Сравнение эффективности различных подходов к защите JPEG-изображений полухрупкими водяными знаками

А.А. Егорова[1], В.А. Федосеев[1,2]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086
[2]Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

Аннотация. Одним из способов защиты изображений от подделки является встраивание в них цифровых водяных знаков (ЦВЗ) – добавочной информации, разрушающейся при внесении несанкционированных изменений. Отдельной сложностью при проектировании алгоритмов встраивания подобных ЦВЗ является обеспечение их стойкости к допустимым преобразованиям, наиболее характерным примером которых является сжатие с потерями. Такие ЦВЗ называются полухрупкими. Настоящая работа посвящена исследованию различных алгоритмов встраивания ЦВЗ, проявляющих себя как полухрупкие по отношению к JPEG-сжатию. Интерес представляет исследование влияния объёма встраиваемой информации, местоположения отбираемых для встраивания спектральных коэффициентов, а также конкретных методов их модификации на качество результирующего (защищённого) изображения, а также на точность решения искомой задачи аутентификации. Данное исследование проведено с целью выработки рекомендаций по выбору сочетаний этих параметров в зависимости от конкретных условий использования защищаемого изображения.

1. Введение

На сегодняшний день в связи с повсеместным распространением Интернета получение доступа к цифровой информации, в том числе к изображениям, не представляет трудности. В то же время современные средства редактирования, обработки изображений позволяют с лёгкостью вносить изменения в содержимое изображений даже рядовому пользователю. В ряде случаев такие изменения могут быть преднамеренно вредоносными или могут непреднамеренно повлиять на интерпретацию содержимого, что может привести к нарушению авторских прав и нанести тем самым значительные убытки правообладателю. По этой причине защита изображений от изменений и проверка их подлинности является весьма актуальной задачей.

Одним из способов её решения является встраивание в изображения хрупкого или полухрупкого цифрового водяного знака (ЦВЗ) – малозаметной и легко удаляемой компоненты, наличие которой может свидетельствовать о подлинности изображения [1]. Хрупкие ЦВЗ удаляются при любых операциях. Однако чаще всего в задаче защиты изображений от изменений предполагается существование некоторого набора допустимых операций. В таком случае применяются полухрупкие ЦВЗ, являющиеся стойкими к разрешённым преобразованиям и хрупкими ко всем прочим. К числу разрешённых изменений, как правило, относят искажения, которые не оказывают существенного влияния на содержимое

изображения, не нарушают его структуру. Наиболее характерным примером являются искажения, возникающие вследствие сжатия изображения с потерями.

В настоящей статье в качестве разрешённого преобразования рассматривается сжатие в формате JPEG. С момента появления этого формата было разработано не менее двух десятков систем встраивания ЦВЗ, проявляющих стойкость к JPEG при хрупкости к большинству других преобразований. Наибольшее распространение получили системы, производящие встраивание в частотную область, а именно в коэффициенты дискретного косинусного преобразования (ДКП), которые подвергаются операции квантования при JPEG-сжатии [2-15]. Такие системы обеспечивают визуальную неразличимость ЦВЗ и одновременно с этим обеспечивают устойчивость к JPEG при низких значениях показателя качества сжатия. Среди них особую ценность представляют системы, позволяющие задавать минимальное значение показателя качества JPEG, при котором искажения расцениваются как разрешённые [4, 7, 9].

Несмотря на большое число готовых решений, в литературе практически отсутствует информация об их сравнении при различных условиях использования. Или, говоря более широко, не исследованным является вопрос влияния объёма встраиваемой информации, местоположения отбираемых для встраивания спектральных коэффициентов, а также конкретных методов их модификации на качество результирующего изображения, а также на точность решения искомой задачи аутентификации.

Так, большинство алгоритмов [5-13] предполагают использование низкочастотных или среднечастотных коэффициентов, но на сегодняшний день нет работ, которые бы доказывали безусловную правильность такого подхода. Так, к числу его минусов можно отнести тот факт, что эти коэффициенты являются более информативными, нежели высокочастотные, таким образом, их изменение может привести к ухудшению качества защищаемого изображения. Помимо этого, известны работы [2, 4], в которых встраивание осуществляется в область высоких частот и при этом обеспечивается хорошее качество детектирования ЦВЗ.

