УДК 621.395

ПРИНЦИПЫ САМОРЕКОНСТРУИРУЮЩЕЙ СТЕГАНОГРАФИИ И ЗАЩИТА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

М. А. Дрюченко

Воронежский государственный университет

Поступила в редакцию 06.05.2015 г.

Аннотация. Рассматривается новый подход к защите цифровых изображений, основанный на внесении не поддающихся компенсации, видимых искажений в защищаемые объекты, приводящий к невозможности их использования неавторизованными лицами. Для восстановления исходного представления искаженных объектов используются принципы «самореконструирующей» стеганографии. Исследуются показатели качества работы предложенного алгоритма на примере изображений формата jpeg.
Ключевые слова: стеганография, цифровые водяные знаки, реконструкция, защита авторских прав.
Annotation. A new approach for digital images protection is considered. It is based on the introduction of significant visible distortions in protected images which leads to the impossibility of their normal usage by unauthorized users. The principles of «self reconstruction» steganography are used to restore the original representation of distorted objects. Quality indicators of the proposed algorithm on an example of jpeg images are represented.
Keywords: steganography, digital watermarks, reconstruction, copyright protection.

ВВЕДЕНИЕ

В эпоху развития цифровых технологий, проблема защиты информации встает особенно остро. Для противодействия возможным злоупотреблениям, связанным с умышленным разрушением, кражей, несанкционированным доступом, чтением, бесконтрольным копированием и тиражированием информации, необходимо применять обоснованные методы и средства обеспечения защиты информации в сочетании с административными и законодательными мероприятиями в этой области.

На сегодняшний день для защиты информации в компьютерных системах чаще всего применяются программно-аппаратные средства, использующие современные криптографические методы. Последние позволяют решить целый ряд вопросов безопасности, связанных с обеспечением конфиденциальности и целостности данных, однако для отдельных приложений информационной безопасности, таких как скрытая коммуникация, защищенное скрытое хранение конфиденциальной информации, защита авторских прав и контроль незаконного тиражирования цифровых объектов, традиционных криптографических методов бывает недостаточно. Для решения перечисленных задач и обеспечения наибольшей степени стойкости к преднамеренным атакам с целью разрушения или выявления защищаемой информации можно использовать методы компьютерной стеганографии [1].

К числу наиболее перспективных и, что, немаловажно, законных направлений практического применения стеганографических методов следует отнести защиту авторских прав на цифровые объекты, а также защиту от незаконного копирования и тиражирования цифровых данных. Популярные на сегодняшний день технологии создания невидимых цифровых водяных знаков (ЦВЗ) и «отпечатков пальцев» (fingerprinting) [2-5], предполагают использование стеганографических принципов скрытного добавления уникальной, идентифицирующей владельца

контента информации, в структуру защищаемых цифровых объектов. В случае выполнения ряда технологических требований, связанных с незаметностью нанесения и обеспечения устойчивости встроенных меток к возможным искажениям маркированного контента, классические схемы создания ЦВЗ частично позволяют решить задачу подтверждения прав авторства и отслеживания несанкционированного распространения защищаемых данных. Следует, однако, отметить, что не нарушаемая при встраивании ЦВЗ функциональность маркируемых объектов, теоретически дает возможность любому желающему осуществлять несанкционированный просмотр полученных незаконным путем маркированных изображений или видео, естественно без дальнейшего их размещения и распространения в Сети.

Одним из возможных перспективных подходов к развитию технологий контроля использования и защиты прав авторства на цифровые изображения (и любые объекты графического контента, обладающие визуальной избыточностью), является подход, предусматривающий внесение значительных видимых искажений в подобные объекты, приводящий к невозможности нормального их использования третьими лицами, с сохранением возможности восстановления исходного представления искаженных объектов авторизованными пользователями за счет использования принципов «самореконструирующей» стеганографии. В простейшем случае, вносимые в изображения искажения представляют собой заливку выделенной области определенным цветом или ее пикселизацию с настраиваемым размером ячейки. Важно также отметить, что с целью ограничения функциональности «маркированных» объектов создаваемые искажения должны затрагивать информативно значимые фрагменты, а также не должны поддаваться компенсации с использованием известных алгоритмов восстановления испорченных областей изображения, наподобие алгоритмов Inpaint [6].

1. ОСНОВНЫЕ ЭТАПЫ «САМОРЕКОНСТРУИРУЮЩЕГО» СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ

Под термином «самореконструкция» будем понимать процесс восстановления исходного или приближенного к исходному представлению цифрового объекта на основе его текущего (отличного от исходного) представления. В терминах стеганографии исходным представлением объекта является пустой контейнер-изображение, а текущим – заполненный контейнер [1].

Пусть I – исходное изображение размером $W \times H$ пикселей, $I_{xy}^{(b)} \subset I$ – искажаемый фрагмент (в простейшем случае прямоугольной формы, размером $w \times h,\ w << W,\ \ h << H,$ имеющий смещение на исходном растре $x = 1, W - w,\ \ y = 1, H - h$). Алгоритм формирования заполненного и восстановленного контейнера включает следующие этапы.

