УДК 004.056.5

А.А. Кобозева,
доктор технических наук, профессор

ОСНОВЫ НОВОГО ПОДХОДА К ПРОБЛЕМЕ ВЫЯВЛЕНИЯ ФАЛЬСИФИКАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ, ХРАНИМОГО В ПРОИЗВОЛЬНОМ ФОРМАТЕ

Разработаны основы нового подхода к решению задачи выявления и локализации фальсификации цифрового изображения, базирующегося на анализе максимальных сингулярных чисел блоков соответствующих матриц.

***Ключевые слова**: фальсификация, сингулярные числа, цифровое изображение.*

Розроблено основи нового підходу до розв'язання задачі виявлення та локалізації фальсифікації цифрового зображення, що базується на аналізі максимальних сингулярних чисел блоків відповідних матриць.

***Ключові слова**: фальсифікація, сингулярні числа, цифрове зображення.*

The fundamentals of a new approach to the problem of falsification detection and localization in digital images, based on the analysis of the maximum singular values of the blocks of the corresponding matrices, are considered.

***Keywords**: falsification, singular values, digital image.*

Развитие подходов к решению проблемы защиты информации шло по пути от обеспечения защиты чисто формальными механизмами, содержащими, главным образом, технические и программные средства в рамках ОС и СУБД, через выделение управляющего компонента, ядра безопасности, и развитие неформальных средств защиты к формированию взгляда на защиту как на непрерывный процесс, к развитию стандартов на защиту информации, усилению тенденции аппаратной реализации функций защиты, формированию вывода о взаимосвязи защиты информации, архитектуры систем обработки данных и технологии их функционирования, к формированию системного комплексного подхода к информационной безопасности, являющегося определяющим на современном этапе развития [1, 2].

Широкомасштабное использование вычислительной техники, применение цифровых сигналов во всех областях человеческой деятельности, последние успехи в создании, развитии и общедоступность редактирующего цифровые сигналы программного обеспечения (Adobe Photoshop, Adobe Illustrator, Adobe Flash, CorelDRAW и др.) требуют обязательного включения в современную комплексную систему информационной безопасности методов проверки подлинности цифровых изображений (ЦИ), видео, аудио, а также методов и алгоритмов обнаружения и локализации их фальсификации [3–6].

Решению этих вопросов сегодня уделяется много внимания, однако методы, информация о которых доступна из открытой печати, не лишены существенных

недостатков: многие не имеют под собой строгой математической базы [7, 8], некоторые опираются лишь на специфические возможности используемых для получения цифровых сигналов технических средств [9].

В последнее время были предложены новые подходы к решению рассматриваемой задачи: техника, основанная на оценке местоположения источника света [10]; методы, которые основаны на выявлении результатов элементарных операций обработки сигнала, используемых при его фальсификации [8], эффект двойного квантования [11], общий подход к анализу состояния и технологии функционирования информационных систем, базирующийся на теории возмущений [12] и др.

Однако многие из существующих методов не гарантируют при обнаружении фальсификации сигнала ее локализацию, особенно, если размеры области фальсификации малы. Подавляющее большинство методов ориентированы на конкретные форматы хранения цифровых сигналов. В открытой печати отсутствует информация о методе или алгоритме, локализующем область фальсификации, значения размеров которой малы в абсолютном выражении, независимо от формата хранения сигнала.

Все вышесказанное делает актуальным поиск новых подходов к решению рассматриваемой задачи.

В нашей работе для определенности в качестве цифрового сигнала рассматривается ЦИ, хранимое в произвольном формате.

Характер и способы фальсификации изображений могут быть различными. Пусть часть ЦИ, которое будем называть *основным изображением* (ОИ), заменяется частью другого ЦИ, далее называемой *замещающей областью* (ЗО), или вклейкой, причем для большей наглядности никакая последующая обработка производиться не будет. Фальсифицированное изображение (фотомонтаж) сохраняется в произвольном формате (при этом формат как ОИ, так и ЗО также произволен).

