УДК 004.056.5

И.И. Бобок,
А.А. Кобозева

СТЕГАНОАНАЛИЗ КАК ЧАСТНЫЙ СЛУЧАЙ АНАЛИЗА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Работа посвящена одному из основных направлений стеганографии – стеганоанализу. Основным результатом является получение качественных характерных особенностей сингулярных спектров матриц изображений, позволяющих отделить контейнер от стеганосообщения, сформированного на основе цифрового изображения, хранимого в формате JPEG. Приводятся результаты вычислительных экспериментов.

Ключевые слова: *стеганоанализ, информационная система, стеганосообщение, цифровое изображение, вычислительный эксперимент.*

Роботу присвячено одному з основних напрямів стеганографії – стеганоаналізу. Основним результатом є одержання якісних характерних особливостей сингулярних спектрів матриць зображень, що дозволяють відокремити контейнер від стеганоповідомлення, сформованого на основі цифрового зображення, збереженого у форматі JPEG. Наводяться результати обчислювальних експериментів.

Ключові слова: *стеганоаналіз, інформаційна система, стеганоповідомлення, цифрове зображення, обчислювальний експеримент.*

This paper is dedicated to one of the main areas of steganography – steganalysis. The main result is to obtain qualitative characteristics of the features of the singular spectra of image's matrix. Analysis of these features makes it possible to separate the container from stegano-message, formed on the basis of the digital images stored as JPEG. Results of computational experiments are given.

Keywords: *steganalysis, information system, stegano-message, digital image, computing experiment.*

Трагические события 11 сентября 2001 г., повлекшие за собой запрет шифрования на законодательном уровне во многих странах мира, привели к значительной активизации разработок в области стеганографии [1,2], где скрывается сам факт существования тайного сообщения. Общей чертой стеганографических методов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый безобидный, не привлекающий внимание объект – основное сообщение (ОС), или контейнер. В качестве ОС для определенности и упрощения изложения последующего материала рассматривается цифровое изображение (ЦИ). Процесс погружения ДИ в контейнер будем называть стеганопреобразованием, а результат этого погружения – стеганосообщением (СС). После встраивания информации СС открыто транспортируется адресату по каналу связи или хранится в таком виде.

Активизация научной деятельности в области стеганографии привела к росту возможностей использования получаемых новых разработок различными террористическими структурами [3]. В силу этого чрезвычайно *актуальным* в настоящий момент является решение вопросов, связанных с повышением эффективности стеганоанализа (СА) [1].

СА сегодня развивается в двух основных направлениях: разработка алгоритмов, позволяющих детектировать результаты работы конкретных стеганографических методов, и так называемых, универсальных, или слепых (blind), методов, позволяющих путем выявления или констатации отсутствия определенных характерных признаков в анализируемом информационном контенте делать вывод о произведенном внедрении секретной информации или отсутствии такового, не привязываясь к конкретике использованного стеганографического метода [3–6]. В свою очередь, универсальные методы СА делятся на две группы: методы, работающие в пространственной области, получающие необходимую информацию для возможности детектирования наличия ДИ, анализируя непосредственно пиксели изображения, и методы, работающие в частотной области.

При всем многообразии имеющихся стеганоаналитических методов [3–6] общего подхода к проблеме СА (в смысле детектирования произведенного внедрения секретной информации или вывода об отсутствии такого внедрения) до настоящего момента не существует.

В [7,8] был разработан новый общий математический подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), в частности, систем защиты информации, основанный на теории возмущений и матричном анализе, 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 соответствующих матриц. Для простоты изложения, не ограничивая при этом общности рассуждений, в качестве математической модели информационной системы будем рассматривать двумерную $m \times n$-матрицу 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:

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

где $\Delta F = f(F)$, т.е. 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 [7]. Одним из таких наборов, преимущества которого подробно обсуждаются в [7], является совокупность сингулярных чисел (СНЧ) и сингулярных векторов (СНВ), полученных при помощи нормального спектрального разложения матрицы, отвечающей рассматриваемой системе.

Любое преобразование информационной системы возмутит ее матрицу , следовательно определенным образом возмутит ее СНЧ и СНВ, а значит любое преобразование, в том числе и стеганопреобразование, представимо в виде совокупности возмущений СНЧ и (или) СНВ соответствующей матрицы. Это позволяет естественным образом свести задачу анализа процесса преобразования, в частности, стеганоанализа, и итогового состояния системы к анализу возмущений СНЧ и СНВ.

Таким образом, о результате преобразования информационной системы, 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 последующей разработки единого подхода к СА.

Глобальной целью авторов является разработка универсального метода СА, работающего как в пространственной, так и в частотной области, путем адаптации ОПАИС в область стеганографии.