Сначала к I применяется процедура внесения визуальных искажений

$$\tilde{I} = E\left(I, x, y, w, h\right). \qquad (1)$$

Далее в искаженное изображение $\tilde{I}$ с использованием ключа k реализуется процедура стеганографического встраивания исходного представления испорченного фрагмента $I_{xy}^{(b)}$

$$J = F\left(\tilde{I}, I_{xy}^{(b)}, k\right). \qquad (2)$$

В результате формируется «защищенное» изображение J, содержащее искаженную область, не поддающуюся исправлению без знания ключа k. Для восстановления первоначального представления изображения I' применяется процедура стеганографического декодирования вида

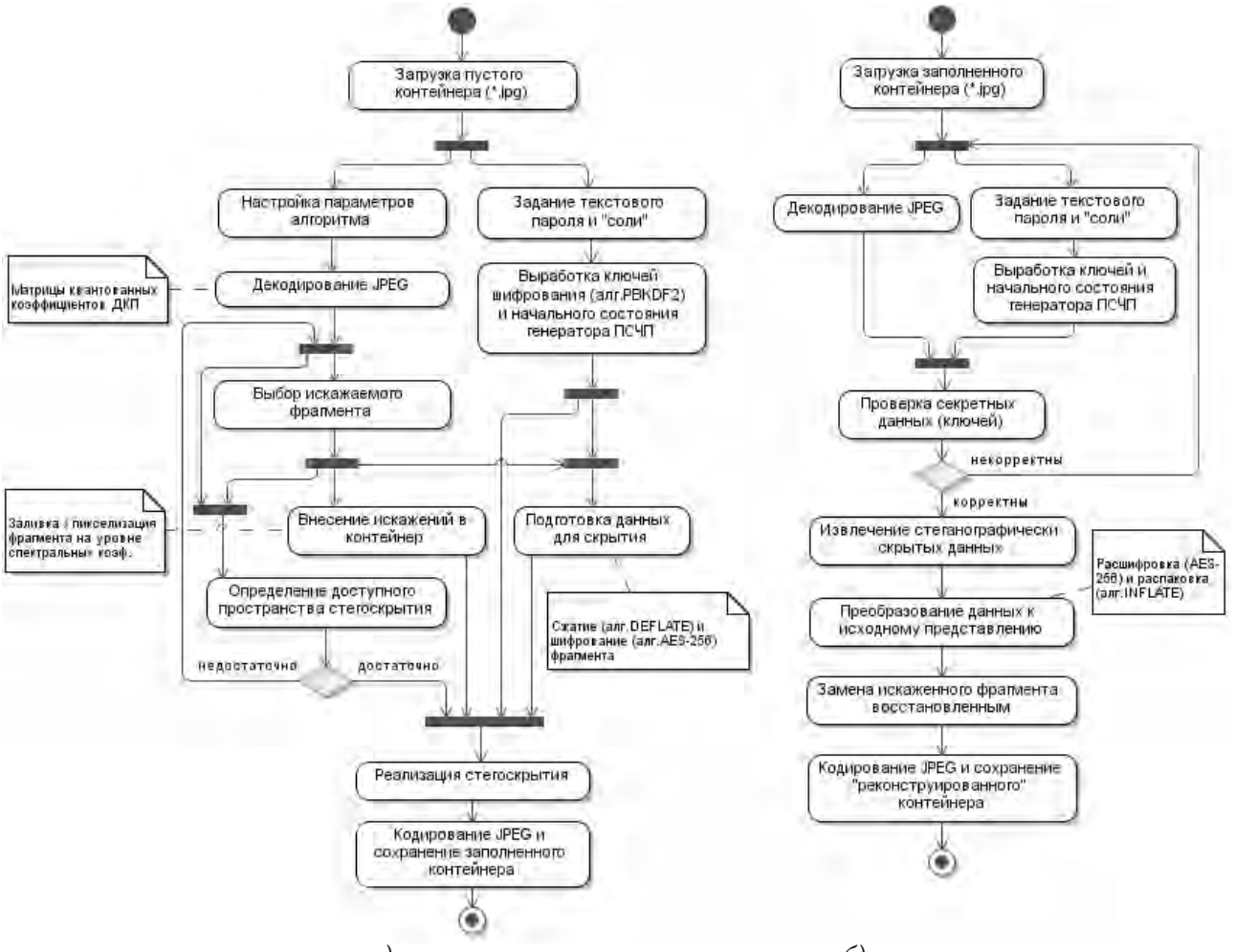
$$I' = F^{-1}\left(J, k\right). \qquad (3)$$

При этом требуется обеспечить выполнение условия $\left\|I - I'\right\| \to \min,$ то есть «реконструированное» изображение должно минимальным образом отличаться от исходного. Для повышения надежности схемы защиты в части противодействия попыткам возможной компенсации искажений Inpaint-подобными алгоритмами, необходимо максимизировать отношение площади искажаемой

области к общей площади исходного растра $S\left(I_{xy}^{(b)}\right)\Big/S\left(I\right)=(wh)/(WH)\to\max$. В терминах стеганографии это может означать максимизацию коэффициента эффективного использования (КЭИ) контейнера, выражаемого отношением размера наибольшего сообщения, которое возможно скрыть в контейнер к объему последнего $КЭИ=\left|I_{xy}^{(b)}\right|\Big/\left|I\right|\to\max$.

Следует также отметить, что помимо размера искажаемого фрагмента, важной характеристикой, определяющей применимость предлагаемой схемы защиты, является местоположение фрагмента(ов) на изображении-носителе. Целесообразным представляется предварительная оценка и выбор наиболее информативных с точки зрения высокоуровневых свойств человеческого зрения областей, искажение которых приведет к обезличиванию или потере смысловой составляющей защищаемого изображения (например, искажение области лиц представленных на фотографии людей).