Размеры ЗО будут рассматриваться не относительно размеров ОИ, как чаще всего поступают авторы современных публикаций, что сводит при больших размерах ОИ “малые” ЗО к десяткам или даже сотням блоков, получаемых при стандартном разбиении матрицы изображения [13], а в абсолютном виде. Будем далее считать ЗО *малой*, если ее линейные размеры сравнимы с размерами стандартного блока. Задача определения и локализации таких ЗО, как свидетельствуют материалы открытой печати, остается на сегодня не только нерешенной, но даже практически не обсуждается в силу своей сложности.

Целью данной работы является разработка теоретического базиса для создания нового метода выявления и локализации малых ЗО (МЗО) ЦИ, хранимых в произвольных форматах.

Для достижения поставленной цели в работе решаются следующие *задачи*:

1. Определение таких математических параметров ЦИ, отличие которых для разных форматов хранения одного изображения незначительно, при этом анализ характера их изменения позволит отделить фальсифицированное ЦИ от нефальсифицированного;

2. Обеспечение минимизации количества анализируемых параметров;

3. Обеспечение малой вычислительной сложности процесса обработки характеристик анализируемого ЦИ.

Для определенности, не ограничивая общности рассуждений, далее рассматриваются монохромные ЦИ. С учетом отсутствия принципиальных различий между представлениями монохромных и цветных изображений, все полученные ниже результаты без труда могут быть использованы для последних.

ЦИ характеризуется множеством параметров, значимость изменения которых для него различна. Для решения поставленных задач интерес представляют такие параметры, которые характеризуют изображение (или его подобласть) в целом. Одной из важнейших таких характеристик для любого цифрового сигнала является его энергия [13].

Пусть $F - m \times n$ – матрица ЦИ, с элементами f_{ij}, $i = \overline{1,m}$, $j = \overline{1,n}$. Его энергия E может определяться в соответствии с формулами [14]:

$$E = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}^2 , \qquad (1)$$

$$E = \sum_{u=0}^{m-1} \sum_{v=0}^{n-1} P(u,v) , \qquad (2)$$

где $P(u,v)$, $u = \overline{0,m-1}$, $v = \overline{0,n-1}$ – энергетический спектр сигнала [14], представлением которого является матрица F.

Доказательство подлинности ЦИ является важной задачей во многих областях человеческой деятельности: медицине, прессе, судебных разбирательствах и т.д. В подавляющем большинстве случаев качество тестируемого изображения должно быть приемлемым. Это означает, что на ЦИ недопустимо наличие артефактов, которые могут возникнуть, например, после сжатия. Кроме того, плохое качество изображения само по себе вызывает сомнение в его подлинности, что требует от активных нарушителей его целостности дополнительных усилий. Все это приводит к тому, что в процессе решения поставленных задач при рассмотрении для ЦИ форматов с потерями не имеет смысла рассматривать сжатие с произвольно большими коэффициентами. В общем случае логика проведения фотомонтажа потребует от его “автора” использования изображений примерно одного качества (устанавливаемого, возможно, путем субъективного ранжирования), т.к. иначе возрастет вероятность того, что фальсификация будет обнаружена. Таким образом, если ОИ (ЗО) сохранены без потерь, то и ЗО (ОИ) имеет смысл брать без потерь, либо с потерями, но в достаточно высоком качестве. В этом случае энергия изображения в наибольшей степени зависит от его “наполненности”, сцены, а не от формата хранения: если одно и то же ЦИ сохранено без потерь и с потерями в приемлемом качестве, то это практически не отразится на его энергии. Действительно, предположим, что ЦИ, хранимое без потерь, пересохраняется в каком-либо формате с потерями (в приемлемом качестве). Составной необратимой частью сжатия ЦИ является квантование его частотных коэффициентов с последующим округлением до целого значения [13], что при достаточно высоком качестве сжатия приведет к обнулению высокочастотных (наименьших по значению) коэффициентов и незначительному возмущению остальных, дающих основной вклад в E в соответствии с (2). Таким образом,

энергия ЦИ после сжатия с допустимыми коэффициентами изменится незначительно. Если же для хранения ОИ (ЗО) использовался формат с потерями (принципиально здесь можно говорить о произвольном коэффициенте сжатия), то не вызывает сомнения, что для ЗО (ОИ) целесообразно использовать сжатое ЦИ, коэффициент сжатия для которого сравним с аналогичным параметром для ОИ (ЗО).