В настоящее время хранение и передача ЦИ по каналам телекоммуникаций в связи со значительным увеличением объемов информации осуществляется в сжатом состоянии. Этот немаловажный факт не может не учитываться при разработке подхода к решению задачи СА. Одним из самых популярных в настоящее время форматов хранения ЦИ является формат JPEG, который может быть основан на вейвлет-преобразовании или на дискретном косинусном преобразовании (ДКП), которое и будет рассматриваться ниже для определенности.

В соответствии с ОБАИС, о состоянии и изменении состояния JPEG-изображения в связи с его стеганопреобразованием можно судить по характерным свойствам соответствующих СНЧ и СНВ матрицы ЦИ. В связи с этим, *целью* настоящей работы является выявление качественных характерных особенностей СНЧ матриц JPEG-изображений до и после стеганопреобразования, которые впоследствии позволят отделить контейнер от СС, сформированного на основе ЦИ, хранимого в формате JPEG.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1. Определить формальные параметры ЦИ, возмущения которых будут одинаковыми, независимыми от области анализа ЦИ (пространственной, частотной). Решение данной задачи обеспечит универсальность разрабатываемого впоследствии метода СА с точки зрения возможности его эффективной работы для проведения анализа как в пространственной, так и в частотной области (в зависимости от удобства и специфики рассматриваемой задачи).

2. Определить и обосновать качественные отличия СНЧ ЦИ, хранимого без потерь, от ЦИ, коэффициенты которого подвергались операции квантования.

3. Выявить зависимость возмущений СНЧ матриц ЦИ от объема погружаемой информации.

4. Определить и обосновать качественные отличия множества СНЧ СС, сформированного на базе JPEG-контейнера, от множества СНЧ контейнера.

Состояние как контейнера, так и СС определяется набором СНЧ и СНВ соответствующих матриц. Говоря о стеганопреобразовании, предполагаем, что результирующее возмущение матрицы контейнера является малым. Такое ограничение вызвано требованием обеспечения надежности восприятия СС (зрительно СС не должно отличаться от контейнера), выдвигаемым при работе любого стеганографического метода.

Анализ состояния контейнера (СС) целесообразности свести к анализу только СНЧ, являющихся в соответствии с соотношением [9]

$$\max_{1\le j\le n}\left|\sigma_j(F)-\sigma_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2, \qquad (2),$$

где $\sigma_j(F)$, $\sigma_j(F+\Delta F)$ – СНЧ матриц F, $F+\Delta F$ соответственно, $\left\|\Delta F\right\|_2$ – спектральная норма [9] матрицы возмущения, нечувствительными к возмущающим воздействиям (иначе – хорошо обусловленными), поскольку реакция СНВ на возмущающие воздействия различна, а в некоторых случаях – непредсказуема. В [10] показано, что для обеспечения надежности восприятия СС стеганопреобразование достаточно производить таким образом, чтобы возмущения претерпели СНВ, отвечающие СНЧ с малой отделенностью, где отделенность $\sigma_j(F)$ определяется в соответствии с формулой:

$$svdgap(i,F)=\min_{i\ne j}\left|\sigma_j-\sigma_i\right| \qquad (3).$$

Малую отделенность, как правило, имеют наименьшие и средние по величине СНЧ. В [11] показано и обосновано, что для СНВ, отвечающих СНЧ с малой отделенностью, их реакция на возмущающее воздействие (в том числе, малое) объективно непредсказуема. Таким образом, при анализе возмущений СНВ возможна ситуация, когда принципиально невозможно сделать вывод о характере воздействия, вызвавшего соответствующие возмущения. В силу этого анализ состояния контейнера (СС) далее будет ограничен только анализом возмущений СНЧ соответствующих матриц.

Покажем, что для ЦИ СНЧ (возмущения СНЧ) матрицы яркости (пространственная область) и матрицы коэффициентов ДКП (частотная область) одинаковы, т.е. множество СНЧ является тем набором формальных параметров ЦИ, который определяет решение задачи 1.

Поскольку ЦИ с матрицей предполагается сохраненным в формате JPEG, который производит в процессе сжатия предварительное стандартное разбиение матрицы изображения на блоки 8×8, произведем такое же разбиение для F. Пусть F_B – 8×8-матрица произвольного блока исходного изображения, для которой строится сингулярное разложение [9]

$$F_B=U\Sigma V^T \qquad (4),$$

где U, V– 8×8-матрицы, $\Sigma=diag(\sigma_1,...,\sigma_8)$, $\sigma_1\ge...\ge\sigma_8\ge0$. При этом U, V удовлетворяют соотношениям: $U^TU=I$, $V^TV=I$, где I – единичная 8×8-матрица, т.е. являются ортогональными. Столбцы $u_1,...,u_8$ матрицы U и $v_1,...,v_8$ матрицы V– соответственно левые и правые СНВ матрицы F_B, $\sigma_1,...,\sigma_8$ – СНЧ. Необходимо отметить, что в общем случае сингулярное разложение матрицы определяется неоднозначно за счет неоднозначности СНВ. Этого можно избежать за счет

построения нормального сингулярного разложения [7, 8]. Однако в силу того, что анализу в дальнейшем будут подвергаться только СНЧ (определяемые однозначно), отмеченная особенность обычного сингулярного разложения, которое используется везде ниже, оказывается незначащей.