Реализация предложенного алгоритма защиты изображений была выполнена на примере обработки файлов формата JPEG. Выбор JPEG в качестве базового формата был обусловлен наибольшей его распространенностью для хранения цветных и полутоновых многоградационных изображений фотографий и другой сложной графики, т.е. потенциально защищаемого контента. Обобщенные схемы в нотации языка UML, отражающие основные этапы создания заполненного искаженного и реконструированного контейнеров формата JPEG, приведены на рис. 1. Далее рассмотрим подробнее каждый из этапов работы предлагаемого алгоритма.



а) *б)*

Рис. 1. Обобщенные схемы формирования искаженного заполненного (а) и реконструированного (б) JPEG-контейнера

2. JPEG КОДИРОВАНИЕ/ ДЕКОДИРОВАНИЕ

Основные этапы работы алгоритма сжатия JPEG с добавленным блоком стеганографического встраивания/извлечения массивов данных, описывающих искажаемые фрагменты, приведены на рис. 2.

При обработке полноцветных растров на этапе дискретизации осуществляется преобразование цветового пространства RGB в пространство яркости/цветности YCbCr. На этапе субдискретизации, с учетом свойств человеческого зрения, осуществляется уменьшение разрешения менее информативных каналов цветности Cb, Cr путем усреднения в них групп пикселей. Далее выполняется дискретное косинусное преобразование (ДКП), позволяющее переходить от пространственного представления изображения к спектральному и обратно. Воздействуя на спектральное представление, т. е. отбрасывая наименее значимые «гармоники», можно балансировать между качеством воспроизведения и степенью сжатия изображения. ДКП применяется к блокам 8×8 (реже 16×16) пикселей каждого канала цветности и яркости, в результате чего получаются матрицы коэффициентов ДКП $c_n(i,j)$, n – номер блока, (i,j) – позиция коэффициента внутри блока, $i,j=\overline{0,7}$ $\left(i,j=\overline{0,15}\right)$. За низкочастотную составляющую отвечает DC-коэффициент $c_n(0,0)$. Он содержит информацию о яркости всего блока. Остальные коэффициенты матрицы обозначаются как AC-коэффициенты и отвечают за средние и высокие частоты сигнала. Устранение избыточных высокочастотных коэффициентов происходит на этапе квантования. Полученные матрицы коэффициентов ДКП поэлементно делят на матрицы квантования, после чего значения коэффициентов округляются до целого. Большая часть известных стеганографических методов из тех, что не дописывают данные в конец JPEG файла, используют для встраивания информации именно квантованные коэффициенты ДКП [7].

Последним этапом создания JPEG-файла является переупорядочивание элементов квантованных матриц ДКП для получения векторов коэффициентов, содержащих длинные серии нулевых значений, с последующим кодированием (арифметическим или по Хаффману) данных серий. Сжатые данные записываются в JPEG-файл после специального «SOS» (Start of Scan) маркера – маркера начала сканирования [8].

3. ВНЕСЕНИЕ ИСКАЖЕНИЙ В КОНТЕЙНЕР

На практике преднамеренное скрытие или искажение части картинки используется на телевидении, например, для цензуры, в криминальной хронике, при скрытии логотипов товарных марок и т. д. В качестве базовых преобразований E в (1) рассматривались два типа искажений – однородная заливка и пикселизация выбранной прямоугольной области контейнера $I_{xy}^{(b)}$. Значения пикселей вне искажаемой области не модифицировались $\tilde{I}_{i,j}=I_{i,j},\ i\notin[x,x+w]\vee\ j\notin[y,y+h]$.

В случае заливки всем пикселям, принадлежащим искажаемой области, присваивалось заданное значение цвета $\tilde{I}_{i,j}=\alpha$, $i\in[x,x+w]\vee\ j\in[y,y+h]$, α – цвет заполнения. При обработке JPEG-контейнеров заливка выбранной области осуществлялась изменением отдельных значений квантованных коэффициентов ДКП. Так, для заливки черным цветом блока изображения размером 8×8 соответствующие ему матрицы ДКП яркостных и цветностных составляющих обнулялись, а в низкочастотный коэффициент яркостной матрицы записывалось значение $c_n(0,0)=-150$ или $c_n(0,0)=-127$ для кон-

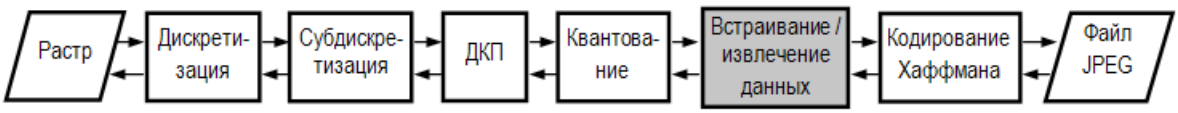


Рис. 2. Конвейер операций, используемый в алгоритме JPEG, дополненный блоком стеганографического встраивания/извлечения данных

а) *б)* *в)*

Рис. 3. Исходное (а), искаженное заливкой (б) и пикселизаций (в) тестовое изображение «Lena.jpg»

тейнеров глубиной цвета 24 или 8 бит/пиксель, соответственно.

Пикселизация фрагмента приводит к уменьшению его разрешения и реализуется усреднением значений пикселей в ячейках заданного размера

$$\tilde{I}_{i,j} = d^{-2} \sum_{k=0,l=0}^{d-1,d-1} I_{i+k,j+l},$$

$$i = x, x+d, \ldots x+w-(w \bmod d) \vee$$

$$j = y, y+d, \ldots y+h-(h \bmod d), \quad d = 4,8,16,32$$

– размер ячейки. При обработке JPEG-изображений пикселизация реализовывалась обнулением всех коэффициентов ДКП в области искажения за исключением низкочастотных. Низкочастотным коэффициентам соседних матриц ДКП, попадающим в одну ячейку, присваивалось их усредненное значение. Примеры описанных вариантов искажений для тестового изображения приведены на рис. 3.

