ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

УДК 004.056.5: 517.983.28

А.А. Кобозева, д-р. тех. наук, проф., Одес. нац. политехн. ун-т

ОСНОВЫ ОБЩЕГО ПОДХОДА К РАЗРАБОТКЕ УНИВЕРСАЛЬНЫХ СТЕГАНОАНАЛИТИЧЕСКИХ МЕТОДОВ ДЛЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

Введение. Активизация научной деятельности в области стеганографии, наблюдаемая сегодня, публикации новых результатов в открытой печати привели к росту возможностей использования получаемых разработок различными антигосударственными, террористическими структурами. В силу этого чрезвычайно важным в настоящий момент является решение вопросов, связанных с повышением эффективности стеганоанализа за счет уменьшения ошибок первого рода при выявлении наличия вложения дополнительной информации (ДИ) в различные информационные контенты, в частности, цифровые изображения (ЦИ), которые очень часто используются сегодня как контейнера при организации скрытого (стеганографического) канала связи [1].

Развитие стеганоанализа происходит в двух основных направлениях [2, 3]:

— разработка универсальных стеганоаналитических методов (САМ), способных выявлять вложение ДИ независимо от конкретики использованного для ее погружения стеганографического алгоритма [4-6];

— разработка САМ, ориентированных на выявление вложений, проведенных при помощи конкретных стеганоалгоритмов [1, 2].

Анализ последних исследований и публикаций. Существующие в настоящий момент САМ, которые позиционируются как универсальные, в той или иной степени остаются ориентированными хоть и на представительный, состоящий из наиболее часто используемых, но все равно ограниченный набор стеганоалгоритмов, учитывая особенности их работы для организации стеганоанализа [2, 3, 7]. Это говорит о том, что при появлении новых стеганоалгоритмов такие САМ принципиально не могут гарантировать их детектирование. Кроме того, эффективность работы многих существующих САМ критическим образом зависит от формата ЦИ, которое было использовано в качестве контейнера, а также формата, в который сохраняется изображение после внедрения в него дополнительной (конфиденциальной) информации. Важной не решенной до конца задачей стеганоанализа остается на сегодняшний день выявление вложений ДИ с малой скрытой пропускной способностью (СПС) [2, 8].

Все это говорит о несостоятельности существующих подходов, используемых при разработке универсальных САМ, о необходимости построения принципиально нового подхода к стеганоанализу с привлечением “нетрадиционных” в этой области математических инструментов и теорий.

Стеганопреобразование ЦИ независимо от конкретики используемого для этого стеганографического алгоритма, является возмущением оригинального изображения-контейнера, приводит к нарушению его целостности. Часто при обсуждении в научных публикациях, на конференциях, семинарах рассматриваемых в настоящей работе задач возникает вопрос о том, каким образом можно отличить результат погружения ДИ от результата некоторого возмущающего воздействия, отличного от стеганопреобразования? В общем случае принципиальных отличий между ними не существует: внедрение ДИ в контейнер может осуществляться при помощи самых различных его возмущений. А это значит, что нарушение целостности ЦИ является необходимым условием стеганопреобразования, а его выявление может рассматриваться как основа стеганоанализа.

DOI 10.15276/opu.2.44.2014.25

На сегодняшний день при решении задач, связанных с выявлением нарушения целостности различных информационных контентов, хорошо зарекомендовал себя общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), основанный на теории возмущений и матричном анализе [9, 10], где изменение состояния любой информационной системы, представляемой в виде конечного множества двумерных матриц, формально описывается в виде совокупности возмущений полного набора параметров, однозначно определяющих систему [9]. В качестве такого набора может использоваться множество сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей матрицы (матриц), удовлетворяющих определенным требованиям [9].

С учетом возможностей, предоставляемых ОПАИС при анализе информационных систем, основополагающая идея нового подхода к разработке универсальных САМ для ЦИ заключается в следующем. Все ЦИ могут храниться в форматах двух видов: с потерями и без потерь. Хотя таких форматов существует множество, но основная идея здесь одна: потери происходят за счет уменьшения вклада высокочастотной (возможно, и среднечастотной) составляющей сигнала. Оригинальные ЦИ сохраняются в каждый из существующих форматов (количество которых конечно) по определенному алгоритму, а, значит, их формальное представление в каждом из существующих форматов подчиняется определенным законам, приводит к определенным характерным особенностям формальных параметров (СНЧ и СНВ соответствующих матриц), определяющих ЦИ (в каждом формате). Выявление/нарушение этих особенностей даст возможность отделять оригинальные ЦИ от ЦИ, целостность которого нарушена, независимо от способа нарушения и формата хранения изображения.

Цель статьи и постановка заданий. В связи с вышесказанным *глобальной целью* автора является повышение эффективности стеганоанализа для ЦИ путем разработки новых универсальных САМ, эффективных, в том числе, при малой СПС, где показателем эффективности будет служить количество ошибок первого рода, допускаемых в результате стеганоанализа.

Целью настоящей работы является разработка основ нового подхода к организации универсального стеганоанализа как частного случая выявления нарушения целостности ЦИ на базе ОПАИС.

Для достижения цели необходимо решить следующие *задачи*:

1. Установить характерные особенности формальных параметров, определяющих ЦИ, которые позволят отделить оригинальное ЦИ от изображения, претерпевшего возмущающее воздействие, независимо от особенностей формата (с потерями, без потерь), в котором хранится изображение;

2. Установить размеры блока матрицы ЦИ, обеспечивающие наибольшую эффективность при организации анализа изображения с учетом выявленных характерных особенностей определяющих его формальных параметров;

3. Качественно и количественно оценить степень изменения выявленных характерных особенностей формальных параметров оригинального ЦИ при его возмущении.