Другим вопросом при разработке полухрупких к JPEG ЦВЗ-систем является выбор метода изменения спектральных компонент при встраивании ЦВЗ. Наибольшее распространение получил метод QIM (Quantization Index Modulation) и его модификации [16], а также метод изменения наименее значимых бит (НЗБ-встраивание) [1]. Однако известны и иные подходы, в частности, базирующиеся на изменении позиции последнего ненулевого элемента (Last Non Zero, LNZ) [10] или на использовании табличных преобразований [11].

Наконец, в зависимости прикладной задачи количество встраиваемых бит также может варьироваться. Если необходимо, чтобы была осуществлена не только проверка подлинности изображения (аутентификация), но и процедура восстановления искажённой информации (получение оригинала) или извлечение информации о правообладателе, то, как правило, требуется встроить большее число бит. Дополнительные требования к высокой надёжности метода также требуют встраивания большего количества информации.

Настоящая работа посвящена исследованию влияния выбора позиций квантованных коэффициентов ДКП для встраивания, их количества, а также метода встраивания на объективные показатели качества результирующей ЦВЗ-системы с целью определения их сочетаний, обеспечивающих наилучшие показатели в различных условиях.

2. Алгоритм JPEG сжатия с потерями

JPEG-сжатие включает следующие ключевые шаги (см. рисунок 1) [17]:

- Исходное изображение $I(n_1, n_2)$ размера $N_1 \times N_2$ делится на непересекающиеся блоки $I_i(n_1, n_2)$ размера 8×8, где $i = 1, \dots, N$ – номер блока, а $N = N_1 N_2 / 64$ – общее количество непересекающихся блоков.
- Для каждого блока $I_i(n_1, n_2)$, состоящего из 64 отсчётов, вычисляется прямое ДКП, которое раскладывает значения отсчётов блока по различным частотам. Полученные значения мы будем обозначать $B_i(m_1, m_2)$. Коэффициенты, расположенные вблизи левого верхнего угла, характеризуют низкочастотную составляющую.

- Производится квантование коэффициентов каждого блока $B_i(m_1, m_2)$ с использованием матрицы квантования Q_{QF} размера 8×8, соответствующей заданному пользователем значению параметра качества сжатия QF (от 1 до 100). Квантование осуществляется по формуле

$$D_i(m_1, m_2) = round\left(\frac{B_i(m_1, m_2)}{Q_{QF}(m_1, m_2)}\right). \quad (1)$$

Снижение значения QF приводит к увеличению значений в матрице Q_{QF}, что в свою очередь влечёт большее число нулей среди значений $D_i(m_1, m_2)$ и, как следствие, меньший размер архива.

- Обход значений $D_i(m_1, m_2)$ в порядке зигзагообразной развёртки (см. рисунок 2) и последующее статистическое кодирование этих значений.

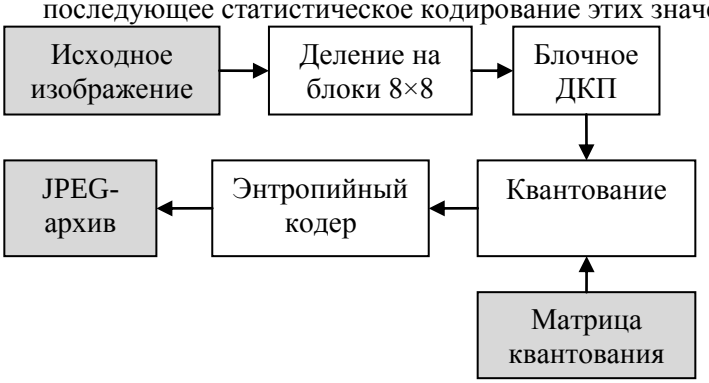

Рисунок 1. Схема кодирования изображения в формате JPEG.

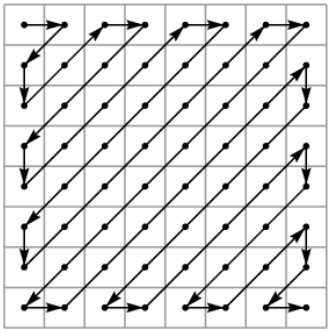

Рисунок 2. Зигзагообразная развёртка спектра ДКП.