4. СЖАТИЕ И ШИФРОВАНИЕ ИСКАЖАЕМОГО ФРАГМЕНТА

В интересах повышения стойкости предлагаемой схемы защиты изображений к возможным атакам злоумышленника, направленным на восстановление искаженных областей контейнера, в дополнение к стеганографическим преобразованиям целесообразно применять криптографические методы. Согласно представленной на рис. 1 схеме перед стеганографическим встраиванием для уменьшения размера исходного представления искажаемого фрагмента $I_{xy}^{(b)}$ реализуется его сжатие без потерь с использованием алгоритма DEFLATE [9] (библиотека zlib). Сжатие данных потенциально позволяет увеличить размер искажаемой области и т.о. максимизировать КЭИ контейнера. Сжатые данные далее шифруется блочным симметричным алгоритмом AES на 256-битном ключе. Для выработки криптографического ключа на основе задаваемых пользователем значений строкового пароля P и случайной синхропосылки s – «соли», в соответствии с рекомендациями PKCS#5, используется функция диверсификации PBKDF2 (Password-Based Key Derivation Function) [10].

5. СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ФРАГМЕНТА

Основными требованиями, предъявляемыми к алгоритму стеганографического встраивания массивов данных, описывающих исходное представление искажаемых фрагментов, в рамках предлагаемой схемы защиты изображений являются:

– строгий (не вероятностный) характер работы процедуры восстановления информации, позволяющий безошибочно извлекать ранее скрытые данные;

– высокая пропускная способность алгоритма, позволяющая «реконструировать» большие области контейнера.

В качестве базового алгоритма стеганографического скрытия, удовлетворяющего указанным требованиям, был реализован алгоритм модификации наименее значащих бит (НЗБ) квантованных дискретных косинусных

коэффициентов JPEG-контейнера. Для стандартных фотографических изображений данный алгоритм позволяет эффективно скрывать массивы данных, соответствующие искажаемым фрагментам площадью до 10–15 % от площади незаполненного контейнера. Для рандомизации процесса стеганографического скрытия коэффициенты выбираются в порядке, определяемом псевдослучайной числовой последовательностью (ПСЧП), зависящей от введенных пользователем секретных данных P и s. Алгоритм реализует встраивание данных либо в исходный несжатый растр одновременно с осуществлением сжатия изображения (весь конвейер операций на рис. 2), либо в уже сжатое алгоритмом JPEG изображение (последние два этапа на рис. 2). При необходимости искажения больших областей JPEG-контейнера в алгоритме предусмотрено мультиплексирование пропускной способности за счет использования более старших бит коэффициентов ДКП. Следует, однако, отметить, что для большинства фотореалистичных изображений модификация более трех младших разрядов коэффициентов ДКП не желательна, поскольку способна привести к заметному ухудшению качества реконструируемого контейнера.

Перед реализацией стеганографического встраивания оценивается информационная емкость искаженного контейнера $U(\tilde{I}) = \left|\tilde{I}_{xy}^{(b)}\right| \Big/ H\left(\tilde{I}, m\right)$, где $\tilde{I}_{xy}^{(b)} = AES_{K256}\left(deflate\left(I_{xy}^{(b)}\right)\right)$ – сжатый и зашифрованный фрагмент, $\left|\tilde{I}_{xy}^{(b)}\right| \le \left|I_{xy}^{(b)}\right|$; $H\left(\tilde{I}, m\right)$ – пространство стеганографического скрытия, определяемое количеством младших двоичных разрядов квантованных коэффициентов ДКП (во всех каналах JPEG-контейнера), пригодных для встраивания данных, $m = 1, 2, 3$ – определяемое пользователем максимальное число используемых для записи информации младших бит коэффициентов. При малых значениях информационной емкости встраивание реализуется лишь в спектральные коэффициенты цветностных компонент, что позволяет снизить порождаемые стеганографическим скрытием визуальные искажения результирующего контейнера.

Особенностью предлагаемой схемы является ее полная «прозрачность», заключающаяся в отсутствии классического противника, стремящегося определить факт стеганографического скрытия в анализируемом контейнере. В нашем случае потенциальный противник будет иметь в своем распоряжении искаженный заполненный контейнер, гарантированно содержащий данные, необходимые для его реконструкции. Рассмотрение возможных направлений атак противника в части выделения стеганографически скрытых данных и их дешифровки выходят за рамки данной работы. Подробнее рассмотрим вопросы анализа перцептивных искажений, вносимых описанным выше стеганографическим алгоритмом.

