УДК 004.056.5

И. И. БОБОК, аспирант ОНПУ, г. Одесса;
А. А. КОБОЗЕВА, д-р техн. наук, проф. ОНПУ, г. Одесса

ОБЩИЙ СТЕГАНОАНАЛИТИЧЕСКИЙ ПОДХОД, ОСНОВАННЫЙ НА МАТРИЧНОМ АНАЛИЗЕ

Работа посвящена одному из основных направлений стеганографии – стеганоанализу. Разработаны основы общего стеганоаналитического подхода, основным инструментом которого явился матричный анализ. Получены качественные характеристики сингулярных спектров матриц изображений, хранимых в различных форматах, позволяющие отделить незаполненный контейнер от стеганосообщения, сформированного на основе цифрового изображения, хранимого в формате с потерями

Робота присвячена одному з основних напрямків стеганографії – стеганоаналізу. Розроблені основи загального стеганоаналітичного підходу, основним інструментом якого є матричний аналіз. Отримані якісні характеристики сингулярних спектрів матриць зображень, які зберігаються в різних форматах, що дозволяють відокремити незаповнений контейнер від стеганоповідомлення, сформованого на основі цифрового зображення, збереженого у форматі з втратами

This work is dedicated to one of the main areas of steganography – steganalysis. Designed the fundamentals of general steganalysis approach the main tool of which was the matrix analysis. Obtained qualitative characteristics of the singular spectra of images stored in various formats that allows separating the blank container from a message, formed on the basis of a digital image stored in lossy formats

Введение. Террористические акты, произошедшие в мире за последние годы, привели к запрету шифрования на законодательном уровне во многих странах, что дало значительный толчок для разработок в области стеганографии [1, 2], где скрывается сам факт существования тайного сообщения. Отрицательным последствием упомянутого процесса активизации научной деятельности явился рост возможностей использования получаемых новых разработок различными антигосударственными структурами [3]. В силу этого чрезвычайно *актуальным* в настоящий момент является решение вопросов, связанных с повышением эффективности стеганоанализа (СА) [1].

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 рассматривается цифровое изображение (ЦИ) в градациях серого. Процесс погружения ДИ в контейнер будем называть стеганопреобразованием (СП), а результат этого погружения – стеганосообщением (СС). После встраивания информации СС открыто транспортируется адресату по каналу связи или хранится в таком виде.

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 существовало.

Цель статьи и постановка исследований. В [7, 8] разработан общий математический подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), в частности, систем защиты информации, основанный на теории возмущений и матричном анализе, в соответствии с которым произвольная информационная система, в том числе, стеганографическая система (или отдельно рассматриваемые контейнер, СС), формализуется в виде двумерной матрицы (конечного множества двумерных матриц). О результате преобразования информационной системы, ее свойствах можно судить по характерным особенностям совокупности возмущений однозначно определяющих ее формальных параметров – сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей матрицы (матриц) [7, 8].

Глобальной целью авторов является разработка универсального метода СА – метода, не зависящего не только от области анализа ЦИ – пространственной или частотной, но и от конкретики стеганографического алгоритма, использованного при погружении ДИ, путем адаптации ОПАИС в область СА.

Глобальная цель приводит к следующей *глобальной задаче*: необходимо выявить такие характерные особенности СНЧ (СНВ) матриц незаполненного контейнера, которые качественно (и количественно) изменяются при любом даже малом возмущающем воздействии, в частности, при СП, что позволит отделить СС от ОС.

Очевидно, что искомые определяющие характеристики соответствующих матриц будут зависеть от формата, который используется для хранения ЦИ, главным образом, от того, происходят или нет потери информации при сохранении изображения в этом формате. Поскольку в настоящее время хранение и передача ЦИ по каналам телекоммуникаций осуществляется в сжатом состоянии, а одним из самых популярных форматов хранения является JPEG, то рассмотрим, в первую очередь, процесс СП на основе контейнера, хранящегося в формате JPEG (для определенности в качестве основы для JPEG выбрано дискретное косинусное преобразование (ДКП)).

Целью настоящей работы является создание теоретических основ метода СА, предусматривающего хранение ОС в формате с потерями, путем выявления качественных характерных особенностей СНЧ матриц JPEG-изображений до и после возмущающего воздействия – СП.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- обеспечить универсальность разрабатываемого метода СА с точки зрения его независимости от области анализа ЦИ – пространственной или частотной;

- определить и обосновать качественные отличия СНЧ ЦИ, хранимого без потерь, от ЦИ, частотные коэффициенты которого подвергались операции квантования;
- выявить зависимость возмущений СНЧ матриц ЦИ от объема погружаемой информации;
- определить и обосновать качественные отличия множества СНЧ СС, сформированного на базе JPEG-контейнера, от множества СНЧ ОС.