Изложение основного материала. Не ограничивая общности рассуждений, в качестве формального представления ЦИ будем рассматривать одну матрицу F [9]. Разобьем F на квадратные непересекающиеся $l \times l$ -блоки B. Пусть

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

— нормальное сингулярное разложение B [10], определяемое однозначно, где U, V - ортогональные $l \times l$ -матрицы, столбцы которых $u_1, ..., u_l$ и $v_1, ..., v_l$ — соответственно левые и правые СНВ B, левые СНВ являются лексикографически положительными [11], $\Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_l)$, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ — СНЧ B.

Можно показать, что СНВ u_1 и v_1, отвечающие максимальному СНЧ σ_1 блока B матрицы ЦИ, полученные в ходе (1), являются нечувствительными к возмущающим воздействиям, а также sign-нечувствительными, близкими к n-оптимальному вектору n^0 пространства R^l [12],

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

где $n^0 = \left(\frac{1}{\sqrt{l}}, \frac{1}{\sqrt{l}}, \frac{1}{\sqrt{l}}, ..., \frac{1}{\sqrt{l}}\right)^T \in R^l$. Основой для этого является теорема Фробениуса [13], в соответствии с которой любая неразложимая неотрицательная матрица M всегда имеет собственное значение $\bar{\lambda}(M) > 0$, модуль которого не меньше модулей всех других собственных значений M, при этом соответствующий $\bar{\lambda}(M)$ собственный вектор $\bar{\varphi}(M)$ имеет все положительные координаты.

Для симметричной неотрицательной матрицы BB^T с учетом (1) имеет место соотношение:

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

которое в силу ортогональности матрицы U и лексикографической положительности ее столбцов, а также диагональности матрицы Σ^2 представляет собой нормальное спектральное разложение BB^T [9], определяемое однозначно, при этом собственные значения матрицы BB^T, как следует из соотношения (2), равны квадратам СНЧ B, в частности, $\bar{\lambda}(BB^T) = \sigma_1^2$, а левые СНВ B — ортонормированные лексикографически положительные собственные векторы BB^T.

Покажем, что BB^T является неразложимой [13], т.е. симметричными перестановками строк и столбцов ее нельзя привести к виду:

$$PBB^T P^T = \begin{pmatrix} A_1 & 0 \\ A_3 & A_2 \end{pmatrix}, \quad (3)$$

где A_1, A_2 — $l_1 \times l_1$ и $l_2 \times l_2$ — матрицы соответственно,

P — $l \times l$ – матрица перестановок (в каждой строке и в каждом столбце P один элемент равен единице, а все остальные — нули).

Учитывая, что BB^T — симметричная, представление (3) можно уточнить:

$$PBB^T P^T = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \quad (4)$$

где $A_1 = A_1^T$, $A_2 = A_2^T$.

Для того чтобы представление (4) принципиально было возможно, матрица BB^T должна содержать нулевые элементы, причем этих элементов не может быть меньше определенного количества, зависящего от размера B, чтобы они могли сформировать нулевые блоки в матрице $PBB^T P^T$ (4). Так для блока 4×4 для разложимости BB^T она должна содержать не меньше шести нулевых значений. Элементы матрицы BB^T получаются в результате скалярного произведения строк B. С учетом неотрицательности B нулевое значение в BB^T возможно лишь при наличии в B строк, для которых каждая пара элементов, принадлежащих одному столбцу, обязательно содержала хотя бы одно нулевое значение. Для обеспечения шести нулей в BB^T таких пар строк должно быть три. Требуемое расположение элементов в строках в блоке оригинального ЦИ маловероятно, причем вероятность, очевидно, будет уменьшаться с ростом размера блока, т.к. будет увеличиваться количество нужных для обеспечения вида (4) нулей в BB^T (например, для 8×8 – блока это количество должно быть больше 13).

Для подтверждения выдвинутой гипотезы в среде MathWorks MATLAB был проведен вычислительный эксперимент, в котором было задействовано 370 ЦИ размером 1000×1000 пикселей разного формата (TIF, JPEG). Среди тестируемых были изображения, полученные непрофессиональными фотографами, а также ЦИ из базы NRCS [14], которая является традиционной при тестировании стеганографических и стеганоаналитических алгоритмов. Далее указанное множество изображений будем называть экспериментальным множеством (ЭМ).

При проведении вычислительного эксперимента на рассматриваемой стадии исследования матрица ЦИ разбивалась на непересекающиеся 8×8-блоки. В результате эксперимента установлено, что количество ЦИ из ЭМ, не содержащих блоков, для которых матрица BB^T имела

бы нулевые значения, составило 86 % от общего числа. Для ЦИ (14 % от общего количества тестируемых), в которых присутствовали нулевые значения среди элементов BB^T для какого-либо из блоков B, среднее количество таких блоков составило 32 или 0,2% от общего числа блоков ЦИ. С учетом того, что для разложимости 8×8-матрицы BB^T количество нулевых значений в ней не может быть меньше 14, в среднем лишь 0,07 % от общего числа блоков ЦИ, в которых присутствовали нулевые значения в BB^T, принципиально могли оказаться разложимыми. Рассмотрим эти блоки подробно.