В [15] получена еще одна формула для вычисления энергии сигнала, представлением которого является матрица *F*:

$$E = \sigma_1^2 + \sigma_2^2 + ... + \sigma_n^2, \quad (3)$$

где

$$\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_n \geq 0 \quad (4)$$

– сингулярные числа [16] (СНЧ) *F*. Основной вклад в *E* вносит σ_1.

Хотя формулы (1), (2), (3) определяют одну и туже величину, вычислительные затраты для ее подсчета здесь различные. Для большей наглядности приводимых результатов предположим, что *m=n*, тогда вычислительные затраты в (1) и (2) определяются как $\underline{O}(n^2)$ арифметических операций, а в (3) – $\underline{O}(n)$, что сразу говорит в пользу (3).

Однако формула (3) представляет интерес не только по указанной выше причине. Все слагаемые в (1) – величины яркости пикселей ЦИ – равнозначны для изображения, ни одно из этих значений не обладает каким-то приоритетом, не несет в себе информацию об изображении в целом, а значит невозможно указать общего способа для уменьшения вычислительной сложности (1) за счет "игнорирования" каких-то слагаемых. Качественная картина меняется в формуле (2): здесь более значимыми по своей величине являются низкочастотные составляющие спектра, делающие основной вклад в значение *E*. Однако учет только низкочастотных составляющих спектра при анализе состояния ЦИ (с целью уменьшения вычислительной сложности при оценке значения *E* путем отбрасывания высокочастотных составляющих) был бы принципиально неправильным: информация о высоких частотах изображения была бы просто утеряна.

Рассмотрим более подробно формулу (3). Каждое СНЧ (в совокупности с соответствующими ортонормированными лексикографически положительными сингулярными векторами) содержит в себе информацию о всех составляющих частотного спектра ЦИ, при этом максимальные СНЧ определяются преимущественно низкими частотами, а минимальные СНЧ – преимущественно высокими [15]. Таким образом, каждое СНЧ, в той или иной мере, несет в себе информацию о сигнале, представлением которого является матрица *F*, в целом. Учитывая особенности человеческого зрения и соотношение (4), наиболее информативными являются максимальные СНЧ. Это дает возможность упростить с вычислительной точки зрения формулу (3), отбрасывая часть последних (наименьших) слагаемых.

Разобьем матрицу ЦИ стандартным образом на 8×8 – блоки [13]. Пусть – матрица произвольного из полученных блоков. Для 8×8 матрицы *B* ее сингулярный спектр в абсолютном большинстве случаев имеет максимальное СНЧ, которое по величине значительно превосходит оставшиеся 7 (примеры приведены

в табл. 1). Учитывая это, для оценки энергии блока ЦИ *E(B)* возможно использовать формулу:

$$E(B) \approx \sigma_1^2, \tag{5}$$

определяющую энергию B по значению единственного параметра – максимального СНЧ σ_1.

О пользе использования для анализа состояния ЦИ значений максимальных СНЧ блоков соответствующей матрицы, кроме (5), идется далее.

Процесс сжатия ЦИ, обеспечивающий его приемлемое качество, является малым возмущающим воздействием для изображения, хранимого первоначально без потерь. Поэтому, если предположить, что B – матрица блока исходного ЦИ с СНЧ $\sigma_j(B)$, $j=\overline{1,8}$, а $B+\Delta B$ – возмущенная в процессе сжатия матрица блока изображения, сохраненного с потерями, где ΔB – соответствующая матрица возмущения, спектральную матричную норму которой обозначим $\|\Delta B\|_2$, то с учетом соотношения [16]:

$$\max_{1\le j\le 8}\left|\sigma_j(B)-\sigma_j(B+\Delta B)\right| \le \|\Delta B\|_2, \tag{6}$$

говорящего о хорошей обусловленности СНЧ, процесс сжатия ЦИ возмутит их незначительно. Иллюстрацией этого может служить следующий типичный пример. Сингулярный спектр 8×8 – блока тестируемого ЦИ, хранимого в формате TIF, имеет вид:

582.5745 10.4029 8.9692 5.5476 3.6722 1.5267 0.7093 0.4504.