Независимость стеганоаналитического метода, основанного на анализе сингулярных чисел матрицы изображения, от анализируемой области изображения. Говоря о СП, предполагаем, что результирующее возмущение прямоугольной матрицы F 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), в частности, стеганоанализ, целесообразности свести к анализу только СНЧ, являющихся в соответствии с соотношением [9]

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

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, поскольку реакция СНВ на возмущения различна, а в некоторых случаях – непредсказуема [9].

Покажем, что сведение СА к анализу совокупности СНЧ соответствующей матрицы (если такое сведение в итоге окажется возможным) позволит обеспечить независимость разрабатываемого метода от области, пространственной или частотной, анализируемого изображения.

Поскольку контейнер 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]

$$F_B=U\Sigma V^T, \quad (2)$$

где U, V – ортогональные 8×8-матрицы, столбцы которых – левые и правые СНВ матрицы F_B соответственно, $\Sigma=diag(\sigma_1,...,\sigma_8)$, $\sigma_1\ge...\ge\sigma_8\ge 0$ – СНЧ.

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

$$F_{DCT}=PF_BP^T, \quad (3)$$

где матрица P – ортогональная с элементами p_{ij}, определяемыми в соответствии с соотношением [10]:

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

Учитывая (2), формула (3) приобретает вид:

$$F_{DCT}=PU\Sigma V^TP^T=(PU)\Sigma(PV)^T. \quad (4)$$

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

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

где I – единичная 8×8-матрица, т.е. матрицы PU, PV – ортогональны, Σ – диагональная, а потому (4) является сингулярным разложением матрицы F_{DCT}, для которой, очевидно множество СНЧ совпадает с множеством СНЧ матрицы F_B.

Таким образом, возмущения (или отсутствие возмущений) СНЧ, являющиеся показателем проведенного СП (или его отсутствия), проявятся одинаково для ЦИ как в пространственной, так и в частотной области, независимо от того, в пространственной или частотной области производилось погружение ДИ.

Качественные особенности сингулярных чисел матрицы изображения в различных форматах хранения. Общая схема сжатия (с потерями) для ЦИ включает в числе обязательных шагов процесс квантования коэффициентов, полученных в частотной области после предварительного стандартного разбиения матрицы изображения на блоки [11]. Эта процедура является необратимой и приводит к некоторым закономерным особенностям СНЧ блоков. Если для ЦИ, хранимым без потерь, лишь малая часть общего числа блоков (ОЧБ) имеет нулевые СНЧ (в среднем – менее 3% [12]), то в том случае, когда для хранения ЦИ используется схема JPEG, после квантования коэффициентов ДКП и частичного восстановления (ЧВ)(т.е. восстановления, не предусматривающего округление значений яркости пикселей после «возвращения» изображения в пространственную область) у полученных матриц практически все блоки содержат нулевые СНЧ (в среднем таких блоков более 95 % от ОЧБ [12]). Полное восстановление (ПВ) (т.е. приведение значений яркости пикселей в диапазон целых значений от 0 до 255) возмутит матрицу ЦИ, полученную после ЧВ, определенным образом изменит количество нулевых СНЧ в блоках. В тех блоках, где после ЧВ не было элементов, значи-

тельно меньших 0 или больших 255 (как показывает вычислительный эксперимент, таких блоков большинство), возмущение матрицы будет малым, а поскольку СНЧ в соответствии с (1) являются нечувствительными к возмущающим воздействиям, в данном случае – к округлениям, их возмущения также будут незначительными [7]. Нулевые СНЧ блоков матрицы частично восстановленного ЦИ в большинстве своем станут ненулями после ПВ, но их значения будут сравнимы с погрешностью округления и друг с другом, что не характерно для блоков ЦИ, хранимого без потерь. Это приведет к тому, что скорость изменения наименьших СНЧ JPEG-блоков (вырожденных после ЧВ) будет значительно меньше аналогичного параметра для соответствующих TIF(BMP)-блоков. Такая особенность дает возможность различать блоки ЦИ, ПВ после сжатия, и ЦИ, хранимого в формате, не предусматривающем квантование коэффициентов.

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

Количественные оценки возмущений сингулярных чисел матрица контейнера в процессе стеганопреобразования. В соответствии с ОПАИС, произвольное СП можно представить в виде аддитивного погружения некоторой информации в пространственной области:

$$\overline{F} = F + \Delta F \,, \qquad (5)$$

где F – матрица контейнера, $\overline{F}$ – матрица СС, ΔF – матрица возмущения вследствие СП.