Пусть F_{DCT} – соответствующая F_B матрица коэффициентов ДКП. Тогда:

$$F_{DCT} = PF_BP^t \quad (5),$$

где матрица P – ортогональная с элементами p_{ij}, определяемыми в соответствии с соотношением [12]:

$$p_{ij} = \begin{cases} \frac{1}{\sqrt{8}}, \ i = 1, \ 1 \le j \le 8, \\ \frac{1}{2}\cos\frac{\pi(2j-1)(i-1)}{16}, \ 2 \le i \le 8, \ 1 \le j \le 8 \end{cases}.$$

Учитывая (4), формула (5) приобретает вид:

$$F_{DCT} = PU\Sigma V^T P^T = (PU)\Sigma(PV)^T \quad (6).$$

При этом, с учетом ортогональности матриц P, U, V, имеем:

$$(PU)(PU)^T = PUU^TP^T = I, \ (PV)(PV)^T = PVV^TP^T = I,$$

т.е. матрицы PU, PV – ортогональны, Σ – диагональная, а потому (6) является сингулярным разложением матрицы F_{DCT}, для которой, очевидно, множество СНЧ совпадает с множеством СНЧ матрицы F_B.

Таким образом, любые возмущения СНЧ проявятся абсолютно одинаково для матрицы ЦИ, как в пространственной, так и в частотной области.

Общая схема сжатия (с потерями) для ЦИ состоит из трех основных шагов: отображение в частотную область, квантование полученных коэффициентов, энтропийное кодирование. Восстановление включает в себя шаги, обратные к перечисленным выше, в обратном порядке [13]. Далее, говоря о восстановлении ЦИ, будем рассматривать два возможных способа: частичное восстановление (ЧВ) после "возвращения" матричных коэффициентов из частотной области в пространственную не предполагает их округления, в отличие от полного восстановления (ПВ).

Квантование коэффициентов, полученных в частотной области, является необратимой процедурой и приводит к некоторым закономерным особенностям СНЧ блоков, полученных после предварительного стандартного разбиения матриц ЦИ.

Для ЦИ, сохраняемого без потерь, лишь малая часть общего числа блоков (ОЧБ) имеет нулевые СНЧ (в среднем – менее 3 % [14]). Данный факт не

случаен. Ранг любой матрицы определяется количеством ее ненулевых СНЧ [9]. Однако для произвольного ЦИ вероятность того, что строки (столбцы) очередного блока соответствующей матрицы окажутся линейно зависимыми, невелика. Чаще всего это происходит в случае коллинеарности (или просто совпадения) векторов, которая для реального ЦИ, сохраняемого без потерь, встречается редко, что и подтверждается вычислительным экспериментом.

Пускай для хранения ЦИ используется схема JPEG, но после квантования коэффициентов ДКП восстановление было частичным. Тогда у полученных матриц практически все блоки содержат нулевые СНЧ (в среднем таких блоков более 95 % от ОЧБ [14]). Действительно, после квантования и округления коэффициентов ДКП блоков многие из них, отвечающие высоким и средним частотам, обнулятся, оставаясь нулями после ЧВ, что в соответствии с [7] приведет к тому, что нулевыми окажутся наименьшие (а, возможно, и средние по величине) СНЧ матриц блоков.

Пускай исходное ЦИ, подвергшееся JPEG-сжатию, восстанавливается полностью. Это действие возмутит матрицу ЦИ, полученную после ЧВ, определенным образом изменит количество нулевых СНЧ в блоках. В тех блоках, где после ЧВ не было элементов, значительно меньших 0 или больших 255 (как показывает вычислительный эксперимент, таких блоков большинство), возмущение матрицы будет малым, а поскольку СНЧ в соответствии с (2) являются нечувствительными к возмущающим воздействиям, в данном случае – к округлениям, их возмущения также будут незначительными [7]. Нулевые СНЧ блоков матрицы частично восстановленного ЦИ хоть и станут нулями после ПВ, но их значения будут сравнимы с погрешностью округления и друг с другом, что не является характерным для блоков ЦИ, сохраняемого без потерь. Для иллюстрации описанной качественной картины рассмотрим блок одного из тестируемых изображений, сохраняемых первоначально без потерь (формат TIF). В исходном ЦИ сингулярный спектр этого блока имеет вид:

950.92, 164.12, 61.74, 17.10, 7.13, 4.10, 1.58, 0.70.