После пересохранения этого ЦИ в среде Photoshop в формате JPEG с коэффициентом качества Q=10 сингулярный спектр соответствующего блока претерпел незначительное возмущение:

579.9638 12.5090 9.2304 4.9672 0.9116 0.7002 0.5646 0.0114.

Как видно, максимальное СНЧ, наряду с другими СНЧ, возмутилось незначительно.

Сжатие с большим коэффициентом ЦИ без потерь приведет к более значительным возмущениям максимальных СНЧ блоков. Однако, как было указано выше, при создании фотомонтажа использование хотя бы одного из ОИ и ЗО в формате с потерями с большим коэффициентом, требует и от другого (ЗО или ОИ) формата с потерями сравнимого качества, т.е. характер относительных возмущений в процессе сжатия для максимальных СНЧ блоков как ОИ, так и ЗО, будет качественно практически одинаков.

Таким образом, максимальное СНЧ блока матрицы изображения, наряду с энергией (как показано выше), может рассматриваться как параметр, значение которого практически не зависит от формата хранения. Если говорить о целесообразности дальнейшего использования анализа какого-то из этих параметров – σ_1 или *E(B)* – в процессе выявления и локализации фальсификации ЦИ,

предпочтение на этом этапе обсуждения с учетом вычислительной сложности процесса в целом, очевидно, следует отдать максимальному СНЧ блока.

Таблица 1

Примеры сингулярных спектров блоков тестируемых изображений

№ ЦИ	Формат ЦИ	Сингулярный спектр в порядке убывания СНЧ
1	JPEG	**127.5088** 7.7738 6.3255 2.8162 1.7325 0.9187 0.5016 0.1958
2	JPEG	**107.1995** 3.8881 2.8478 2.1935 0.9315 0.4709 0.3688 0.0665
3	TIF	**1824.5** 3.9000 3.2000 2.0000 1.7000 0.7000 0.3000 0.1000
4	TIF	**777.6581** 93.1154 32.8976 12.6501 7.9000 4.3342 1.9368 0.7656

Как известно, в ЦИ существует корреляция между близлежащими пикселями [13]: значения соседних пикселей, как правило, не могут отличаться очень значительно. Это приведет к тому, что при сдвиге 8×8−блока (влево, вправо, вниз, вверх) в пределах изображения на 1 пиксель энергия блока, с учетом формулы (1), в большинстве случаев изменится незначительно. Незначительные возмущения энергии при сдвиге блока в ЦИ, не подвергавшемся каким-либо несанкционированным изменениям, будут означать незначительные возмущения максимального СНЧ σ_1 в соответствии с (5). Аналогичный вывод об изменении σ_1 при сдвиге блока вытекает из соотношения (6). Таким образом, при переходе от блока к блоку в подавляющем большинстве случаев максимальное СНЧ будет изменяться “плавно”, значения σ_1 будут находиться на гладкой кривой для каждой блоковой строки (столбца) одного ЦИ независимо от формата его хранения. Такое поведение максимального СНЧ является показателем целостности изображения.

Подтверждением сказанному служат результаты вычислительного эксперимента, проведенного в среде Matlab, некоторые из которых приводятся в данной работе для иллюстрации. При проведении эксперимента в тестовых ЦИ выбирались блоковые строки шириной в 1 блок и длиной 1500 пикселей. Для каждого блока, начиная с крайнего левого, со сдвигом на 1 пиксель вправо находилось максимальное СНЧ. Примеры графиков максимальных СНЧ представлены на рис. 1.