3. Анализ существующих систем полухрупких ЦВЗ для JPEG-изображений

Как отмечалось ранее, потеря информации в алгоритме JPEG происходит на этапе квантования коэффициентов ДКП. По этой причине встраивание ЦВЗ в частотных системах (алгоритмах) происходит либо также на этапе квантования, либо непосредственно вслед за ним.

В основе многих методов лежат два главных свойства процедуры квантования, применяемой в стандарте JPEG [3]:

- Отношения между коэффициентами блоков до и после квантования не изменяются.
- Квантованное с некоторым (первоначальным) шагом значение можно восстановить после последующего квантования с меньшим шагом, если к искажённому числу повторно применить процедуру квантования с первоначальным шагом.

Так, например, в системе Ho & Li, 2004 [4] учитывается свойство сохранения отношений между коэффициентами соседних блоков. Сначала в рассматриваемом блоке для встраивания выбираются 4 самые высокочастотные ненулевые коэффициенты. Для каждого из них формируется группа низкочастотных коэффициентов, взятых в этом же блоке и в восьми соседних с ним. На основе значений коэффициентов групп вычисляются две характеристики: одна зависит от знака коэффициентов группы, а вторая – от их величины, после чего с учётом значений вычисленных характеристик выполняется встраивание методом НЗБ. Авторы отмечают, что алгоритм является стойким к JPEG при уровне сжатия выше заданного, а при любых других искажениях в частотной или пространственной области ЦВЗ разрушается. Недостатком системы [4] является сложная процедура выбора коэффициентов соседних блоков для расчёта характеристик.

Пример другой ЦВЗ-системы, в которой также используется НЗБ-встраивание, представлен в работе Huang, 2013 [5]. В отличии от [4], в [5] производится встраивание четырёх бит в низкочастотные коэффициенты, находящиеся в фиксированных позициях. При этом биты ЦВЗ рассчитываются на основе низкочастотных значений блоков контейнера. Данный алгоритм прост в реализации, однако, в силу этого может быть легко подвержен атакам.

Помимо НЗБ-встраивания, во многих полухрупких к JPEG системах встраивание выполняется при помощи метода QIM или его модификаций [3, 6-9].

Так, в Ye et al., 2003 [6] в процессе формирования ЦВЗ и для встраивания используются 4 отсчёта из числа первых 19-ти (в зигзагообразной развёртке) низкочастотных коэффициента (за исключением DC-отсчёта – коэффициента $D_i'(0,0)$). Встраивание осуществляется методом DC-QIM (Distortion-compensated QIM) [16].

Система, предложенная в работе Preda & Vizireanu, 2015 [7], согласно заявлению авторов, устойчива к сжатию JPEG с заданным значением параметра качества QF вплоть до $QF = 50$. ЦВЗ представляет собой значение хэш-функции, параметрами которой являются координаты блока и секретная последовательность. Количество встраиваемых бит на блок N_b является изменяемым параметром. Встраивание осуществляется вариацией метода QIM в первые p низкочастотных коэффициента блока (в зигзагообразной развёртке), кроме DC-отсчёта. Минусом [7] является значительное число параметров в сравнении с другими алгоритмами, в частности, значение N_b подбиралось авторами экспериментально на основании не вполне понятных принципов.

В работе Wang et al., 2011 [8] предложен полухрупкий к JPEG алгоритм, предназначенный для аутентификации изображения с возможностью восстановления искажённого содержимого (для этого встраиваются дополнительные биты информации). Встраивание производится при помощи модификации метода QIM, формула которого определена в [8]. Для аутентификации встраивание осуществляется в 6 случайно выбранных (при помощи секретного ключа) низкочастотных коэффициента (исключая DC-коэффициент). Для восстановления изображения дополнительно встраивается ещё 4 бита информации. Недостатком этого метода также, как и предыдущего, является большое число параметров по сравнению с другими методами, значения которых определяются эмпирически.