Предположим, что для BB^T возможно ее представление в виде (4) для некоторой матрицы перестановок $P=\overline{P}$. Матрицу $\overline{P}B\overline{P}^T$ разобьем на подматрицы $B_i, i=\overline{1,4}$: $\overline{P}B\overline{P}^T=\begin{pmatrix} B_1 & B_4 \\ B_3 & B_2 \end{pmatrix}$, где B_1, B_2 имеют размеры $l_1\times l_1$ и $l_2\times l_2$ соответственно. Для B возможны два варианта: $B_4=0$ (в этом случае B будет разложимой) и $B_4\neq 0$. Пусть $B_4=0$. Тогда:

$$\overline{P}BB^T\overline{P}^T=\overline{P}B^T\overline{P}^T\overline{P}B^T\overline{P}^T=(\overline{P}B\overline{P}^T)(\overline{P}B\overline{P}^T)^T=\begin{pmatrix} B_1 & 0 \\ B_3 & B_2 \end{pmatrix}\begin{pmatrix} B_1^T & B_3^T \\ 0 & B_2^T \end{pmatrix}=\begin{pmatrix} B_1B_1^T & B_1B_3^T \\ B_3B_1^T & B_3B_3^T+B_2B_2^T \end{pmatrix}. \quad (5)$$

Равенство $B_1B_3^T=0$ (в соответствии с (4)) приведет к блочной диагональности матрицы $\overline{P}BB^T\overline{P}^T$, в силу чего ее спектр будет равен объединению спектров ее блоков: матриц $B_1B_1^T$ и $B_3B_3^T+B_2B_2^T$. Таким образом, квадраты СНЧ B будут определять собственные значения $B_1B_1^T$ и $B_3B_3^T+B_2B_2^T$. Равенство $B_1B_3^T=0$ с учетом неотрицательности матриц B_1 и B_3 возможно тогда, когда выполняется следующее условие: каждому ненулевому элементу матрицы B_1, находящемуся в *k*-м столбце, должен соответствовать нулевой *k*-й столбец матрицы B_3; в матрице B_3 *j*-й столбец может быть ненулевым только, если нулевым будет *j*-й столбец матрицы B_1. Нулевой столбец B_1 приведет к ее вырожденности, а также к вырожденности $B_1B_1^T$, в силу чего спектр $B_1B_1^T$ будет содержать нулевое собственное значение, а среди СНЧ B окажется нулевое, что, как показывают многочисленные вычислительные эксперименты, для оригинальных ЦИ крайне редко, а в случае ЦИ в формате без потерь практически невозможно.

Пусть $B_4\neq 0$. Тогда:

$$\overline{P}BB^T\overline{P}^T=\begin{pmatrix} B_1 & B_4 \\ B_3 & B_2 \end{pmatrix}\begin{pmatrix} B_1^T & B_3^T \\ B_4^T & B_2^T \end{pmatrix}=\begin{pmatrix} B_1B_1^T+B_4B_4^T & B_1B_3^T+B_4B_2^T \\ B_3B_1^T+B_2B_4^T & B_3B_3^T+B_2B_2^T \end{pmatrix}. \quad (6)$$

Матрица $\overline{P}BB^T\overline{P}^T$ (6) имеет вид (4) при

$$B_1B_3^T+B_4B_2^T=0 \quad \Leftrightarrow \quad \begin{cases} B_1B_3^T=0, \\ B_4B_2^T=0. \end{cases} \quad (7)$$

С учетом неотрицательности матриц B_1, B_2, B_3, B_4 и вышеоговоренного для выполнения матричного равенства $B_1B_3^T=0$, удовлетворение системе (7) является крайне маловероятным.

Все проведенные выше рассуждения имеют место для квадратного блока B любого размера.

Таким образом, можно считать, что матрица BB^T для блоков оригинального ЦИ является неразложимой. Тогда по теореме Фробениуса собственному значению $\overline{\lambda}(BB^T)$ отвечает собственный вектор $\overline{\varphi}(BB^T)$ с положительными координатами, являющийся, как вытекает из (2), одновременно левым СНВ u_1, отвечающим максимальному СНЧ σ_1 блока B.

Аналогичное утверждение будет следовать для правого СНВ v_1 блока B (при рассмотрении вместо BB^T матрицы B^TB), отвечающего σ_1.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Таким образом, в матрице блока B левый и правый СНВ, отвечающие максимальному СНЧ, имеют положительные координаты. Независимо от возмущающего воздействия, которое претерпевает ЦИ, матрицы BB^T, B^TB будут удовлетворять (5) или (6), т.е. останутся неотрицательными неразложимыми, а значит и обсуждаемые СНВ после возмущения будут иметь все положительные координаты, поэтому эти векторы является не только устойчивыми, но и sign-устойчивыми к *любому* возмущающему воздействию. Это возможно лишь в том случае, когда обсуждаемые СНВ близки к *n*-оптимальному вектору $n^0 \in R^l$ [12].

Представим сингулярный спектр блока B в виде вектора $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_l)^T$ из R^l и нормируем его: $\bar{\sigma} = \dfrac{\sigma}{\|\sigma\|}$. Вектор $\bar{\sigma}$ находится в первом координатном ортанте R^l вместе с левым u_1 и правым v_1 СНВ, отвечающими σ_1. Независимо от претерпеваемых ЦИ возмущающих воздействий все СНЧ остаются неотрицательными, причем в оригинальных ЦИ хотя бы одно из них (σ_1) будет положительным, что говорит о том, что вектор $\bar{\sigma}$ никогда не поменяет координатный ортант, в котором расположен, т.е. является sign-устойчивым.

Таким образом, векторы u_1, v_1, $\bar{\sigma}$ обладают общими свойствами: они устойчивы, sign-устойчивы, неотрицательны, располагаются в первом координатном ортанте пространства R^l, причем это имеет место независимо от конкретного вида формата ЦИ. Установленная общность дает возможность предположить существование определенной связи между u_1, v_1, $\bar{\sigma}$ в блоках оригинального ЦИ.