После сжатия и ЧВ СНЧ блока равны:

950.68, 175.75, 53.64, 12.94, 0.71, 0.00, 0.00. 0.00.

а после ПВ:

944.68, 172.54, 57.38, 13.53, 6.92, 0.84, 0.39, 0.02.

Хотя последние 3 СНЧ стали ненулевыми после ПВ, их значения незначительно отличаются от нуля и друг от друга и явно отличаются от предыдущих. Кроме того, характер их поведения качественно отличается от характера СНЧ с теми же номерами для блока исходного TIF-изображения (рис.1): скорость их изменения, оцениваемая угловым коэффициентом линейной аппроксимации графика зависимости значения СНЧ от его номера (на рис.1 – штриховая линия) значительно меньше аналогичного параметра для TIF-блока. Такая особенность дает возможность различать блоки ЦИ, ПВ после сжатия, и ЦИ, сохраняемого в формате, не предусматривающем квантование коэффициентов.

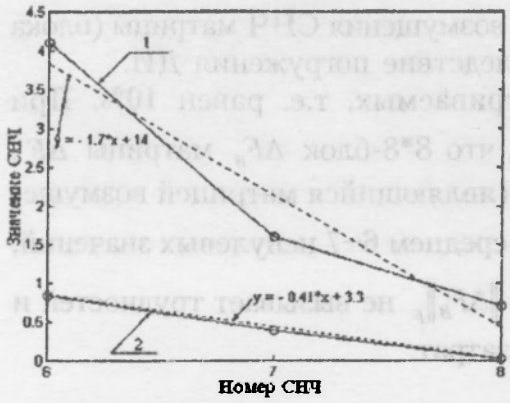

Рис.1. Графики зависимости значения СНЧ от его номера и их линейные аппроксимации: 1 - для блока TIF-изображения, 2 - для блока ПВ ЦИ

Наиболее ярко отличие в поведении СНЧ исходного (TIF) и ПВ блока просматривается на графиках скорости изменения отделенности СНЧ, определяемой согласно (3), при переходе от предыдущего СНЧ к последующему (рис. 2). Для k-го СНЧ значение скорости изменения отделенности определялось при помощи численного дифференцирования при переходе от $(k-1)$-го k -му. Для более яркой иллюстрации отличительных характерных черт скорости изменения на графиках отражены лишь последние (наименьшие) СНЧ. Как видно, скорость изменения отделенности СНЧ для исходного блока практически везде сохраняет свойство монотонного убывания, причем для наименьших СНЧ скорость отлична от нуля. Для последних по порядку СНЧ ПВ блока функция скорости изменения отделенности явно меняет характер монотонности, вырождаясь практически в ноль для наименьших СНЧ.

Сопоставление свойств СНЧ блоков изображений, сохраняемых без потерь и в сжатом состоянии, дает возможность предвидеть характер изменений свойств СНЧ JPEG-контейнера в ходе стеганопреобразования. Исходя из вышесказанного, ожидаемым результатом стеганопреобразования является уменьшение количества нулевых СНЧ, причем это уменьшение будет тем больше, чем большим будет объем погружаемой в ОС ДИ.

В соответствии с (1), произвольное стеганопреобразование можно представить в виде аддитивного погружения некоторой информации в пространственной области, при этом F рассматривается как матрица контейнера, а $\overline{F}$ – матрица СС. ДИ представляется в виде сформированной случайным образом бинарной последовательности.

Одним из наиболее широко используемых на сегодняшний день стеганографических методов является метод модификации наименьшего значащего бита (LSB) [1]. Рассмотрим подробно его работу, полагая, что стегопуть [1] формируется случайным образом.

Результат работы LSB-метода представляется как возмущение матрицы контейнера, при этом матрица возмущения ΔF имеет элементы, значения которых принадлежат множеству $\{-1,0,1\}$. При погружении ДИ в дальнейшем будем учитывать лишь те ее биты, которые вызывают возмущение соответствующих пикселей. Так, будем говорить, что объем погруженной информации (ОПИ) составляет, например, 20 %, если при погружении этой ДИ пятая часть общего числа пикселей ОС претерпела возмущения. При работе LSB-метода, как правило [3–6], погружается ДИ, для которой ОПИ принимает значения от 10 % до 100%.