Особенностью системы, представленной в работе Fan et al., 2011 [9] является низкое минимально допустимое пороговое значение QF, равное 30. Алгоритм встраивания состоит из трёх основных этапов: поиск тех позиций для встраивания, что обеспечат наилучшую устойчивость к сжатию, определение наилучших значений для встраивания, которые не будут разрушены вследствие квантования, а также встраивание информации на основе QIM. На этапе поиска позиций производится JPEG-сжатие для всех возможных уровней сжатия QF (от 1 до 100). Для каждого квантованного блока каждого такого изображения рассчитывается число нулей в каждом отсчёте, затем эти значения складываются поэлементно. Наиболее подходящая позиция для встраивания в каждом блоке определяется как позиция, с наименьшим числом нулей. Таким образом, в каждый блок может быть встроен 1 бит информации в такую позицию. Однако не все такие позиции могут быть использованы, а лишь те, значение нулей в которых превышает некоторый заданный порог. По сравнению с другими алгоритмами, [9] обладает большей вычислительной сложностью. Другим недостатком системы является пропуск блоков, для которых не соблюдаются описанные выше условия.

Помимо НЗБ и QIM, используются также и другие методы изменения коэффициентов ДКП. В работе Fallahpour & Megias, 2016 [10] для этого производится смена чётности позиции последнего ненулевого элемента (Last Non-Zero Element, LNZ). В каждый блок, где значение LNZ-компоненты больше заданного порога, встраивается 1 бит информации. Ещё одним способом является встраивание информации на основе табличного отображения (Mapping Table). В работе Mursi et al., 2009 [11] таким методом изменяются значения первых 5 низкочастотных коэффициентов (после DC). В таблице номерам коэффициентов соответствует некоторая случайная последовательность из нулей и единиц. Встраивание происходит следующим образом: допустим, в некоторый коэффициент нужно встроить бит со значением «1», если в таблице ему соответствует «1», то его значение не изменяется, в противном случае его значение заменяется на значение ближайшего коэффициента, которому в таблице соответствует «1». К следующей группе можно отнести системы, в которых используется встраивание информации на основе расширения спектра (Spread Spectrum Watermarking) [12, 13]. Встраивание в этом методе производится путём внесения небольшой аддитивной или

мультипликативной шумоподобной последовательности в большое число коэффициентов. Для аутентификации выполняется поблочная корреляция модифицированных коэффициентов с заданной шумоподобной последовательностью. Высокое значение корреляции свидетельствует об аутентичности текущего блока. Подобные системы показывают хорошие результаты на однородных областях изображений, но их эффективность снижается на текстурированных фрагментах изображения. Кроме того, системы данного типа не позволяют регулировать допустимый уровень сжатия QF.

Сравнительные характеристики всех рассмотренных систем встраивания полухрупких ЦВЗ для JPEG-изображений представлены в таблице 1.

Таблица 1. Сравнительные характеристики систем встраивания ЦВЗ, полухрупких к JPEG (НЧ – низкие частоты, ВЧ – высокие частоты, СЧ – средние частоты).

Система	Метод изменения коэффициентов	Область частот	Число изменяемых коэффициентов	Минимальное значение QF, при котором сохраняется стойкость системы
Lin & Chang, 2000 [3]	НЗБ	НЧ	Переменное	≥ 50
Ho & Li, 2000 [4]	НЗБ	ВЧ	4	≥ 50
Huang, 2013 [5]	НЗБ	НЧ	4	
Ye et al., 2003 [6]	QIM	НЧ	4	
Preda & Vizireanu, 2015 [7]	QIM	НЧ	Зависит от QF	≥ 50
Wang et al., 2011 [8]	QIM	НЧ	До 10	
Fan et al., 2011 [9]	QIM	НЧ	≤ 1	≥ 30
Fallahpour & Megias, 2016 [10]	Изменение позиции LNZ-компоненты	ВЧ	1	
Mursi et al., 2009 [11]	Табличное отображение	НЧ	5	
Lin et al, 2000 [12]	Расширение спектра	НЧ и СЧ	35	Нет связи с QF
Al-Mualla, 2007 [13]	Расширение спектра	НЧ и СЧ	35	Нет связи с QF

4. Формальное описание базовых методов модификации частотных коэффициентов

Как следует из содержания раздела 3 и таблицы 1, подавляющее большинство систем рассматриваемого класса при изменении коэффициентов ДКП используют методы НЗБ или QIM. Рассмотрим эти методы более подробно.