Элементы вектора $\bar{\sigma}$ обладают характерными особенностями для блоков оригинального ЦИ. Как показывают многочисленные вычислительные эксперименты,

$$\sigma_1 >> \sigma_i,\ i = 2,3,...,l\,. \tag{8}$$

Иллюстрацией этому являются результаты, приведенные в табл.1 для 8×8-блоков, для значений отделенностей СНЧ. В общем случае под отделенностью СНЧ $\sigma_i(B)$, $i = 1,3,...,l$, $l\times l$-блока B понимается svdgap(i,B): $\text{svdgap}(i,B) = \min\limits_{i\neq j}\left|\sigma_j(B) - \sigma_i(B)\right|$. Учитывая (8), можно утверждать, что угол между вектором $\bar{\sigma}$ и положительным направлением координатной оси Ox_1 пространства R^l в большинстве блоков ЦИ будет близок к нулю. Таким образом, для оригинального ЦИ:

$$\angle(u_1,\bar{\sigma}) \approx \angle(v_1,\bar{\sigma}) \approx \angle(n^0,e_1)\,. \tag{9}$$

где $\angle(u_1,\bar{\sigma})$, $\angle(v_1,\bar{\sigma})$, $\angle(n^0,e_1)$ — углы между векторами u_1 и $\bar{\sigma}$, v_1 и $\bar{\sigma}$, n^0 и вектором стандартного базиса $e_1 = (1,0,...,0)$ пространства R^l, отвечающего оси Ox_1, соответственно.

Таблица 1

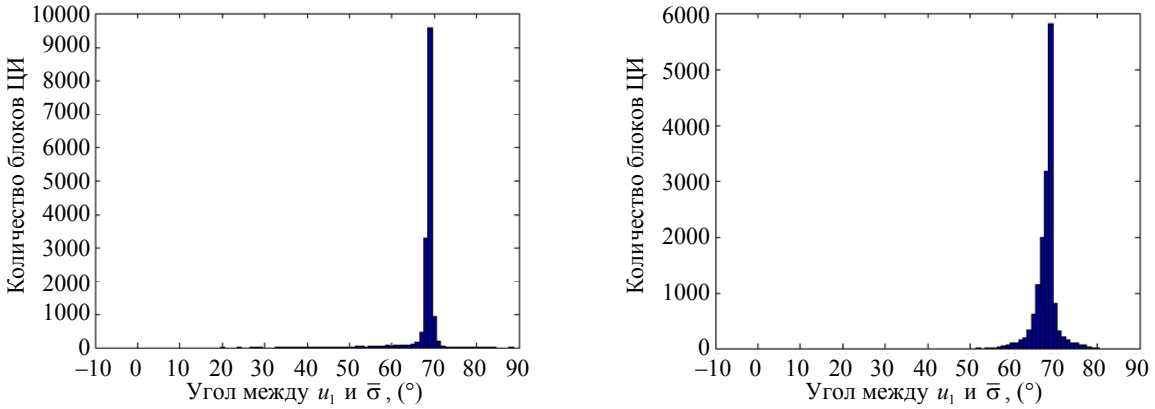
Средние значения отделенности сингулярных чисел 8×8-блоков по 300 ЦИ

Среднее значение svdgap(i,B)							
$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
712,4564	23,1111	7,9843	3,0004	1,4232	0,7125	0,4667	0,5781

Для пространств R^4, R^8, R^{16}, R^{32} в градусном выражении приближенные значения $\angle(n^0,e_1)$ соответственно определяется 60,7°, 69,5°, 75,6°, 79,9°, давая приближенные значения углов $\angle(u_1,\bar{\sigma})$, $\angle(v_1,\bar{\sigma})$ для большинства $l\times l$-блоков оригинального ЦИ при конкретных значениях l.

Для практической проверки полученного утверждения в среде MATLAB был проведен вычислительный эксперимент, в котором были задействованы ЦИ из ЭМ. Результаты эксперимента находятся в полном соответствии с полученными теоретическими выводами. Типичные

результаты исследования двух ЦИ, одно из которых хранилось в формате JPEG, а другое в TIF, выбранных случайным образом из ЭМ, в виде гистограмм (с шагом 1^o) величин углов между векторами u_1 и $\bar{\sigma}$ (Γ_U), блоков, полученных в результате стандартного разбиения ($l = 8$) матрицы изображения, представлены на рис. 1. Аналогичным образом выглядят гистограммы величин углов между векторами v_1 и $\bar{\sigma}$ (Γ_V). Глобальный максимум гистограмм во всех случаях достигается для угла 70^o, что, как подтверждают результаты, приведенные на рис. 2, является неслучайным и отвечает (9). Рис. 2 отражает частоту появления конкретных значений углов между анализируемыми векторами, в которых достигается глобальный максимум Γ_U, Γ_V, отвечающих конкретным изображениям. Как видно, для большинства протестированных ЦИ максимум Γ_U, Γ_V достигается для угла 70^o, причем для оригинальных ЦИ, как и предполагалось, это никак не зависит от формата хранения изображения.



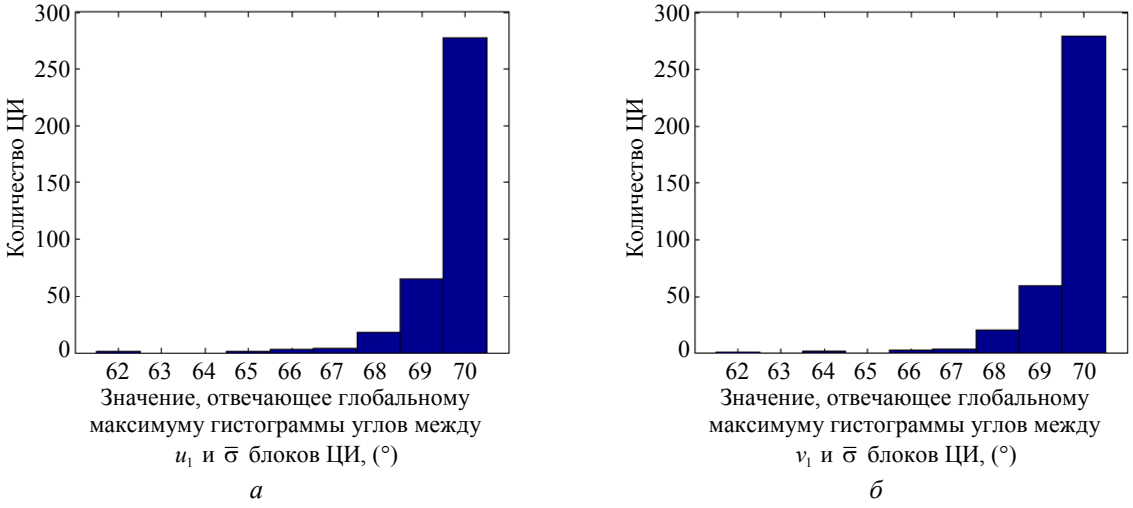
а *б*

Рис. 1. Пример гистограмм значений углов между векторами u_1 и $\bar{\sigma}$ 8×8-блоков в оригинальных ЦИ: а — ЦИ в формате JPEG; б — ЦИ в формате TIF