6. ОЦЕНКА ИСКАЖЕНИЙ, ВНОСИМЫХ СТОГОАЛГОРИТМОМ

По аналогии с классическими схемами создания ЦВЗ в предложенном алгоритме особое значение имеет перцептивное качество изображения, так как внедренная информация, описывающая искаженную область, не должна существенным образом сказаться на восприятии реконструированного изображения. В литературе, посвященной кодированию изображений и видео [11, 12], для оценки искажений часто используются т.н. объективные критерии, основанные на сравнении исходного и преобразованного изображения – среднеквадратическая ошибка (MSE) или пиковое отношение сигнал-шум (PSNR):

$$MSE_{I,I'} = (wh)^{-1} \sum_{i=1,\, j=1}^{w,h} \left(I_{i,j} - I'_{i,j}\right)^2,$$

$$PSNR_{I,I'} = 20 \cdot \log_{10} \frac{Max_I}{\sqrt{MSE_{I,I'}}},$$

где I – оригинальное изображение; I' – реконструированное; w и h – ширина и высота I, I'; Max_I – максимальное значение цвета изображения I. Данные критерии способны показать наличие дополнительной зашумленности, но в полной мере не отражают наличие структурных артефактов кодирования и не отвечают всем аспектам восприятия искаже-

ний человеком. В качестве дополнительного критерия для оценки уровня визуальных искажений в зависимости от характера изображений и параметров алгоритма стегоскрытия рассматривался универсальный индекс качества (УИК) изображений [13]. С помощью данного критерия оцениваются коррелированность, изменение динамического диапазона, а также изменение среднего значения одного изображения относительно другого. Ввиду нестационарности цифрового сигнала, соответствующего произвольному фотографическому изображению, по аналогии с [14] рассматривался вариант вычисления УИК в непересекающихся блоках изображения фиксированного размера $l \times l$, в пределах которых сигнал можно считать стационарным. Также, с учетом обработки полноцветных контейнеров-изображений, УИК предложено вычислять отдельно по каждому цветовому каналу, а итоговый критерий, характеризующий качество изображения целиком, вычислять как среднее геометрическое значений всех компонент (R,G,B):

$$Q = \sqrt[3]{Q^{(R)} Q^{(G)} Q^{(B)}}, \; Q^{(k)} = N^{-1} \sum_{j=1}^{N} Q_j^{(k)},$$

$$k = \{R, G, B\},$$

$$Q_j^{(k)} = \frac{\sigma_{I^{(k)} I'^{(k)}}}{\sigma_{I^{(k)}} \sigma_{I'^{(k)}}} \cdot \frac{2\overline{I^{(k)}}\,\overline{I'^{(k)}}}{\left(\overline{I^{(k)}}\right)^2 + \left(\overline{I'^{(k)}}\right)^2} \cdot \frac{2\sigma_{I^{(k)}} \sigma_{I'^{(k)}}}{\sigma_{I^{(k)}}^2 + \sigma_{I'^{(k)}}^2} =$$

$$= \frac{4\sigma_{I^{(k)} I'^{(k)}}\,\overline{I^{(k)}}\,\overline{I'^{(k)}}}{\left(\sigma_{I^{(k)}}^2 + \sigma_{I'^{(k)}}^2\right)\left(\left(\overline{I^{(k)}}\right)^2 + \left(\overline{I'^{(k)}}\right)^2\right)},$$

где $Q^{(k)}$ – УИК изображения, вычисленный для его k-й цветовой плоскости (здесь и далее в обозначениях индекс k соответствует одному из трех цветовых каналов изображения); N – число блоков размером $l \times l$, внутри которых вычисляется УИК (размер блоков может варьироваться); $Q_j^{(k)}$ – индекс, характеризующий качество j-го блока изображения;

$$\overline{I^{(k)}} = M^{-1} \sum_{i=1,\, j=1}^{l,l} I^{(k)}(i, j),$$

$\sigma_{I^{(k)}} = (M-1)^{-1} \sum_{i=1,\, j=1}^{l,l} \left(I^{(k)}(i, j) - \overline{I^{(k)}}\right)^2$ – среднее и дисперсия оригинального изображения, $\underline{M = l^2}$ – число элементов в блоке $l \times l$; $\overline{I'^{(k)}}, \sigma_{I'^{(k)}}$ – среднее и дисперсия «реконструированного» изображения; $\sigma_{I^{(k)} I'^{(k)}} = (M-1)^{-1} \times$

$\times \sum_{i=1,\, j=1}^{l,l} \left[\left(I^{(k)}(i, j) - \overline{I^{(k)}}\right)\left(I'^{(k)}(i, j) - \overline{I'^{(k)}}\right)\right]$ – взаимная корреляционная функция изображений $I^{(k)}$, $I'^{(k)}$. Значения УИК $Q \in [-1, 1]$, минимальному искажению изображения соответствуют значения $Q \approx 1$.

Экспериментальный анализ разработанного алгоритма в части оценки уровня искажающих изменений контейнера проводился с использованием полноцветных изображений из наборов Kodak Lossless True Color Image Suite [15] и TESTIMAGES [16]. Разрешение изображений варьировалось от 512×512 до 1600×1600 пикселей. Тестовые изображения были разбиты на три группы согласно характеру их содержимого. В первую группу вошли гладкие изображения, содержащие большие участки с плавными переходами цвета; во вторую – контрастные, пестрые изображения; в третью – изображения смешанного типа, содержащие контрастные и монотонные области. Для изначально несжатых тестовых изображений каждой группы формировались JPEG представления заданного качества (quality factor) $q = 10, 20, \ldots 100$. Искажению подвергались центральные области JPEG контейнеров. Для обеспечения максимального КЭИ площадь искажаемых и сжимаемых фрагментов $I_{xy}^{(b)}$ выбиралась максимально возможной. Кроме того, для мультиплексирования пропускной способности контейнера помимо случая использования для записи информации одного младшего бита коэффициентов ДКП, рассматривались варианты использования двух и трех НЗБ. Фрагменты типовых образцов JPEG изображений каждой группы («monarch.jpg», «baboon.jpg», «Lena.jpg»), полученных после искажения и последующей реконструкции, приведены на рис. 4. Представленные на рис. 4 изображения и соответствующие им оригиналы имеют качество JPEG сжатия равное 80. При ближайшем рассмотрении артефакты в виде блочности, возникшие в резуль-