Для простоты примем, что число изменяющихся при встраивании ЦВЗ коэффициентов ДКП равно числу бит N_W, встраиваемых в один блок, и при этом в системе встраивания ЦВЗ не производится анализ окрестных значений коэффициентов ДКП. Обозначим координаты модифицируемых коэффициентов $\left(m_1^k, m_2^k\right)$, где $k = 1..N_W$. Как правило, они выбираются на основе ключа. Тогда встраивание информации методом НЗБ будет осуществляться путём изменения квантованных коэффициентов:

$$D_i^W\left(m_1^k, m_2^k\right) = 2\left\lfloor \frac{D_i\left(m_1^k, m_2^k\right)}{2} \right\rfloor + W_{i,k}, \quad (2)$$

где $W_{i,k}$ – это k-ый бит информации, встраиваемой в i-ый блок. Коэффициенты, отличные от выбранных $\left(m_1^k, m_2^k\right)$, не претерпевают изменений. Способ извлечения встроенной информации W из D^W очевиден.

IM [16] представляет собой целое семейство методов, основанных на переквантовании компонент контейнера с использованием двух или более функций-квантователей, причём неопределённость выбора квантователя обеспечивает возможность встраивания скрытой

информации. Конкретный метод определяется видом используемых функций-квантователей. Одна из наиболее простых форм QIM используется в системе Preda & Vizireanu [7]. Будем далее обозначать данную форму QIM как Preda-QIM. Формулы встраивания и извлечения информации методом Preda-QIM имеют вид:

$$B_i^W\left(m_1^k, m_2^k\right) = round\left(\frac{B_i\left(m_1^k, m_2^k\right)}{2Q_{QF}\left(m_1^k, m_2^k\right)} - W_{i,k}\right) \cdot 2Q_{QF}\left(m_1^k, m_2^k\right) + W_{i,k} \cdot Q_{QF}\left(m_1^k, m_2^k\right), \quad (3)$$

$$W_{i,k} = round\left(\frac{B_i^W\left(m_1^k, m_2^k\right)}{Q_{QF}\left(m_1^k, m_2^k\right)}\right)(mod\ 2). \quad (4)$$

Сравнивая формулу (3) с последовательным применением (1) и (2), можно заметить, что отличия от метода НЗБ в данном случае несущественны. Как и в НЗБ, компоненты $B_i^W\left(m_1^k, m_2^k\right)$ кратны шагам квантования $Q_{QF}\left(m_1^k, m_2^k\right)$. Это делает метод уязвимым по отношению к атакам на основе анализа гистограмм. Меньшей уязвимостью за счёт более широкого диапазона возможных значений обладает метод встраивания, предложенный в статье Глумова и Митекина [18]. Система, рассматриваемая в данной работе, не предназначена для обеспечения стойкости к сжатию JPEG, поэтому встраивание осуществляется в пространственной области. Другим отличием от нашего случая является использование функции округления $\lfloor x \rfloor$ вместо $round(x)$. Собственно процедура изменения одной компоненты контейнера x при встраивании одного бита информации w реализуется по следующей формуле:

$$x^W = \left\lfloor \frac{x}{2\delta} \right\rfloor \cdot 2\delta + w \cdot \delta + x(mod\ \delta), \quad (5)$$

где δ – шаг квантования. Последнее слагаемое в формуле (5) как раз обеспечивает расширение диапазона значений x^W. Данный метод мы обозначим MOD-QIM.

Для использования данного метода в процедуре сжатия JPEG необходимо изменить функцию округления, сохраняя остаток. Это может быть сделано следующим образом:

$$x^W = \begin{cases} 2\delta \cdot round\left(\frac{x}{2\delta}\right) + w\delta + x(mod\ \delta), & x \geq 2\delta \cdot round\left(\frac{x}{2\delta}\right), \\ 2\delta \cdot round\left(\frac{x}{2\delta}\right) - w\delta - (-x)(mod\ \delta), & x < 2\delta \cdot round\left(\frac{x}{2\delta}\right). \end{cases} \quad (6)$$

Из формулы (6) легко получить выражение для встраивания ЦВЗ в коэффициенты ДКП, аналогично (3). Извлечение осуществляется по формуле (4).