С учетом того, что целью работы является разработка нового подхода к решению задачи стеганоанализа, эффективного независимо от конкретного вида стеганоалгоритма, использованного для погружения ДИ, а также при малой СПС, на первый взгляд, при анализе ЦИ имеет смысл использовать блоки, по возможности, большего размера. Действительно, если говорить, например, об одном из наиболее распространенных в настоящий момент стеганометодов – методе модификации наименьшего значащего бита, то с учетом специфики погружения ДИ (некоторые элементы матрицы контейнера могут не изменить своего значения, если последний значащий бит используемого для погружения пикселя совпадает с очередным погружаемым битом ДИ) при малой СПС и малом размере блока ЦИ нарушения установленных соотношений между определяющими формальными параметрами в стеганосообщении по сравнению с контейнером будет крайне сложно выявить. В силу этого соотношения (9) проверялись в ходе вычислительного эксперимента для $l\times l$-блоков, где $l = 16$ и $l = 32$. Результаты эксперимента в целом находятся в соответствии с (9), однако характер гистограмм Γ_U, Γ_V “ухудшается”: хотя глобальный максимум и отвечает (9), количество блоков, в которых угол отличается от ожидаемого значения увеличивается по сравнению с картиной для блоков размера 8×8, что подтверждается общими по всему ЭМ результатами. Происходящие “ухудшения” объясняются увеличением накапливаемой вычислительной погрешности с ростом l при вычислении СНВ и СНЧ блоков.

Полученные результаты заставляют отказаться при анализе ЦИ от блоков, для которых $l > 8$. Очевидно, что соотношения (9) будут тем точнее выполняться, чем меньше будет l. Подтверждением являются результаты вычислительного эксперимента для 4×4-блоков. Глобальный максимум Γ_U, Γ_V здесь достигался в значениях: 58^o – 0,8% от общего числа ЦИ в ЭМ, 59° — 0,8 %, 60^o — 18 %, 61^o — 82 % от общего числа ЦИ в ЭМ. Это делает 4×4-блоки наиболее предпочтительными при анализе ЦИ, основанном на соотношении (9).

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)



а *б*

Рис. 2. Гистограммы аргументов глобальных максимумов Γ_U (а), Γ_V (б) 8×8 -блоков матриц ЦИ

Установленные соотношения (9) характерны для оригинальных ЦИ. При возмущении ЦИ эти соотношения будут нарушаться, что подтверждается результатами проведенных вычислительных экспериментов (рис.3). В качестве возмущающих воздействий здесь использовались аддитивный гауссовский и мультипликативный шумы с различными характеристиками. Использование шумов как возмущающих воздействий является неслучайным, т.к. именно при помощи наложения шума часто происходит моделирование стеганопреобразования [15]. В ходе вычислительного эксперимента для оригинальных ЦИ из ЭМ (для наглядности восприятия результаты приведены для 100 ЦИ, выбранных из ЭМ случайным образом) строились Γ_U, Γ_V, для которых определялся аргумент, в котором достигался глобальный максимум (кривая 1 на рис. 3), затем на ЦИ накладывался шум (аддитивный гауссовский с нулевым матожиданием и дисперсией $D = 0{,}001,\ 0{,}01$; мультипликативный с дисперсией $D = 0{,}001,\ 0{,}01$). Для возмущенных ЦИ строились Γ_U, Γ_V (рис. 3 кривые 2 и 3 соответственно). Как видно из результатов эксперимента, кривые, отвечающие возмущенным ЦИ, определенным образом отличаются от кривых, соответствующих оригинальным изображениям: значения аргументов глобальных максимумов Γ_U, Γ_V для зашумленных ЦИ в подавляющем большинстве меньше, чем для оригинальных. Даже в случае, когда наблюдается совпадение, как, например, для ЦИ №47 (рис. 3, *б*), для которого аргументы глобальных максимумов гистограмм углов между v_1 и $\bar{\sigma}$ для оригинального ЦИ и зашумленного (гауссовский шум с $D = 0{,}001$) равны 60, различить оригинальное и возмущенное ЦИ не представляет труда (рис. 4): значение глобального максимума для оригинального ЦИ в 2 раза больше, чем для возмущенного; гистограмма для зашумленного ЦИ “шире” гистограммы для оригинального. Картина с уменьшение значения глобального максимума и “расширением” гистограммы для возмущенного ЦИ по сравнению с оригинальным имеет место и в случае, когда аргумент гистограммы, в котором этот глобальный максимум достигается, изменяется (уменьшается) в зашумленном ЦИ. Соотношение между значением глобального максимума Γ_U, Γ_V и “шириной” гистограммы, оцененной определенным образом, может стать дополнительной определяющей характеристикой, позволяющей отделять оригинальное ЦИ от возмущенного.

Таким образом, для возмущенных ЦИ наблюдается нарушение соотношений (9) для большинства блоков изображения, что и будет использовано при разработке новых универсальных стеганоаналитических алгоритмов.

Выводы. В результате проведенной работы сформированы основы принципиально нового подхода к разработке универсальных стеганоаналитических методов: с учетом того, что стеганопреобразование ЦИ нарушает целостность этого изображения, выявление нарушения целостности является показателем возможного стеганопреобразования.Такой принцип работы сте-

ганоаналитического метода обеспечит его независимость от формата ЦИ-контейнера и ЦИ-стеганосообщения, а также от конкретного вида стеганографического алгоритма, использованного для погружения ДИ.