Для каждого ЦИ характер функции (область значения, скорость изменения на различных участках области определения, наличие и количество экстремумов, характер выпуклости), определяющей кривую изменения значения σ_1, уникален, поэтому выдвигается следующая *гипотеза*: при нарушении целостности ЦИ путем соединения нескольких изображений в одно это должно проявиться в виде скачка (разрыва первого рода) функции зависимости значения σ_1 от номера блока, отделяющего СНЧ одного ЦИ от СНЧ другого. На практике в большинстве случаев это выглядит так, как проиллюстрировано на рис. 2.

Нарушение гладкости обсуждаемой кривой будет происходить каждый раз при внедрении “инородной” ЗО (МЗО) в ОИ (рис. 3, 4).

Таким образом, очевидной становится целесообразность в качестве единственного параметра, характеризующего каждый блок анализируемого на наличие фальсификации ЦИ, используемого с целью выявления его фальсификации, рассматривать максимальное СНЧ матрицы блока, что находится в полном соответствии с результатами, полученными выше.

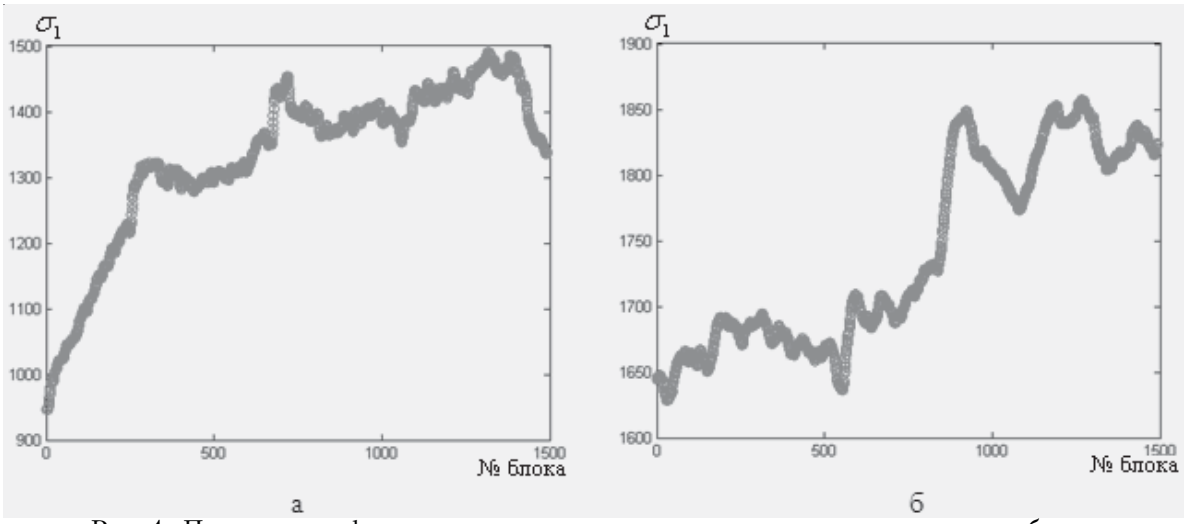

Рис. 1. Примеры графиков изменения максимального сингулярного числа блока в процессе сдвига блока на 1 пиксель для различных ЦИ: а – в формате JPEG; б – в формате TIF