Рассмотрим подробно работу стеганографическогометода модификации наименьшего значащего бита (LSB) [1]. Данный метод выбран авторами, главным образом, потому, что СП здесь, с учетом случайного характера формирования стеганопути [1] и различий в объемах ДИ, может приводить к очень незначительным и случайным возмущениям ΔF матрицы контейнера. Возможность выявления результатов *такого* возмущающего воздействия даст реальную перспективу для разрабатываемого СА метода эффективной работы по выявлению результатов работы других стеганографических методов. Кроме того, LSB является одним из самых распространенных и широко используемых стеганографических методов на сегодняшний день. Результат его работы представляется в соответствии с (5).

При погружении ДИ – случайно сформированной бинарной последовательности – в дальнейшем будем учитывать лишь те ее биты, которые вызывают возмущение соответствующих пикселей контейнера. Так будем говорить, что объем погруженной информации (ОПИ) составляет, например, 20%, если при погружении этой ДИ пятая часть общего числа пикселей ОС претерпела возмущения.

Проанализируем и оценим количественно возмущения СНЧ блоков матрицы JPEG-контейнера, возникающие вследствие погружения ДИ. Хотя абсолютные погрешности СНЧ, возникающие за счет СП, для всех СНЧ согласно (1) ограничены сверху одинаково, для относительных погрешностей картина будет принципиально другой. Для иллюстрации этого в табл.1 приведена часть результатов вычислительного эксперимента для пяти выбранных случайно тестовых ЦИ.

Таблица 1 – Относительные погрешности СНЧ блоков ЦИ-контейнера, возникающие при СП LSB-методом при ОПИ 10%

№ ЦИ	Относительные погрешности СНЧ блоков ЦИ-контейнера при СП LSB-методом для ОПИ 10% (%)							
	Номер СНЧ							
	1	2	3	4	5	6	7	8
1	0.06	1.95	1.48	17.23	5.28	19.27	137.20	12.48
2	0.03	0.08	0.13	0.74	2.41	8.35	11.37	26.15
3	0.02	0.13	1.32	1.98	9.28	9.43	35.19	33.49
4	0.25	2.27	20.51	41.05	26.39	6.45	10.82	0.49
5	0.19	1.80	1.48	3.32	49.69	38.80	76.46	91.16

Очевидно, что в результате СП наиболее значительно относительно других «страдают» наименьшие СНЧ. Причем для подавляющего большинства блоков ЦИ абсолютное значение углового коэффициента прямой, интерполирующей седьмое и восьмое СНЧ (т.е. скорость изменения), после СП возрастает (в среднем в 68% общего числа блоков ЦИ). 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 [9] наименьших СНЧ и, как следствие, к возрастанию скорости изменения. Назовем такие блоки блоками I-го типа. Уменьшение скорости изменения СНЧ после СП практически всегда отвечает блокам, которые уже после ЧВ не имели (или имели малое количество) нулевых СНЧ (такие блоки на изображении отвечают областям, содержащим контуры). 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-го типа), и блоки, содержащие контуры (II-го 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) – I-й тип; наименьшие СНЧ значительно отличаются друг от друга (скорость изменения больше 1) – II-й тип.

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 СП должно резко уменьшиться, количество невырожденных блоков будет тем больше, чем больше ОПИ.

Для проверки этой гипотезы в среде MATLAB был проведен вычислительный эксперимент, в котором тестировалось более 450 различных ЦИ, хранимых в формате JPEG. ДИ, как и ранее, представлялась в виде сформированной случайным образом бинарной последовательности. При этом при СП минимально ОПИ составил 10%. В результате в 100% тестируемых ЦИ было получено строгое монотонное возрастание количества блоков, не содержащих нулевых СНЧ, с ростом ОПИ (типичные картины для четырех из рассмотренных ЦИ представлены на рис.1), 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 следующие результаты:

- В результате погружения ДИ (даже в случае, когда ОПИ равен 10%) матрица СС никогда не содержит блоков, которые бы имели 7,8 нулевых СНЧ. По мере увеличения ОПИ у матриц СС последовательно исчезают блоки с большим количеством нулевых СНЧ (в табл.2 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 СП, которое возмущало бы не менее 10% общего числа пикселей.
- 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.

