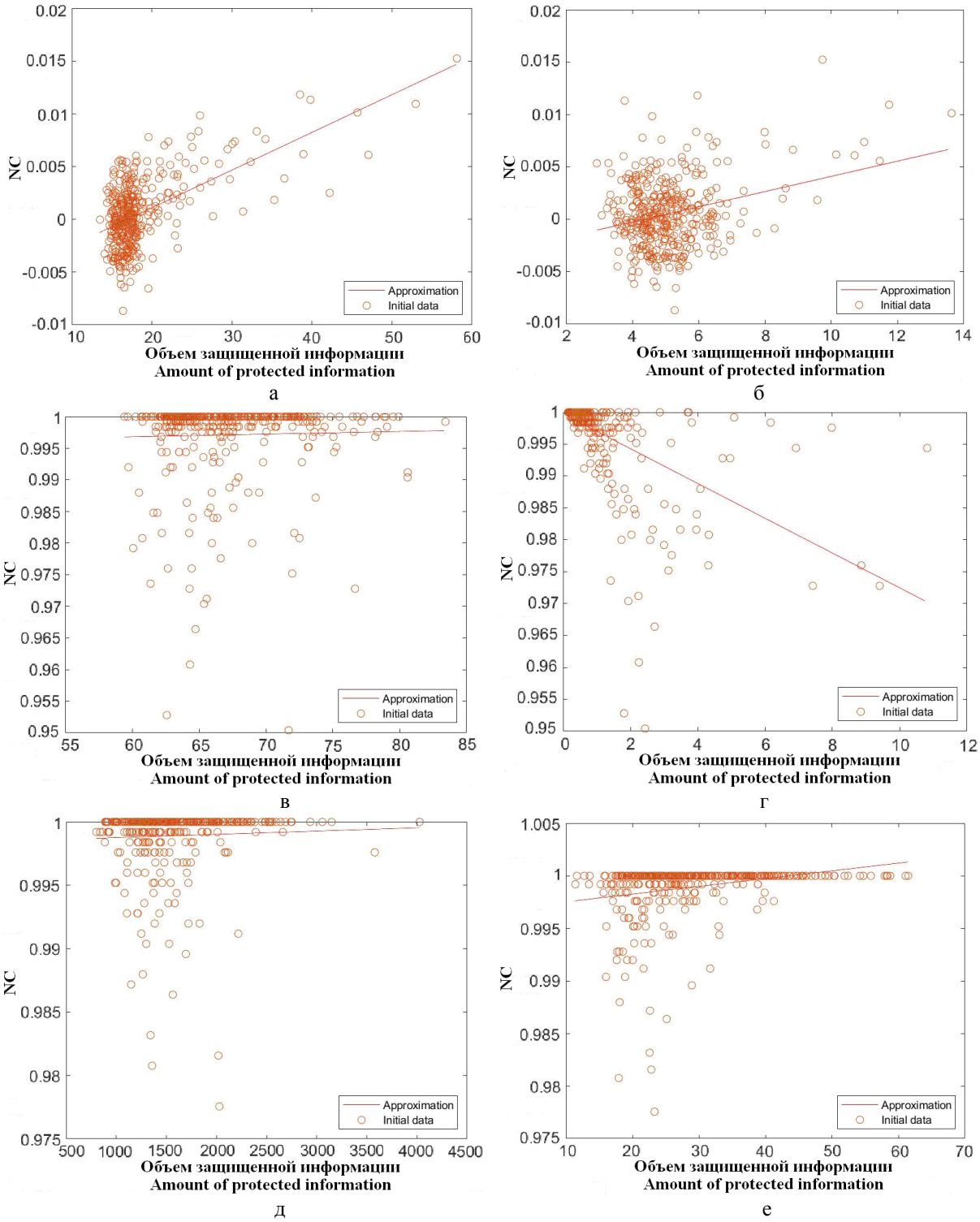

Рис. 5. Графики зависимости коэффициента *NC* от объема ЗИ для различных стеганоалгоритмов, использованных для встраивания ДИ, и различных атак против встроенного сообщения: а – разработанный метод (стеганометод LSB[24], атака сжатием с *QF*=75), б – метод [16] (стеганометод LSB, атака сжатием с *QF*=75), в – разработанный метод (стеганометод [25], атака сжатием с *QF*=75), г – метод [16] (стеганометод [25], атака сжатием с *QF*=75), д – разработанный метод (стеганометод [22], атака – наложение гауссовского шума с *D*=0.0005), е - метод [16] (стеганометод [22], атака – наложение гауссовского шума с *D*=0.0005).[5]

[5] Appendix 1

Таблица 1[6].

Результаты сравнительного анализа разработанного метода с аналогом[7]

Стеганометод (Stegomethod)	Возмущающее воздействие (Disturbing influence)	Значение *NC*, отвечающее максимальному объему ЗИ (*NC* value corresponding to the maximum amount of protected information)		Максимальное значение NC в условиях эксперимента (Maximum NC value under experimental conditions)
		Метод (Method) [16]	Предложенный метод (Proposed method)	
Метод LSB (пространственная область внедрения ДИ) (LSB-method (spatial domain of embedding) [24]	Сжатие с потерями с *QF*=75	0.0101	0.0152	0.0152
	Гауссовский шум с матожиданием 0 и *D*=0.0005	0.0211	0.0211	0.0211
	Мультипликативный шум с *D*=0.0005	0.4267	0.4267	0.4267
Метод с кодовым управлением внедрением ДИ (пространственная область внедрения ДИ) (Method with code-controlled information embedding (spatial domain of embedding)) [25]	Сжатие с потерями с *QF*=75	0.9944	0.9992	1
	Гауссовский шум с матожиданием 0 и *D*=0.0005	0.7496	0.8568 (на 14.3%)	0.8651
	Мультипликативный шум с *D*=0.0005	1	1	1