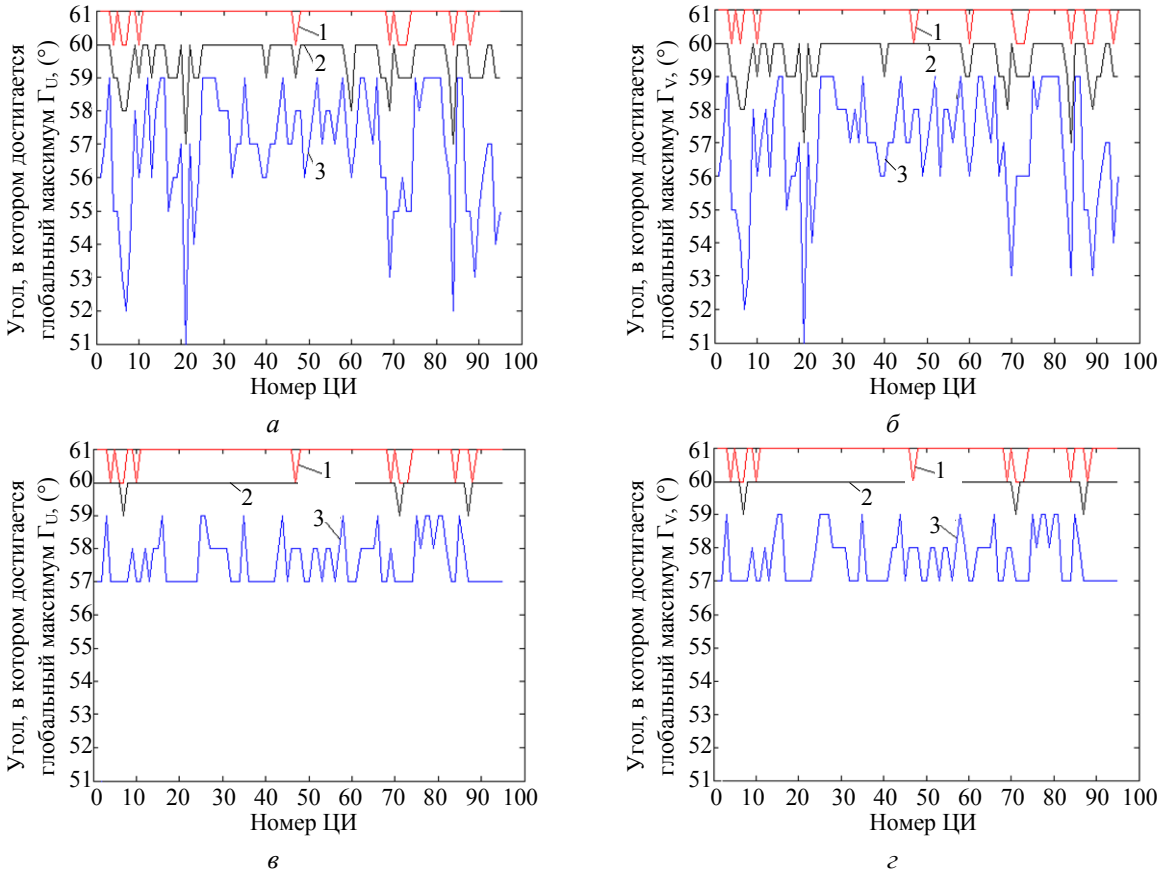


Рис. 3. Кривые, отражающие соответствие аргумента, в котором достигается глобальный максимум Γ_U (а, в), Γ_V (б, г) (при разбиении матрицы ЦИ на 4×4 -блоки) и номера ЦИ: 1 — оригинальное ЦИ; 2 — зашумленное ЦИ (гауссовский (а, б) с нулевым матожиданием, мультипликативный (в, г) шум с $D = 0,001$); 3 — зашумленное ЦИ (гауссовский (а, б) с нулевым матожиданием, мультипликативный (в, г) шум с $D = 0,01$)

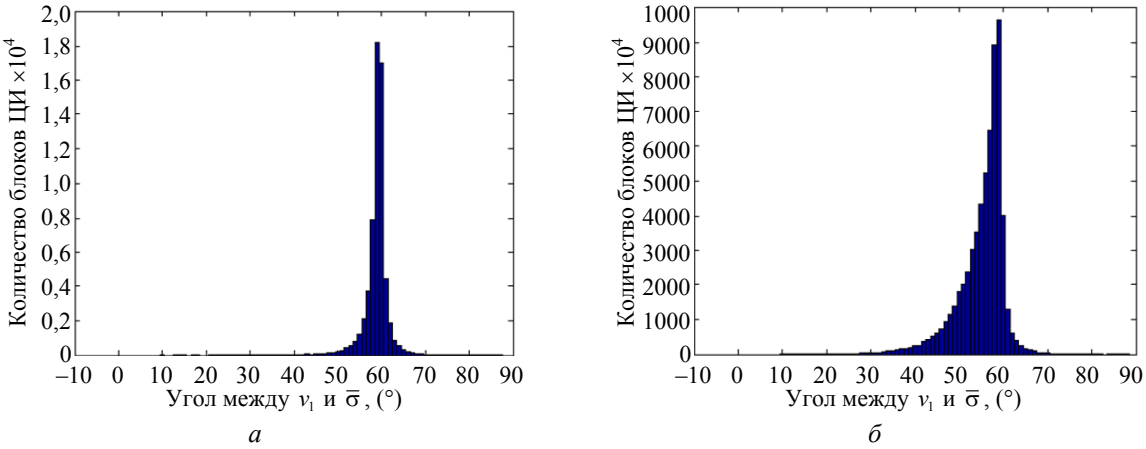


Рис.4. Гистограммы конкретного оригинального (а) и зашумленного (гауссовский шум с нулевым матожиданием и $D = 0,001$) (б) ЦИ (блоки размера 4×4)