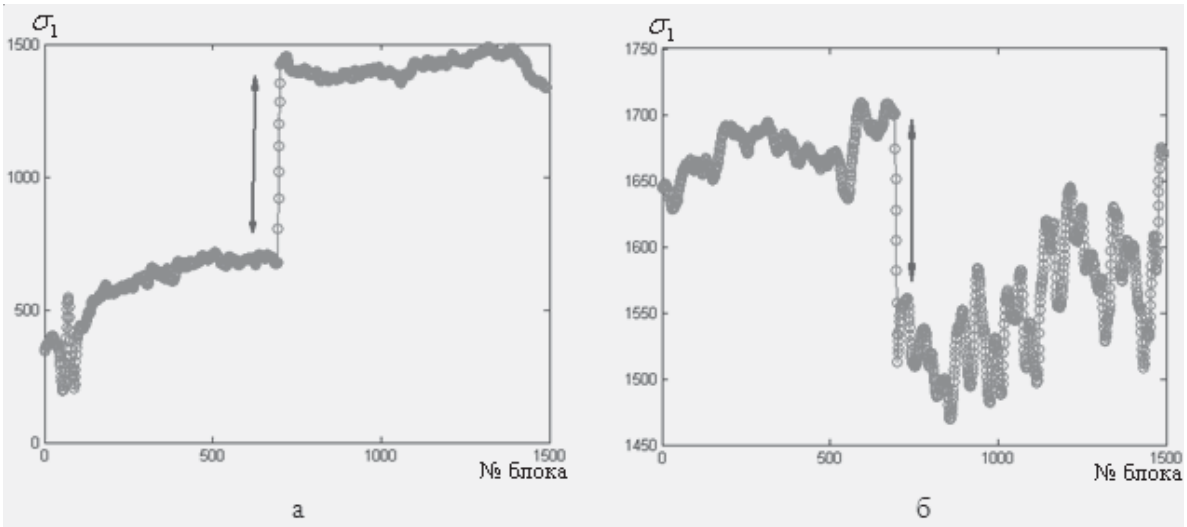

Рис. 2. Характер изменения максимального сингулярного числа блока в процессе сдвига блока на 1 пиксель при соединении двух ЦИ: а – в формате JPEG; б – в формате TIF

Замечание 1. При анализе поведения максимальных СНЧ блоков, определенных выше, возможна ситуация, когда разделение блоков, принадлежащих различным ЦИ (выявление фальсификации), не будет явным (рис. 5). Такая проблема возникает в случае, когда максимальные СНЧ блоков ЦИ, задействованных в фотомонтаже, окажутся близкими по значению в месте соединения изображений: скачок функции изменения максимального СНЧ не будет очевидным. Это приведет к необходимости дополнительных исследований

свойств функции, в частности, ее скорости изменения (производной первого порядка): в малых окрестностях точек разрыва первого рода ее скорость должна быть не просто максимальной по всей области определения, она должна быть близка к бесконечности, что в абсолютном большинстве случаев не свойственно функции изменения максимального СНЧ блока для ЦИ, целостность которых нарушена не была. Практической задачей для автоматизации процесса выявления фальсификации является определение порога для максимального значения производной обсуждаемой функции, отделяющего целостное ЦИ от фальсифицированного.

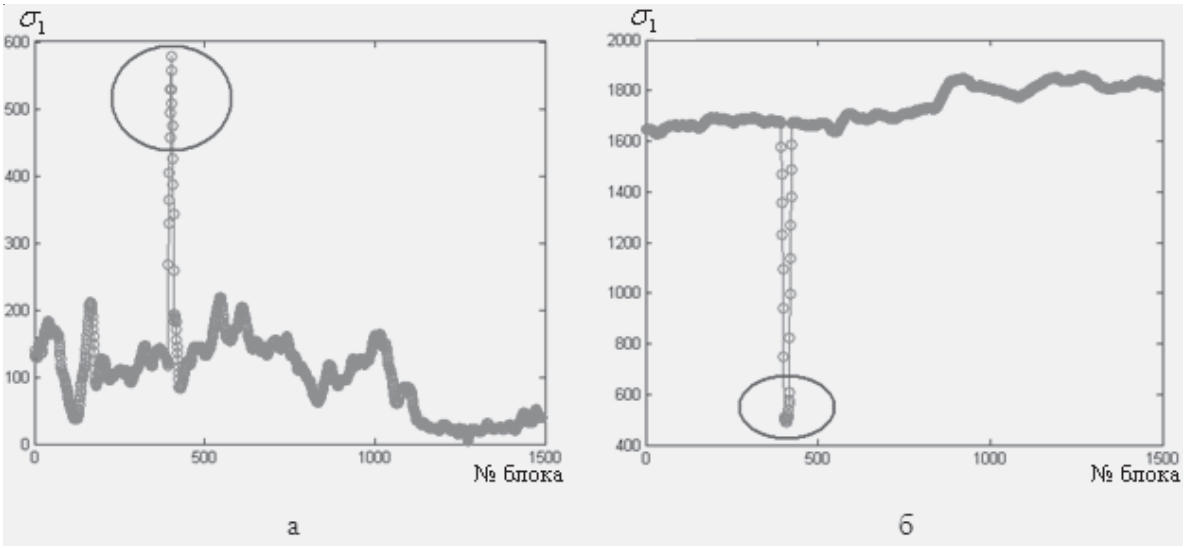

Рис. 3. Характер изменения максимального сингулярного числа блока в процессе сдвига блока на 1 пиксель фальсифицированного ЦИ: а – в формате JPEG; б – в формате TIF (размер ЗО – 8×24 пикселя)