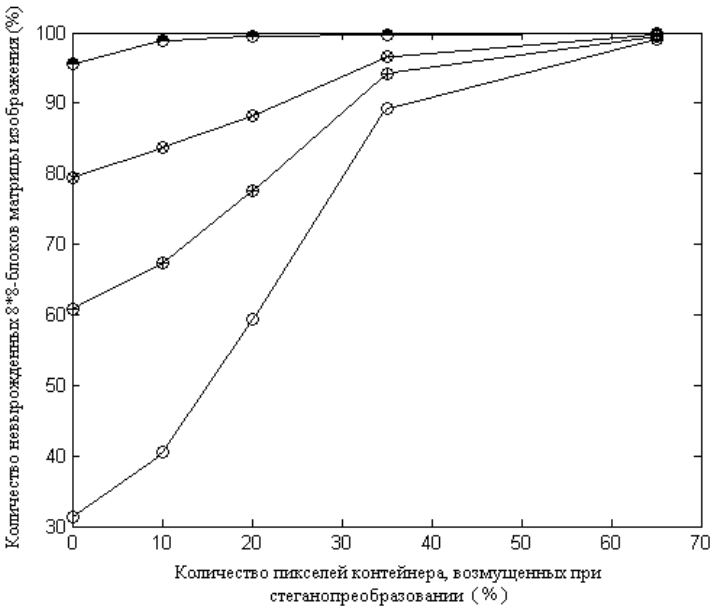

Рис.1 – Зависимость количества невырожденных блоков матрицы ЦИ от ОПИ

Таблица 2– Зависимость количества блоков разного ранга матрицы изображения от ОПИ

		Количество блоков матрицы, содержащих *m* нулевых СНЧ по отношению к ОЧБ, %								
		m=0	*m*=1	*m*=2	*m*=3	*m*=4	*m*=5	*m*=6	*m*=7	*m*=8
Исх. ЦИ		89.36	4.21	1.71	1.43	1.06	0.95	0.57	0.59	0.12
ОПИ, %	10	93.4	3.55	1.88	0.82	0.3	0.05	0	0	0
	20	95.45	3.42	0.91	0.21	0.01	0	0	0	0
	35	98.24	1.63	0.13	0	0	0	0	0	0
	65	99.78	0.22	0	0	0	0	0	0	0

Выводы. Таким образом, в работе путем адаптации ОПАИС в область СА

- разработаны основы общего стеганоаналитического подхода, основанного на сведении процесса СА к анализу СНЧ матриц тестируемых ЦИ;
- получены качественные характеристики сингулярных спектров матриц изображений, хранимых в различных форматах;
- 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 литературы: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 т. / *С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.* – К. : Арий, 2008. **3.** *Gul G.* SVD-Based Universal Spatial Domain Image Steganalysis / *G. Gul, F. Kurugollu* // IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5. – №. 2. – P. 349–353. **4.** *Gul G.* Steganalytic features for JPEG compression based perturbed quantization / *G. Gul, A. E. Dirik, I. Avcibas* // IEEE Signal Process.Lett. – Vol. 14. – №. 3. – P. 205–208. **5.** *Lyu S.* Detecting hidden messages using higher-order statistics and support vector machines / *S. Lyu, H. Farid* // Lecture Notes in Computer Science. New York : Springer-Verlag, 2002. – Vol. 2578. – P. 340–354. **6.** *Avcibas I.* Image steganalysis with binary similarity measures / *I. Avcibas, M. Kharrazi, N. Memon [et al.]* // EURASIP J. Appl. SignalProcess. – 200. – Vol. 17. – P. 2749–2757. **7.** *Кобозева А. А.* Анализ информационной безопасности / *А. А. Кобозева, В. А. Хорошко.* – К. : ГУИКТ, 2009. – 251 с. **8.** *Кобозєва А. А.* Аналіз захищеності інформаційних систем / *А. А.Кобозєва, І. О. Мачалін, В. О. Хорошко.* – К. : ДУІКТ, 2010. – 316 с. **9.** *Деммель Дж.* Вычислительная линейная алгебра / *Дж. Деммель*; пер. с англ. *Х. Д. Икрамова.*– М. : Мир, 2001. – 430 с. **10**. *Кобозева А. 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. **11**. *Гонсалес Р.* Цифровая обработка изображений / *Р. Гонсалес, Р. Вудс*; пер. с англ. под ред. *П. А. Чочиа.* – М. : Техносфера, 2005. – 1072 с. **12**. *Кобозева А. А.* Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / *А. А. Кобозева, О. В. Рыбальский, Е. А. Трифонова* // Вісник Східноукраїнського нац.ун-ту ім. В. Даля. – 2008. – № 8(126), ч.1. – С.62–72.

Надійшла до редколегії 07.06.2011