Метод модификации максимального СНЧ (внедрение ДИ - область сингулярного разложения) (Maximum singular value modification method (matrix singular value domain of embedding))[22]	Сжатие с потерями с *QF*=75	1	1	1
	Гауссовский шум с матожиданием 0 и *D*=0.0005	1	1	1
	Мультипликативный шум с *D*=0.0005	1	1	1
Метод Коха и Жао (частотная область внедрения ДИ) (Koch and Zhao method (frequency domain of embedding)) [26]	Сжатие с потерями с *QF*=75	1	1	1
	Гауссовский шум с матожиданием 0 и *D*=0.0005	0.9752	0.9608	1
	Мультипликативный шум с *D*=0.0005	1	1	1

Результаты вычислительного эксперимента демонстрируют высокую эффективность предложенного метода для каждого из рассмотренных стеганометодов внедрения ДИ (которые намеренно были выбраны так, чтобы проверить эффективность разработанного метода при использовании разных областей стеганопреобразования), что соответствует теоретическим ожиданиям, превосходство разработанного метода по сравнению с аналогом. В новом методе максимальное отличие устойчивости (коэф-

[6,7]Appendix 1

фициента *NC*) СС, полученного на основании контейнера с максимальным объемом ЗИ, от максимально возможного в условиях эксперименнта *NC* составило 3.9%, в то время, как для метода [16] это отличие максимально 11.6% (табл.1). По рис.5 очевидным является возможность нарушения в методе [16] общего тренда увеличения *NC* с увеличением объема ЗИ, для визуализации которого используется линейная аппроксимация полученных данных. Разработанный метод практически везде дает показатель *NC* для СС, построенного на основе выбранного контейнера с максимальным объемом ЗИ, не меньше, чем дает метод [16]. Исключение составляет лишь метод Koch and Zhao, где контейнер, выбранный новым методом, обеспечивает худший результат устойчивости, однако этот проигрыш незначительный (менее 1.5%), при этом отличие в новом методе от максимального по эксперименту *NC* составляет лишь 3.9%.