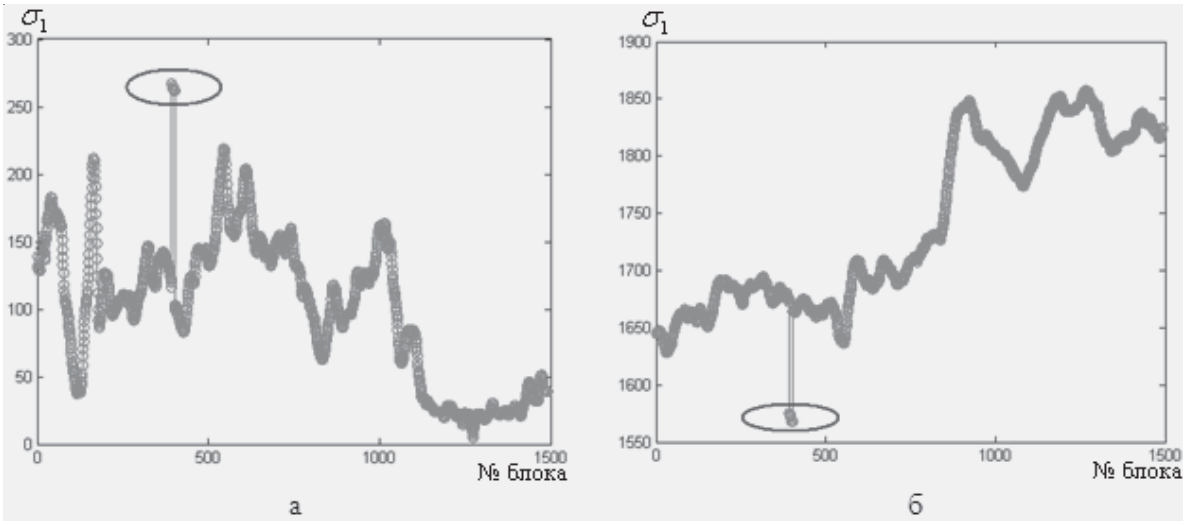

Рис. 4. Характер изменения максимального сингулярного числа блока в процессе сдвига блока на 1 пиксель фальсифицированного ЦИ: а – в формате JPEG; б – в формате TIF (размер ЗО – 8×1пиксель)

Выводы

В работе предложен новый подход к решению проблемы обнаружения и локализации ЗО, в том числе МЗО, в ЦИ произвольного формата. Основой подхода

является анализ поведения максимальных СНЧ блоков тестируемого ЦИ, получаемых при последовательных сдвигах начального блока на 1 пиксель. Вычислительная сложность процесса анализа определяется количеством рассматриваемых блоков ЦИ и максимально составляет $\underline{O}(mn)$ операций, где $m \times n$ – размеры тестируемого изображения.

Как вытекает из проведенных исследований, данный подход позволит построить метод, работающий для ЦИ произвольного формата, выявляющий фальсификации, имеющие линейные размеры, сравнимые с размерами стандартного блока (вплоть до 1 пикселя). Метод должен быть основан на анализе поведения кривых, отражающих изменение максимального СНЧ блока при его последовательном сдвиге на 1 пиксель. Кривая может отвечать блоковой строке матрицы ЦИ (если сдвиг осуществляется вправо–влево) или блоковому столбцу (если сдвиг осуществляется вверх–вниз). Очередная кривая получается при переходе на следующую блоковую строку (следующий блоковый столбец) путем соответствующего сдвига блока на 1 пиксель. Количество блоковых строк (столбцов) определяется при выбранном размере блока как $m - 7$ ($n - 7$). Выявление скачков функции изменения максимального СНЧ блока хотя бы на одной из построенных кривых будет говорить о наличии ЗО, а местоположение скачков даст возможность точной локализации области фальсификации.