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Получены следующие теоретические заключения, нашедшие подтверждение при проведении вычислительных экспериментов:

1. Показано, что для большинства блоков оригинального ЦИ независимо от формата его хранения (с потерями, без потерь) СНВ u_1, v_1, отвечающие максимальному СНЧ, а также нормированный вектор СНЧ $\overline{\sigma}$ имеют общие свойства: устойчивость, sign-устойчивость к возмущающим воздействиям, в том числе, значительным, неотрицательность;

2. Показано, что угол между векторами u_1 и $\overline{\sigma}$, v_1 и $\overline{\sigma}$ для подавляющего большинства $l \times l$-блоков оригинального ЦИ близок к углу между n-оптимальным вектором n^0 и вектором стандартного базиса пространства R^l независимо от формата ЦИ;

3. Показано, что для возмущенных ЦИ соотношение $\angle(u_1, \overline{\sigma}) \approx \angle(v_1, \overline{\sigma}) \approx \angle(n^0, e_1)$ будет нарушаться для большинства блоков, что является показателем нарушения целостности ЦИ, в частности, стеганопреобразования, и может использоваться как основа для разработки новых универсальных стеганоаналитических методов и алгоритмов.

Полученные результаты могут быть использованы не только для разработки универсальных стеганоаналитических методов, на что в настоящий момент направлены усилия автора, но и методов выявления нарушения целостности ЦИ, происходящего в результате любого возмущающего воздействия.

Литература

1. Стеганография, цифровые водяные знаки и стеганоанализ: монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Бобок, И.И. Стеганоанализ как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — № 2. — С. 21 — 34.
3. Natarajan, V. Blind image steganalysis based on contourlet transform / V. Natarajan, R. Anitha // International Journal on Cryptography & Information Security. — 2012. — Vol. 2, Issue 3. — PP. 77 — 87.
4. Gul, G. SVD-based universal spatial domain image steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol. 5, Issue 2. — PP. 349 — 353.
5. Gul, G. Steganalytic features for JPEG compression-based perturbed quantization / G. Gul, A.E. Dirik, I. Avcibas // IEEE Signal Processing Letters. — 2007. — Vol. 14, Issue 3. — PP. 205 — 208.
6. Image steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. Memon, B. Sankur // EURASIP Journal on Applied Signal Processing. — 2005. — Vol. 17. — PP. 2749 — 2757.
7. Agaian, S. Color wavelet based universal blind steganalysis / S. Agaian, H. Cai // The 2004 International Workshop on Spectral Methods and Multirate Signal Processing (SMMSP'2004), September 11–12, 2004, Vienna, Austria. — 2004. — PP. 183 — 189.
8. Fridrich, J. Steganalysis of LSB encoding in color images / J. Fridrich, M. Long // IEEE International Conference on Multimedia and Expo, 30 Jul – 2 Aug 2000, New York, NY. — 2000. — Vol. 3. — PP. 1279 — 1282.
9. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
10. Кобозева, А.А. Общий подход к анализу состояния информационных объектов, основанный на теории возмущений / А.А. Кобозева // Вісн. СНУ ім. В. Даля. — 2008. — № 8(126), Ч. 1. — С. 72 — 81.
11. Bergman, C. Unitary embedding for data hiding with the SVD / C. Bergman, J. Davidson // Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII. — 2005. — Vol. 5681. — PP. 619 — 630.
12. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения-контейнера как основа стеганоалгоритма, устойчивого к сжатию с потерями / А.А. Кобозева, М.А. Мельник // Захист інформації. — 2013. — Т. 15, № 2. — С. 88 — 96.
13. Гантмахер, Ф.Р. Теория матриц: монография / Ф.Р. Гантмахер. — 5-е изд. — М.: Физматлит, 2004. — 559 с.
14. NRCS Photo Gallery: [Электронный ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov/res/sites/photogallery/ (Дата обращения: 01.09.2014).

15. Gkizeli, M. Optimal signature design for spread-spectrum steganography / M. Gkizeli, D.A. Pados, M.J. Medley // IEEE Transactions on Image Processing. — 2007. — Vol. 16, Issue 2. — PP. 391 — 405.