В методе DM-QIM [16], одном из наиболее популярных представителей семейства QIM, защищённость к атакам на основе анализа гистограмм обеспечивается другим способом. Вместо прибавления остатка от деления на шаг квантования в этом методе из квантованного значения вычитается шумоподобная компонента, которая во избежание сдвига среднего значения предварительно прибавляется к компонентам контейнера:

$$B_i^W\left(m_1^k, m_2^k\right) = round\left(\frac{B_i\left(m_1^k, m_2^k\right) + d_{W_{i,k}}(k) \cdot Q_{QF}\left(m_1^k, m_2^k\right)}{2Q_{QF}\left(m_1^k, m_2^k\right)}\right) \cdot 2Q_{QF}\left(m_1^k, m_2^k\right) - d_{W_{i,k}}(k) \cdot Q_{QF}\left(m_1^k, m_2^k\right), \quad (7)$$

где $d_0(\mathrm{k}), d_1(\mathrm{k}) \in \mathbb{R} \cap [-1; 1)$ – два псевдослучайных массива, по которым модулируются биты встраиваемой информации в (7), причём $\mathrm{d}_1(\mathrm{k}) = \mathrm{d}_1(\mathrm{k}) - \mathrm{sign}\left(\mathrm{d}_1(\mathrm{k})\right)$.

5. Экспериментальные исследования

Как отмечалось в разделе 1, целью настоящей работы являлось исследование влияния количества модифицируемых коэффициентов ДКП, их позиций, а также метода встраивания информации на качество ЦВЗ-системы. Для достижения этой цели были проведены два эксперимента.

Первый эксперимент должен был дать ответ на вопрос о работоспособности рассмотренных методов как основы систем встраивания полухрупких ЦВЗ. В рамках этого эксперимента мы встраивали $N_W = 4$ бита информации в одни и те же коэффициенты ДКП (при этом использовались и низко-, и средне-, и высокочастотные коэффициенты). При встраивании

использовалось значение $QF = 50$. Далее полученное изображение сохранялось в формате JPEG с различными показателями качества QF^*, как меньшими, так и превышающими QF. После этого производилась попытка извлечения информации W^R из каждого из полученных изображений и оценивалась ошибка извлечения (Bit Error Rate) по формуле:

$$BER = \frac{1}{N \cdot N_W} \sum_{i=1}^{N} \sum_{k=1}^{N_W} XOR\left(W_{i,k}, W_{i,k}^R\right). \quad (8)$$

Результаты эксперимента, полученные усреднением по 10 изображениям из репозитория университета Ватерлоо [19], представлены на рисунке 3 и в таблице 2. В идеальном случае при $QF^* \geq QF$ значение $BER = 0$, а при меньших QF^* оно должно быть близким к 0,5, что соответствует случайному угадыванию. На практике неизбежно присутствует переходная фаза, когда график BER постепенно снижается с 0,5 до 0 (это наблюдается и для всех рассмотренных методов, согласно рисунку 3). Данная фаза должна быть как можно короче. Кроме того, могут встречаться и ненулевые значения BER при $QF^* \geq QF$, которые могут объясняться округлением значений пикселей после обратного ДКП, и как следствие, искажением спектральных компонент при извлечении информации.

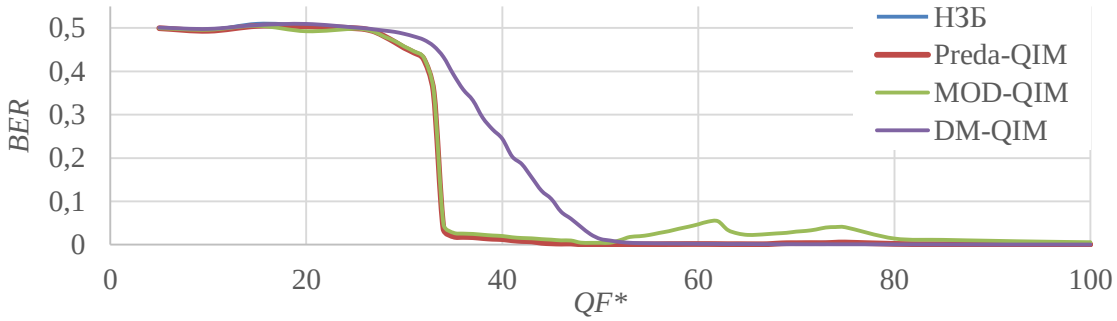

Рисунок 3. Схема кодирования изображения в формате JPEG.