Предложенный в работе метод имеет очень важное в практическом смысле преимущество, по сравнению с аналогами. Исходя из введенного определения ЗИ, можно утверждать, что ЦИ-контейнеры, которые были выбраны для возмущающих воздействий определенной силы *E*, могут быть эффективно использованы в условиях, когда сила такого воздействия снижается: $\|S\|_2$ уменьшается (рис.6).

Стрелками на рис.6 отмечены ЦИ для экспериментов с меньшей силой возмущающего воздействия, которые были определены как обладающие наибольшим объемом ЗИ в эксперименте с большей силой возмущающего воздействия. Как видно, эти ЦИ либо совпадают (рис.6(а)), либо отличаются очень незначительно с точки зрения объема ЗИ (рис.6(б)). Это приводит к тому, что принципиально можно рассмотреть при работе предложенного метода возмущающие воздействия максимальной/значительной силы, которые не нарушают надежности восприятия ЦИ. Выбранные для них единожды контейнеры из заданного множества ЦИ могут использоваться во всех случаях более слабых атак против встроенного сообщения без предварительного поиска.

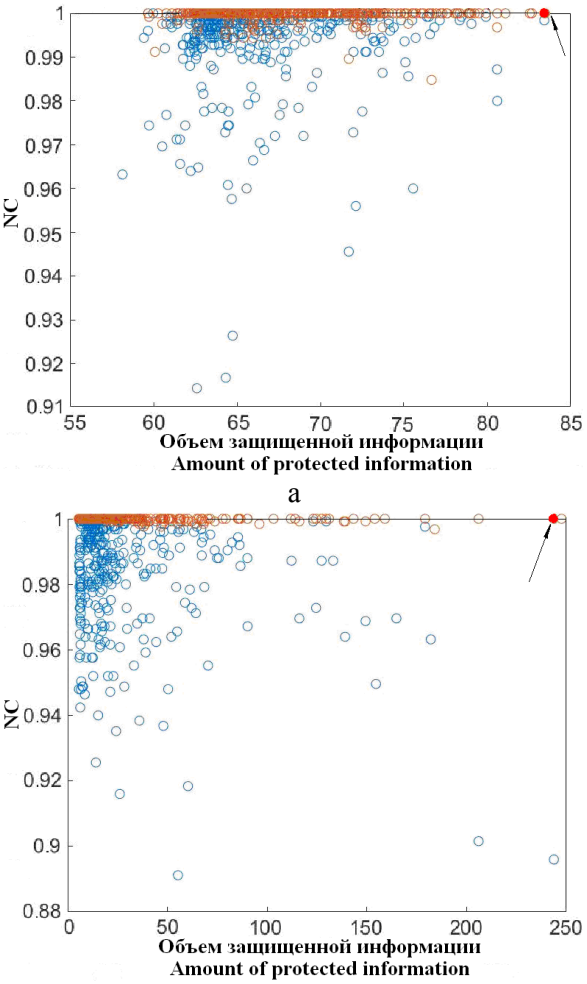

Рис.6. Графики зависимости *NC* от объема ЗИ в условиях атаки сжатием с *QF*=70 (синий цвет), *QF*=85 (красный цвет): а – стеганометод с кодовым управлением; б – метод Koch and Zhao.[8]

ВЫВОДЫ

В работе разработан ~~новый~~ метод выбора контейнера из определенного набора ЦИ для заданной ДИ, основанный на анализе возмущений малоранговых аппроксимаций матрицы контейнера в процессе стеганопреобразования, обеспечивающего для заданной ДИ максимально возможную/близкую к максимально возможной устойчивость формируемого СС к возмущающим воздействиям. Эффективность предложенного метода в целом превышает эффективность аналогов, остается высокой, независимо от используемого для внедрения ДИ стеганографического метода. Так максимальное отклонение коэффициента *NC*, являющегося количественным показателем чувствительности СС к возмущающим

[8]Appendix 1

воздействиям, от максимального значения для контейнеров из заданного множества составило 3.9%, в то время, как для лучшего из аналогов такое отклонение составляет 11.5%, что говорит о значительном повышении эффективности процесса выбора контейнера в результате использования нового метода (в условиях рассмотренного критерия). Практическим достоинством разработанного метода является обеспечиваемая эффективность использования его результатов, полученных в условиях возмущающего воздействия *E*, для атак меньшей силы.