References

1. Agranovskij, A.V., Balakin, A.V., Gribunin, V.G. and Sapozhnikov, S.A. (2009). *Steganography, Digital Watermarking, and Steganalysis*. Moscow: Vuzovskaya kniga.
2. Bobok, I.I. and Kobozeva, A.A. (2011). Steganalysis as a special case of the analysis of the information system. *Suchasna spetsialna tekhnika*, 2, 21-34.
3. Natarajan, V. and Anitha, R. (2012). Blind image steganalysis based on contourlet transform. *International Journal on Cryptography & Information Security*, 2(3), 77-87.
4. Gul, G. and Kurugollu, F. (2010). SVD-based universal spatial domain image steganalysis. *IEEE Transactions on Information Forensics and Security*, 5(2), 349-353.
5. Gul, G., Dirik, A.E. and Avcibas, I. (2007). Steganalytic features for JPEG compression-based perturbed quantization. *IEEE Signal Processing Letters*, 14(3), 205-208.
6. Avcibas, I., Kharrazi, M., Memon, N. and Sankur, B. (2005). Image steganalysis with binary similarity measures. *EURASIP Journal on Applied Signal Processing*, 17, 2749-2757.
7. Agaian, S. and Cai, H. (2004). Color wavelet based universal blind steganalysis. In J. Astola, K. Egiazarian, T. Saramäki (Eds.), *Proceedings of the 2004 International TICSP Workshop on Spectral Methods and Multirate Signal Processing (SMMSP'2004)* (pp. 183-189). Tampere, Finland: Tampere University of Technology.
8. Fridrich, J. and Long, M. (2000). Steganalysis of LSB encoding in color images. In *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2000)* (pp. 1279-1282). Piscataway, NJ: IEEE Service Center.
9. Kobozeva, A.A. and Khoroshko, V.A. (2009). *Analysis of Information Security*. Kyiv: DUIKT.
10. Kobozeva, A.A. (2008). The general approach to the analysis of the state of the information objects based on perturbation theory. *Bulletin of Volodymyr Dahl East Ukrainian National University*, 8(1), 72-81.
11. Bergman, C. and Davidson, J. (2005). Unitary embedding for data hiding with the SVD. In E.J. Delp III, P.W. Wong (Eds.), *Proc. SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII* (pp. 619-630). Bellingham, Wash.: SPIE; Springfield, Va.: IS&T.
12. Kobozeva, A. and Melnik, M. (2013). Sensitivity analysis of singular vectors of cover matrix as basis of steganography algorithm, that steady to lossy compression. *Ukrainian Information Security Research Journal*, 15(2), 88-96.
13. Gantmakher, F.R. (2000). *The Theory of Matrices*. Providence, R.I.; [Great Britain]: AMS Chelsea Pub. (Original work published 1959)
14. USDA: United States Department of Agriculture (n.d.). NRCS Photo Gallery. *United States Department of Agriculture*. Retrieved from http://photogallery.nrcs.usda.gov/res/sites/photogallery/
15. Gkizeli, M., Pados, D.A. and Medley, M.J. (2007). Optimal signature design for spread-spectrum steganography. *IEEE Transactions on Image Processing*, 16(2), 391-405.

АНОТАЦІЯ / АННОТАЦИЯ / ABSTRACT

А.А. Кобозєва. **Основи загального підходу до розробки універсальних стеганоаналітичних методів для цифрових зображень.** У роботі розроблені основи нового загального підходу до організації стеганоаналізу в цифрових зображеннях, у ході чого виявлені, теоретично обґрунтовані й практично перевірені нові властивості формальних параметрів, що визначають зображення. Вперше отримані характеристики взаємного розташування лівого й правого сингулярних векторів, що відповідають найбільшому сингулярному числу матриці (блоку матриці) зображення, і вектора, що складається із сингулярних чисел, отриманих у результаті нормального сингулярного розкладання матриці (блоку матриці): показано, що для більшості блоків оригінального зображення (незалежно від формату зберігання — із втратами, без втрат) кут між лівим (правим) згаданим сингулярним вектором і вектором, що складається з сингулярних чисел, визначається кутом між *n*-оптимальним вектором і вектором стандартного базису простору R^1 відповідної вимірності. Показано, що встановлена особливість порушується для згаданих формальних параметрів в збуреному зображенні, що є показником порушення його цілісності, зокрема, стеганоперетворення, і може бути використаним надалі для розробки нових універсальних стеганоаналітичних методів і алгоритмів, ефективність роботи яких не буде залежати від конкретики стеганоалгоритму, використаного для вбудови додаткової інформації.

Ключові слова: цифрове зображення, матриця, сингулярне число, сингулярний вектор, *n*-оптимальний вектор, нормальне сингулярне розкладання, цілісність зображення, стеганоаналітичний метод.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

А.А. Кобозева. **Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений.** В работе разработаны основы нового общего подхода к организации стеганоанализа в цифровых изображениях, в ходе чего выявлены, теоретически обоснованы и практически проверены новые свойства формальных параметров, определяющих изображение. Впервые получены характеристики взаимного расположения левого и правого сингулярных векторов, отвечающих наибольшему сингулярному числу матрицы (блока матрицы) изображения, и вектора, составленного из сингулярных чисел, полученных в результате нормального сингулярного разложения матрицы (блока матрицы): показано, что для большинства блоков оригинального изображения (независимо от формата хранения — с потерями, без потерь) угол между левым (правым) упомянутым сингулярным вектором и вектором, составленным из сингулярных чисел, определяется углом между *n*-оптимальным вектором и вектором стандартного базиса пространства R^l соответствующей размерности. Показано, что установленная особенность нарушается для упомянутых формальных параметров в возмущенном изображении, что является показателем нарушения его целостности, в частности, стеганопреобразования, и может быть использовано в дальнейшем для разработки новых универсальных стеганоаналитических методов и алгоритмов, эффективность работы которых не будет зависеть от конкретики стеганоалгоритма, использованного для погружения дополнительной информации.

Ключевые слова: цифровое изображение, матрица, сингулярное число, сингулярный вектор, *n*-оптимальный вектор, нормальное сингулярное разложение, целостность изображения, стеганоаналитический метод

A.A. Kobozeva. **A basis of common approach to the development of universal steganalysis methods for digital images.** In this paper a new common approach to the organization of steganalysis in digital images is developed. New features of formal parameters defining the image are identified, theoretically grounded and practically tested. For the first time characteristics of mutual disposition of the left and right singular vectors corresponding to the largest singular value of the matrix (block of matrix) of an image and the vector composed of the singular values obtained as a result of normal singular decomposition of the matrix (block matrix) are obtained. It is shown that for the majority of the blocks of the original image (regardless of the storage format — lossy, lossless) the angle between the left (right) singular vector and the vector composed of singular numbers is determined by the angle between the *n*-optimal vector and the standard space basis of the corresponding dimension. It is shown that the discovered feature is violated for the mentioned formal parameters in the disturbed image. This is an indicator of integrity violation, particularly steganotransformation, and it can be used to develop new universal steganalysis methods and algorithms. Their efficiency does not depend on the specifics of steganoalgorithm used for insertion of additional information.

Keywords: digital image, matrix, singular value, singular vector, *n*-optimal vector, normal singular decomposition, image integrity, steganalysis method.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Чечельницкий В.Я.

Поступила в редакцию 3 ноября 2014 .