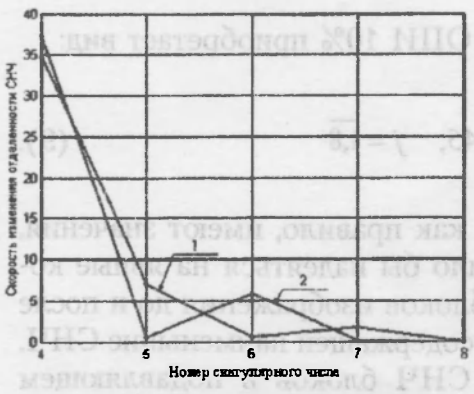

Рис.2. Графики зависимости скорости изменения отделенности СНЧ от его номера: 1 – для блока исходного ЦИ; 2 – для блока ПВ ЦИ

Проанализируем и оценим количественно возмущения СНЧ матрицы (блока матрицы) JPEG-контейнера, возникающие вследствие погружения ДИ.

Пусть ОПИ минимальный из рассматриваемых, т.е. равен 10%. При сделанных выше предположениях это значит, что 8*8-блок ΔF_B матрицы ΔF, полученный после ее стандартного разбиения (являющийся матрицей возмущения для блока F_B матрицы ОС), будет иметь в среднем 6–7 ненулевых значений, равных 1 или – 1. Оценка нормы Фробениуса $\|\Delta F_B\|_F$ не вызывает трудностей и не требует дополнительных вычислительных затрат:

$$\|\Delta F_B\|_F \approx \sqrt{6} \approx 2.45 .$$

Однако оценка (2) возмущения СНЧ блока контейнера предполагает знания спектральной матричной нормы $\|\Delta F_B\|_2$. Покажем, что для любой $n \times n$-матрицы A имеет место соотношение:

$$\|A\|_2 \le \|A\|_F \qquad (7).$$

Действительно, векторная 2-норма ($\|\bullet\|_2$) и матричная норма Фробениуса связаны соотношением [9]:

$$\|Az\|_2 \le \|A\|_F \|z\|_2 \qquad (8),$$

где z – вектор длины n. Поскольку спектральная матричная норма индуцирована векторной 2-нормой [9], то с учетом (8):

$$\|A\|_{l2} = \max_{z \ne 0} \frac{\|Az\|_2}{\|z\|_2} \le \max_{z \ne 0} \frac{\|A\|_F \|z\|_2}{\|z\|_2} = \|A\|_F .$$

что доказывает (7).

С учетом (7) оценка (2) для блока F_B при ОПИ 10% приобретает вид:

$$\left|\sigma_j(F_B) - \sigma_j(F_B + \Delta F_B)\right| \le 2.45, \quad j = \overline{1,8} \qquad (9).$$

В силу того, что наименьшие СНЧ блоков, как правило, имеют значения, сравнимые с единицей, исходя из (9), можно было бы надеяться на явные количественные отличия в сингулярных спектрах блоков изображения до и после стеганопреобразования, по крайней мере, в части, содержащей наименьшие СНЧ. Однако на практике абсолютная погрешность СНЧ блоков в подавляющем большинстве случаев оказывается гораздо меньше указанной верхней границы

в (9), а потому ее использование для распознавания ОС и СС вызывает затруднение.

Хотя абсолютные погрешности СНЧ, возникающие за счет стеганопреобразования, для всех СНЧ ограничены сверху одинаково, для относительных погрешностей картина будет принципиально другой. Для иллюстрации этого в таблице 1 приведена часть результатов вычислительного эксперимента для пяти выбранных случайно тестовых ЦИ.

Таблица 1

Относительные погрешности СНЧ блоков ЦИ-контейнера, возникающие при стеганопреобразовании LSB-методом при ОШИ 10 %

№ ЦИ	Относительные погрешности СНЧ блоков (%)
1	0.0605 1.9531 1.4846 17.2256 5.2750 19.2736 137.1945 12.4750
2	0.0274 0.0831 0.1253 0.7436 2.4138 8.3467 11.3690 26.1539
3	0.0203 0.1300 1.3231 1.9764 9.2759 9.4315 35.1892 33.4940
4	0.2488 2.2687 20.5072 41.0460 26.3921 6.4525 10.8207 0.4913
5	0.1943 1.8031 1.4811 3.3200 49.6878 38.8003 76.4647 91.1596