Предложенный метод позволяет повысить в целом устойчивость стеганосистемы к атакам против встроенного сообщения при его использовании.

APPENDIX 1 (ПРИЛОЖЕНИЕ 1)

[1]**Fig. 1.** Correspondence of perturbations of singular vectors of the matrix of a digital image to the separation of singular numbers: a - graph of the dependence of the separation of a singular number from its number; b - graph of the dependence of the perturbation of the singular vector on its number under the conditions of the perturbing influence *E*, randomly generated

[2]**Fig. 2.** The dependence of the singular value on its number for the original digital image

[3]**Fig. 3.** The dependence of the NC coefficient on the amount of protected information when using the steganographic method [22] under conditions of multiplicative noise with D=0.004

[4]**Fig. 4.** An illustration of a possible violation of the reliability of the perception of a digital image under the considered disturbing effect: a - the original digital image; b – digital image under multiplicative noise overlay with D=0.004

[5]**Fig. 5.** The graphs of the dependence of the NC coefficient on the amount of protected information for various stegano algorithms used to embed additional information, and various attacks against an embedded message: a – the developed method (LSB [24] stegano method, compression attack with QF=75), b – method [16] (LSB stegano method, compression attack with QF=75), c – developed method (stegano method [25], compression attack with QF=75), d – method [16] (stegano method [25], compression attack with QF=75), e – developed method (stegano method [22], attack – Gaussian noise overlay with D=0.0005), f – method [16] (stegano method [22], attack – Gaussian noise overlay with D=0.0005)

[6,7]**Table 1.** The results of comparative analysis of the proposed method and analogue

[8]**Fig. 6.** The graphs of dependence of NC on the amount of protected information under compression attack with QF=70 (blue color), QF=85 (red color): a – code-controlled stegano method; b – Koch and Zhao method.

Литература (References)

[1] Rai A., Singh A.S., Kumar A.S. A Review of Information Security: Issues and Techniques. *International Journal for Research in Applied Science & Engineering Technology*, 2020, vol. 8, no. 5, pp. 953-960.

[2] Torten R., Reaiche C., Boyle S. The impact of security awarness on information technology professionals' behavior. *Computers & Security*, 2018, vol. 79, pp. 68-79.

[3] Alqahtani F.H. Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, 2017, vol. 124, pp. 691-697.

[4] Mandal P.C., Mukherjee I., Paul G., Chatterji B.N. Digital image steganography: A literature survey. *Information Sciences*, 2022, vol. 609, pp. 1451-1488.

[5] Taher M.M., Ahmad A.R., Hameed R.S., Mokri S.S. A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*, 2022, vol. 100, no. 5, pp. 1412-1427.

[6] Dhawan S., Gupta R. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, 2021, vol. 30, no. 2, pp. 63-87.

[7] Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. *Communications of the ACM*, 2014, vol. 57, no. 3, pp. 86-95.

[8] Bandyopadhyay S., Goyal V., Dutta S., Pramanik S., Sherazi H. *Unseen to Seen by Digital Steganography: Modern-Day Data-Hiding Techniques*. Available at: https://www.researchgate.net/publication/351828629_Unseen_to_Seen_by_Digital_Steganography_Modern-Day_Data-Hiding_Techniques (accessed 23.09.2022)

[9] Agranovskiy A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. *Steganografiya, tsifrovye vodyanye znaki i steganoanaliz* [Steganography, digital watermarks and steganalysis]. Moscow, 2009. 220 p. (In Russian).