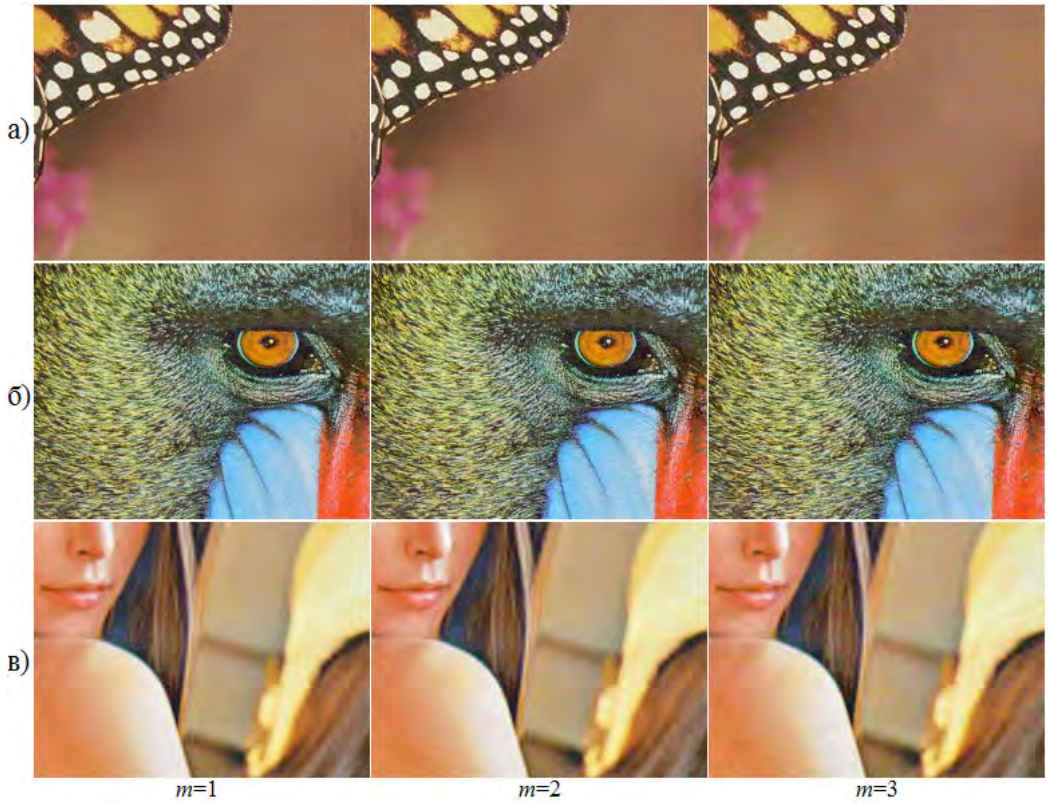


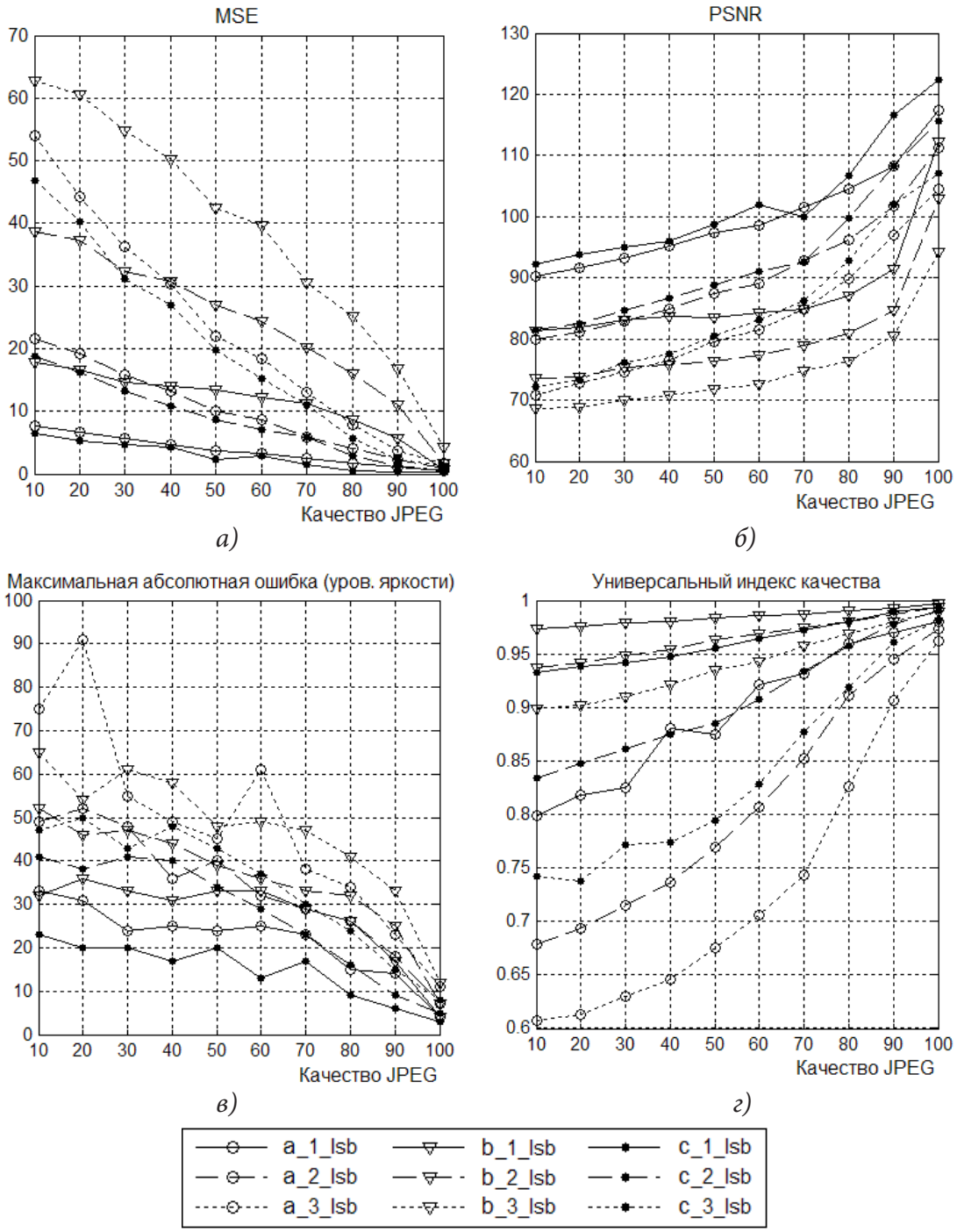
Рис. 4. Фрагменты гладких (а), контрастных (б) и смешанного типа (в) реконструированных тестовых изображений, полученных для трех уровней мультиплексирования пропускной способности контейнера