Очевидно, что в результате стеганопреобразования наиболее значительно относительно других "страдают" наименьшие СНЧ. Причем если в общем случае при возмущении СНЧ возможны варианты, представленные как на рис. 3 (а), так и на рис. 3 (б), то на практике для подавляющего большинства блоков ЦИ абсолютное значение углового коэффициента прямой, интерполирующей седьмое и восьмое СНЧ (т.е. скорость изменения СНЧ) после стеганопреобразования возрастает (часть результатов для иллюстрации сказанного приведена в таблице 2). Это явление является ожидаемым и объясняется следующим образом. После ПВ ЦИ, как уже было отмечено выше, наименьшие СНЧ, бывшие нулевыми после ЧВ, сравнимы друг с другом (и незначительно отличаются от 0), т.е. скорость изменения по абсолютной величине близка к нулю. Поэтому даже малое возмущающее воздействие в таких блоках приведет к увеличению отделенности наименьших СНЧ и, как следствие, к возрастанию скорости изменения. Качественная картина, изображенная на рис. 3 (б), практически всегда отвечает блокам, которые уже после ЧВ не имели (или имели малое количество) нулевых СНЧ (такие блоки на изображении отвечают областям, содержащим контура). Отсюда вытекает вывод, что для получения количественных оценок качественных отличий возмущений СНЧ блоков контейнера от блоков СС необходимо будет различать блоки, соответствующие условно "фоновым" подобластям ЦИ (блоки I типа), и блоки, содержащие контура (II типа). Такие подобласти можно выделять различными способами, однако в силу специфики решаемой задачи разделение блоков на указанные два типа можно проводить при помощи оценки значений наименьших СНЧ: если наименьшие СНЧ сравнимы с нулем и друг с другом (скорость изменения близка к 0) – тип; наименьшие СНЧ значительно отличаются друг от друга (скорость изменения больше 1) – тип.

Пример блока I типа:

СНЧ блока исходного ЦИ –

2017.7 4.1 2.4 2.0 1.2 0.8 **0.4 0.2**

(поведение последних трех из них говорит о том, что после ЧВ они были нулями). После стеганопреобразования с ОПИ 10% для этого блока в силу вышесказанного предполагаем увеличение скорости изменения последних двух СНЧ. Действительно, возмущенный сингулярный спектр имеем вид:

2017.3 4.6 2.7 2.2 1.0 0.7 **0.4 0.1**,

что говорит о возрастании скорости изменения наименьших СНЧ с 0.2 до 0.3.

Пример блока II типа:

СНЧ до стеганопреобразования –

489.7936 54.3842 22.4475 18.4699 6.7756 3.4225 **3.2970 0.2741**.

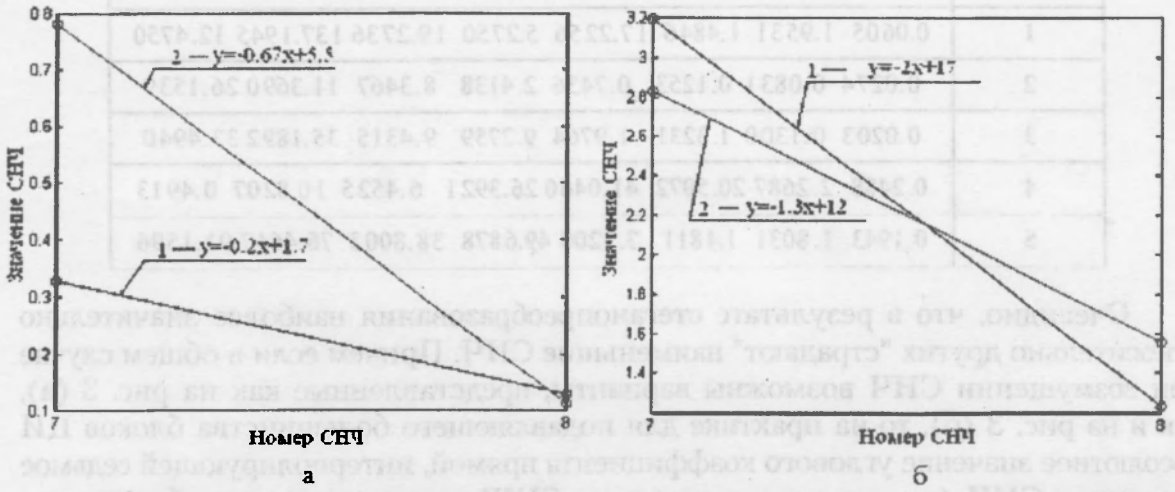

Рис.3. Изменение поведения наименьших СНЧ ЦИ в результате стеганопреобразования, возмущающего 10% пикселей (значение возмущения пикселя принадлежит множеству {–1,1}): а – ЦИ 1; б – ЦИ 2; 1 – прямая, отвечающая изображению-контейнеру; 2 – прямая, отвечающая стеганосообщению

Поскольку для последних СНЧ скорость изменения больше 1, предполагается уменьшение этой скорости после стеганопреобразования. Действительно, возмущенный сингулярный спектр имеет вид:

489.9882 55.0505 22.5530 18.3902 6.7993 3.8677 **2.6872 0.8622**.