[10] Abed S., Al-Roomi S.A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. *EURASIP Journal on Image and Video Processing*, 2019, 87. doi: 10.1186/s13640-019-0486-8

[11] Majeed M.A., Sulaiman R., Shukur Z., Hasan M.K. A Review on Text Steganography Techniques. *Mathematics*, 2021, vol. 9, no. 21, 2829.

[12] Qi Q. *A Study on Countermeasures against Steganography: an Active Warden Approach*. Available at: https://digitalcommons.unl.edu/ceendiss/25 (accessed 23.09.2022)

[13] Sun Y., Liu F. *Selecting Cover for Image Steganography by Correlation Coefficient*. Available at: https://dx.doi.org/10.1109/ETCS.2010.33 (accessed 23.09.2022)
[14] Mustafayeva E. Principles of Choosing Containers for Steganographic Systems. *International Journal of 3D Printing Technologies and Digital Industry*, 2020, vol.4, no. 3, pp. 264-229.
[15] Nikishova A.V., Omelchenko T.A., Makedonskij S.A. Steganographic embedding in containers-images. *Journal of Physics: Conference Series*, 2018, vol. 1015, no. 4. doi: 10.1088/1742-6596/1015/4/042041
[16] Kobozeva A.A., Narimanova E.V. Stegoimage disturb sensitivity estimate. *System Research and Information Technologies*, 2008, no. 3, pp. 52-65. (In Russian).
[17] Nadvotskiy A. A cover image selection method providing stego-object robustness to various image processing attacks. *Informatics and Mathematical Methods in Simulation*, 2021, vol. 11, no. 3, pp. 216-226. (in Ukrainian).
[18] Bergman C., Davidson J. *Unitary embedding for data hiding with the SVD*. Available at: https://dr.lib.iastate.edu/entities/publication/bb2b5041-1c92-4ff5-b7f4-ff73c3483eed (accessed 23.09.2022)
[19] Demmel J. *Applied Numerical Linear Algebra*. SIAM, 1997. 430 p.
[20] Demmel J. Accurate singular value decompositions of structured matrices. *SIAM Journal on Matrix Analysis and Applications*, 2000, vol. 21, no. 2, pp. 562-580.
[21] Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. *Transport and Telecommunication Journal*, 2016, vol. 17, no. 2, pp. 128–137.
[22] Melnik M.A. Steganoalgoritm, ustoichivyi k szhatiyu [A compression resistant stegano algorithm]. *Informatsiyna Bezpeka – Information Security*, 2012, no. 2, pp. 99-106. (In Russian).
[23] Lin W.-H, Wang Y.-R., Horng S.-J., Kao T.-W., Pan Y. A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*, 2009, vol. 36, no. 9, pp. 11509–11516.
[24] Singh A.K., Singh J., Singh H.V. Steganography in Images Using LSB Technique. International *Journal of Latest Trends in Engineering and Technology*, 2015, vol. 5, no. 1, pp. 426-430.
[25] Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*, 2021, vol. 11, no. 3, pp. 147-161.
[26] Fedorov A., Rubel A.S. *Detection of Hidden Data Embedded by the Koch and Zhao Method*. Available at: https://www.researchgate.net/publication/283463767 (accessed 23.09.2022)

Сведения об авторах.

Бобок Иван Игоревич – д.т.н., доц., Национальный университет «Одесская политехника». Область научных интересов: стеганография, стеганоанализ, социальная инженерия.
E-mail: onu_metal@ukr.net

Сокальский Сергей Николаевич – аспирант Национальный университет «Одесская политехника». Область научных интересов: стеганография.
E-mail: sokalskiyserhiy1@gmail.com

Кобозева Алла Анатольевна – д.т.н., проф., Национальный университет «Одесская политехника». Область научных интересов: стеганография, стеганоанализ.
Email: alla_kobozeva@ukr.net