тате стегоскрытия, наблюдаются на гладких изображениях (рис. 4а) при $m \geq 2$. В меньшей степени визуальные искажения проявляются на контрастных и смешанных изображениях (рис. 4б, в).

Значительное влияние на перцептивное качество реконструируемых JPEG контейнеров оказывает параметр качества их сжатия. Зависимости *MSE*, *PSNR*, максимальной абсолютной ошибки и модифицированного УИК от качества сжатия тестовых JPEG-изображений и максимального числа НЗБ, используемых для скрытия данных, приведены на рис. 5.

Как показали результаты экспериментов (для максимального КЭИ контейнеров) среднеквадратическая ошибка существенно возрастает с уменьшением качества искажаемых JPEG контейнеров параллельно с использованием для стегоскрытия более одного НЗБ спектральных коэффициентов. В большей степени это касается контрастных изображений из второй группы. Так, для изображений данной группы $MSE > 20$ при $q = 70$ и $m \geq 2$. Важно отметить, что минимальные значения *MSE* при $m \leq 2$ наблюдаются для гладких и смешанных изображений, что в общем случае противоречит визуальному их восприятию. Характер зависимостей уровня искажения по критерию *PSNR* от q и m (рис. 5б) аналогичен соответствующему характеру зависимостей для критерия *MSE*. С точки зрения данных критериев приемлемые искажения наблюдаются для качественных ($q > 60$) гладких и смешанных, а также для очень качественных ($q \geq 90$) контрастных изображений, содержащих скрытые данные не более чем в двух НЗБ спектральных коэффициентов.

Достаточно большие значения абсолютной ошибки (рис. 5в), определяемой наибольшей по модулю разностью значений яркости пикселей оригинального и реконструированного изображений, при относительно малом количестве модифицируемых НЗБ ($m \leq 3$), можно объяснить принципом работы самого алгоритма JPEG и используемым принципом стеганографического скрытия, когда модификация значения одного спектрального коэф-



«a» – гладкие; «b» – контрастные; «c» – изображения смешанного типа; «1,2,3_lsb» – число НЗБ, используемых для стегоскрытия

Рис. 5. Зависимости среднеквадратической ошибки искажения контейнера (а), пикового отношения сигнал-шум (б), максимальной абсолютной ошибки (в) и модифицированного УИК от качества сжатия тестовых JPEG-изображений и максимального числа НЗБ, используемых для скрытия данных

фициента приводит к изменению значений множества пикселей в рамках блока 8×8. Если для $m=3$ максимальное десятичное значение, на которое могут изменяться коэффициенты ДКП, равно семи, то при декодировании JPEG в растр соответствующие пиксели оригинального и модифицированного изображений могут отличаться более чем на семь единиц, особенно в случае модификации нескольких коэффициентов ДКП в одном

блоке. Максимальные значения абсолютной ошибки были получены для контрастных и гладких групп изображений при $m = 3$.

Наиболее точные оценки перцептивного качества реконструированных изображений были получены с использованием модифицированного УИК, который рассчитывался для блоков размером 15×15 пикселей (рис. 5г). При обработке гладких изображений приемлемые (визуально незаметные) искажения фиксируются при $Q \geq 95$ для JPEG контейнеров высокого качества ($q \geq 80$ при $m = 1$ и $q \approx 100$ при $m \geq 2$). Для изображений смешанного типа приемлемые искажения наблюдаются для контейнеров высокого ($q > 80$ при $m \geq 2$) и среднего ($q \geq 50$ при $m = 1$) качества. Для контрастных изображений первоначальное высокое качество JPEG сжатия ($q \geq 70$) необходимо при использовании трех НЗБ спектральных коэффициентов для скрытия данных. Следует отметить, что пороговое значение УИК, определяющее приемлемый уровень искажений, может меняться в зависимости от характера изображений. Так, зависимости, полученные для большинства из рассмотренных тестовых изображений (исключая очень гладкие и имеющие $q \geq 50$), при $Q \geq 90$ будут хорошо согласовываться с визуальной экспертной оценкой.