Возмущения, которые претерпевают СНЧ при даже очень малом ОПИ, очевидно приведут к изменению качественной картины наличия нулевых СНЧ в блоках при стандартном разбиении матрицы ЦИ, о чем уже говорилось выше. Поскольку вырожденность блоков определяется линейной зависимостью столбцов (строк) соответствующих матриц, а погружение ДИ, изменяя значения элементов столбцов (строк), с большой вероятностью приведет к «разрушению» этой линейной зависимости (а значит к росту ранга матрицы блока СС), выдвигается *гипотеза*: количество вырожденных блоков ОС после стеганопреобразования должно резко уменьшиться, количество невырожденных блоков будет тем больше, чем больше ОПИ.

Таблица 2

Изменение скорости роста (убывания) наименьших СНЧ в блоках ЦИ-контейнера после стеганопреобразования с ОПИ 10%

№ ЦИ	Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после стеганопреобразования		№ ЦИ	Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после стеганопреобразования		№ ЦИ	Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после стеганопреобразования	
	уменьшается	возрастает		уменьшается	возрастает		уменьшается	возрастает
1	35.3	64.7	4	28.8	71.1	7	22.1	77.9
2	40.6	59.3	5	24.7	75.2	8	31.5	68.5
3	30.0	69.9	6	24.0	76.0	9	38.0	62.0
Среднее значение (тестировались более 230 ЦИ)								
Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после стеганопреобразования уменьшается				Кол-во блоков (%), для которых скорость изменения наименьших СНЧ после стеганопреобразования возрастает				
32				68				

Для проверки этой гипотезы в среде MATLAB был проведен вычислительный эксперимент, в котором тестировалось более 350 различных ЦИ, сохраняемых в формате JPEG. ДИ, как и ранее, представлялась в виде сформированной случайным образом бинарной последовательности. При этом при стеганопреобразовании минимально ОПИ составил 10%. В результате в 100% тестируемых ЦИ было получено строгое монотонное возрастание количества блоков, не содержащих нулевых СНЧ, с ростом объема погруженной информации (типичные картины для четырех из рассмотренных ЦИ представлены на рис.4), причем, когда ОПИ был больше 60%, то практически все блоки матрицы оказывались невырожденными (во всех тестируемых изображениях более 99 % общего числа блоков).

В ходе проведенного вычислительного эксперимента также были получены результаты, изложенные ниже.

1. В результате погружения ДИ (даже в случае, когда стеганопреобразование возмущает лишь 10 % пикселей контейнера) матрица стеганосообщения никогда не содержит блоков, которые бы имели 7,8 нулевых СНЧ. По мере увеличения объема погружаемой информации у матриц СС последовательно исчезают блоки с большим количеством нулевых СНЧ (в табл. 3 приведен типичный пример результата исследования одного из тестируемых ЦИ). Данный результат может быть использован в процессе СА: если у исследуемого ЦИ матрица содержит блоки с 7 или 8 нулевыми СНЧ, то изображение не подвергалось стеганопреобразованию, которое возмущало бы не менее 10 % от общего числа пикселей.

2. Для матриц СС при любом ОПИ число блоков с максимально возможным количеством нулевых СНЧ всегда меньше числа блоков, у которых нулевых СНЧ на единицу меньше максимально возможного количества. Это свойство часто не соблюдается для блоков матриц ЦИ-контейнеров, что сигнализирует об отсутствии погруженной ДИ и может быть использовано при СА.