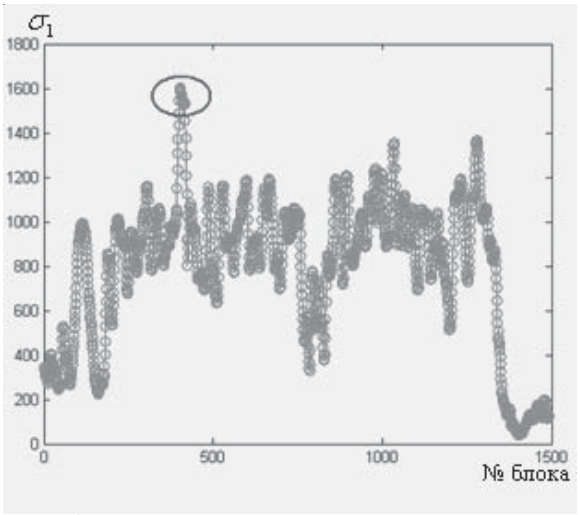

Рис. 5. Характер изменения максимального СНЧ блока в процессе сдвига блока на 1 пиксель фальсифицированного ЦИ: (размер ЗО – 8×16 пикселей)

Выбранный в работе размер блока на данном этапе исследования не является принципиальным, а отвечает лишь стандартному разбиению матрицы ЦИ.

Основной задачей для непосредственной разработки метода выявления ЗО (МЗО) в ЦИ произвольного формата является определение порога для максимального значения производной функции изменения максимального СНЧ блока, отделяющего фальсифицированное изображение от изображения, целостность которого не была нарушена, над решением которой в настоящий момент работает автор.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 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. – Т. 2 : Информационная безопасность. – 2008. – 344 с.

3. *Кобозєва А.А.* Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид-во ДУІКТ, 2010. – 316 с.

4. *Журавель В.В.* К развитию теории выявления следов цифровой обработки сигналограмм / В.В. Журавель, О.В. Рыбальский // Захист інформації. – 2007. – № 1 (32). – С. 83–85.

5. *Рыбальский О.В.* Анализ тенденций разработки современных методов и аппаратуры экспертизы материалов и средств видео и звукозаписи / О.В. Рыбальский // Інформатика та ма тематичні методи в моделюванні. – 2011. –Т. 1, № 1. – С. 12–16.

6. *Кобозева А.А.* Разработка общей теории выявления следов цифровой обработки сигналограмм и ее реализация аппаратно-программным комплексом "Теорема-М" / А.А. Кобозева, О.В. Рыбальский, В.И. Соловьев // Сучасна спеціальна техніка. – 2010. – № 1 (20). – С. 5–14.

7. *Popescu A.C.* Exposing digital forgeries by detecting traces of re-sampling / A.C. Popescu, H. Farid // IEEE Trans. Signal Process. – 2005. – Vol. 53(2). – P. 758–767.

8. *Bayram S.* Image manipulation detection / S. Bayram, B. Sankur, N. Memon // Journal of Electronic Imaging. – 2006. – Vol. 15 (4). – P. 1–17.

9. *Fridrich J.* Invertible authentication / J. Fridrich, M. Goljan, M. Du // Proc. SPIE, Security and Watermarking of Multimedia Contents III. – 2001. – Vol. 3971. – P. 197–208.

10. *Johnson M.K.* Exposing digital forgeries by detecting inconsistencies in lighting / M.K. Johnson, H. Farid // Proc. ACM Multimedia and Security Workshop, 2005. – P. 1–10.

11. *Нариманова Е.В.* Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е.В. Нариманова // Вісник Східноукр-го нац-го ун-ту ім. В. Даля. – 2008. – № 8 (126) – Ч. 1. – С. 47–55.

Отримано 04.12.2012