ЗАКЛЮЧЕНИЕ

В работе рассмотрен новый подход к защите от несанкционированного использования цифровых изображений формата jpeg, основанный на внесении значительных видимых искажений во фрагменты изображениия с одновременным стеганографическим кодированием исходного представления искаженных фрагментов в нетронутые области графического контейнера. Для восстановления легальными пользователями исходного представления изображения применяется обратное стеганографическое преобразование. Среди преимуществ предложенного алгоритма можно отметить следующие:

– отсутствие у неавторизованных лиц возможности полноценного использования контента без знания секретных ключей (фактически соответствующих разрешений со стороны правообладателя);

– отсутствие необходимости хранения исходных копий неискаженных изображений или видео файлов;

– возможность предварительного ознакомления потенциальных пользователей с «частично испорченным» контентом с перспективой дальнейшего его приобретения;

– относительная простота реализации.

В качестве ограничений по использованию предложенного алгоритма можно отметить невозможность его применения для защиты данных, не допускающих даже минимальных потерь качества (например, астрономических снимков).

Тестирование алгоритма на разных изображениях показало, что практическая его применимость в значительной мере определяется характером содержимого и качеством сжатия искажаемых и реконструируемых JPEG контейнеров. На основе совокупности рассмотренных критериев оценки искажений наилучшие результаты (с точки зрения максимального КЭИ контейнера и минимального уровня искажений реконструируемых изображений) фиксируются для JPEG контейнеров смешанного типа. Для стегоскрытия испорченных фрагментов целесообразно использовать не более двух младших бит спектральных коэффициентов JPEG. Оптимальный размер и местоположение искажаемых фрагментов, чаще всего зависят от содержимого оригинального изображения и, следовательно, должны определяться индивидуально для каждого контейнера в контексте решаемой задачи.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 13-01-97507 р_центр_а и Фонда содействия развитию малых форм предприятий в научно-технической сфере по программе «Старт-2014» заявка №2014-1-01262.

СПИСОК ЛИТЕРАТУРЫ

1. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков. – М. : Солон-пресс, 2002. – 272 с.

2. *Coatrieux G.* A watermarking-based medical image integrity control system and an image moment signature for tampering characterization / G. Coatrieux, H. Huang, H. Shu, and L. Luo // IEEE Journal of Biomedical and Health Informatics. – 2013. – Vol. 17(6). – P. 1057–1067.

3. *Lee J. S.* The system integration of DRM and fingerprinting / J. S. Lee, K. S. Yoon // in Proceedings of the 8th International Conference Advanced Communication Technology (ICACT'06). – 2006. – Vol. 3. – P. 2180–2183.

4. *Liu K. C.* Colour image watermarking for tamper proofing and pattern-based recovery / IET Image Processing. – 2012. – Vol. 6(5). – P. 445–454.

5. *Сирота А. А.* Нейросетевые функциональные модели и алгоритмы преобразования информации для создания цифровых водяных знаков / А. А. Сирота, М. А. Дрюченко, Е. Ю. Митрофанова // Известия высших учебных заведений. Радиоэлектроника. – 2015. – Т. 58, № 1. – С. 3–16.

6. *Oliveira M.* Fast Digital Image Inpainting / M. Oliveira, B. Bowen, R. McKenna, Yu-Sung Chang // International Conference on Visualization, Imaging and Image Processing (VIIP 2001), Marbella, Spain. 2001.

7. *Provos N.* Hide and seek: An introduction to steganography / N. Provos, P. Honeyman // IEEE Security Privacy. – 2003. – P. 32–44.

8. *Миано Дж.* Форматы и алгоритмы сжатия изображений в действии / Дж. Миано. – М. : ТРИУМФ. – 2005. – 330 с.

9. An Explanation of the Deflate Algorithm [Электронный ресурс]. – URL: www.zlib.net/feldspar.html (дата обращения 02.05.2015).

10. PKCS #5: Password-Based Cryptography Specification Version 2.0 [Электронный ресурс]. – URL: http://www.rfc-base.org/txt/rfc-2898.txt (дата обращения 02.05.2015).

11. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.

12. *Сэломон Д.* Сжатие данных, изображений и звука / Д. Сэломон. – М.: Техносфера, 2004. – 368 с.

13. *Wang Z.* A Universal Image Quality Index / Z. Wang, A. C. Bovik // IEEE Signal processing letters. – 2002. – Vol. 9(3). – P. 81–84.

14. Модифицированный критерий оценки качества восстановленных изображений / С. А. Арляпов [и др.] // Доклады 8-й Международной конференции «Цифровая обработка сигналов и ее применение» Обработка и передача изображений, № 2. – 2006. – С. 411–414.

15. A set of test images «Kodak Lossless True Color Image Suite» [Electronic resource]. – URL: http://r0k.us/graphics/kodak/ (request date 02.05.2015).

16. A set of test images «TESTIMAGES» [Electronic resource]. – URL: http://testimages.tecnick.com (request date 02.05.2015).

Дрюченко Михаил Анатольевич – доцент кафедры технологий обработки и защиты информации Воронежского государственного университета.
E-mail: m_dryuchenko@mail.ru.

Dryuchenko Mikhail Anatolievich – docent at the Chair of Information Processing and Security Technologies at Voronezh State University.
E-mail: m_dryuchenko@mail.ru.