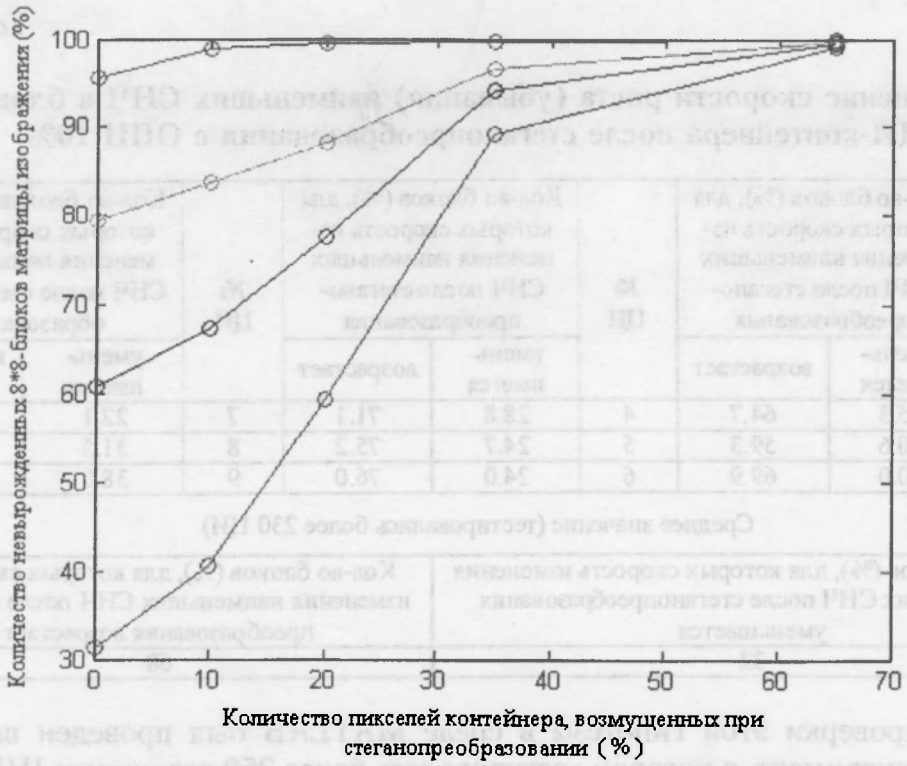

Рис.4. Зависимость количества невырожденных блоков матрицы ЦИ от ОПИ

Таблица 3

Зависимость количества блоков разного ранга матрицы изображения от ОПИ

		Количество блоков матрицы, содержащих m нулевых СНЧ по отношению к общему числу блоков, %								
		$m=0$	$m=1$	$m-2$	$m-3$	$m=4$	$m-5$	$m=6$	$m=7$	$m=8$
Исходное ЦИ		89.3555	4.2114	1.7090	1.4343	1.0559	0.9460	0.5737	0.5920	0.1212
СС, сформированное за счет возмущения k пикселей контейнера	$k=10\%$	93.4021	3.5522	1.8799	0.8179	0.2991	0.0488	**0**	**0**	**0**
	$k=20\%$	95.4529	3.4241	0.9094	0.2075	0.0061	**0**	**0**	**0**	**0**
	$k=35\%$	98.2361	1.6296	0.1343	**0**	**0**	**0**	**0**	**0**	**0**
	$k=65\%$	99.7803	0.2197	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Таким образом, в работе получены основные качественные отличия сингулярных спектров блоков СС с разными ОПИ от блоков JPEG-контейнеров. Определение количественных пороговых значений для найденных качественных отличий позволят разработать универсальный метод СА, что является целью дальнейшей работы авторов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Грибунин В.Г.* Цифровая стеганография / В.Г.Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.
2. *Ленков С.В.* Методы и средства защиты информации: В 2 тт. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008 – Т. 2 : Информационная безопасность. – 2008. – 344 с.
3. *G.Gul, F.Kurugollu.* SVD-Based Universal Spatial Domain Image Steganalysis / IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5, NO. 2. – PP. 349–353.
4. *G. Gul, A. E. Dirik,* and *I. Avcibas.* Steganalytic features for JPEG compression based perturbed quantization. – IEEE Signal Process.Lett., vol. 14, no. 3, pp. 205–208, Mar. 2007.
5. *S. Lyu and H. Farid.* Detecting hidden messages using higher-order statistics and support vector machines / Lecture Notes in Computer Science. New York: Springer-Verlag, 2002, vol. 2578, pp. 340–354.
6. *I. Avcibas, M. Kharrazi, N. Memon,* and *B. Sankur.* Image steganalysis with binary similarity measures / EURASIP J. Appl. Signal Process., vol. 17, pp. 2749–2757, 2005.
7. *Кобозева А.А.* Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К. : Изд. ГУИКТ, 2009. – 251 с.
8. *Кобозєва А.А.* Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.
9. *Деммель Дж.* Вычислительная линейная алгебра / Дж. Деммель; пер.с англ. Х.Д. Икрамова. – М. : Мир, 2001. – 430 с.
10. *Кобозєва А.А.* Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / А.А. Кобозєва // Информационные технологии и компьютерная инженерия. – 2008. – № 1 (11). – С. 164–171.
11. *Кобозева А.А.* Оценка чувствительности стеганосообщения к возмущающим воздействиям / А.А. Кобозева, Е.В. Нариманова // Системні дослідження та інформаційні технології. – 2008. – № 3. – С. 52–65.
12. *Кобозева А.А., Трифонова Е.А.* Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова. –Вестник НТУ "ХПИ". – 2007. – № 18. – С. 81–93.
13. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. под ред. П.А. Чочиа. – М. : Техносфера, 2005. – 1072 с.
14. *Кобозева А.А.* Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукр. нац. ун-ту ім. В.Даля. – 2008. – № 8 (126), ч. 1. – С. 62–72.

Отримано 20.06.2011