Для оценки степени отклонения графиков от идеального случая – ступенчатой функции, по данным, представленным на рисунке 3, рассчитаны следующие показатели:

$$dist_{FN} = QF - \min_{BER(QF^*)<0.47} QF^*, \quad (9)$$

$$dist_{FP} = \max_{BER(QF^*)>0.005} QF^* - QF, \quad (10)$$

$$err_{FN} = \sum_{QF^*=QF-25}^{QF-1} \left(0.5 - BER(QF^*)\right), \quad (11)$$

$$err_{FP} = \sum_{QF^*=QF}^{QF+24} BER(QF^*). \quad (12)$$

Первые две величины характеризуют максимальные отклонения QF^* от QF, при которых BER превышает эмпирически определённые пороги. Величины (11), (12) характеризуют суммарные отклонения в значениях BER от их теоретического значения. Результаты расчёта показателей (9)-(12) представлены в таблице 2. Значения $dist_{FN}$ у всех методов примерно равны, но по показателю err_{FN} метод DM-QIM ведёт себя существенно лучше остальных. Ещё одно преимущество этого метода – наименьшее значение $dist_{FP}$, однако, с другой стороны, у DM-QIM самый высокий показатель err_{FP}. Различия в показателях между НЗБ и Preda-QIM минимальны, а MOD-QIM имеет большое число ошибок в области $QF^* \geq QF$.

Во втором эксперименте мы исследовали влияние числа встраиваемых бит и позиций модифицируемых коэффициентов ДКП на качество результирующего изображения (которое оценивалось по мере PSNR). Позиции коэффициентов определялись псевдослучайным образом исходя из заданного числа коэффициентов в соответствующей частотной области. Областью низких частот считались коэффициенты 2-14 в зигзагообразной развёртке, областью средних

частот – коэффициенты 15-35, остальные относились к высоким частотам. Как и ранее, использовалось значение $QF = 50$. Результаты представлены в таблице 3.

Таблица 2. Показатели отклонения значений BER от их теоретической оценки в серии экспериментов с JPEG-сжатием.

Метод	$dist_{FN}$	$dist_{FP}$	err_{FN}	err_{FP}
НЗБ	19,6	8,5	8,48	0,041
Preda-QIM	19,7	9	8,54	0,041
MOD-QIM	19,1	49,5	8,28	1,286
DM-QIM	18,3	4,7	5,44	0,066

Таблица 3. Показатель PSNR изображений со встроенным ЦВЗ при различных параметрах.

N_W, число бит на блок	Число изменяемых коэффициентов по частотным зонам (НЧ-СЧ-ВЧ)	PSNR			
		НЗБ	Preda-QIM	MOD-QIM	DM-QIM
1	1-0-0	43,95	42,92	44.74	47,03
1	0-1-0	33,85	33,74	33.97	37,72
1	0-0-1	28,93	28,94	28.96	31,67
2	2-0-0	41,55	40,.55	42.17	44,12
2	0-2-0	31,84	31,70	31.98	34,68
2	0-0-2	26,42	26,43	26.45	28,76
4	4-0-0	38,85	37,87	39.42	41,15
4	0-4-0	29,32	29,18	29.50	31,71
4	0-0-4	23,68	23,68	23.72	25,75
4	1-1-2	25,64	25,62	25.70	28,13
10	10-0-0	34,90	33,93	35.45	37,22
10	0-10-0	25,78	25,62	25.97	27,70
10	0-0-10	20,04	20,03	20.09	21,80
10	2-3-5	22,12	22,08	22,55	24,15
10	3-3-4	22,85	22,80	22.19	24,88
10	2-4-4	22,68	22,62	22.76	24,73
10	1-3-6	21,49	21,46	21.56	23,50
Среднее		**29,05**	**28,77**	**29.27**	**31,45**

Данные, представленные в таблице, показывают, что методы НЗБ и Preda-QIM достаточно близки по качеству результирующих изображений (причём НЗБ немного выигрывает), MOD-QIM по качеству превосходит эти методы, а наилучшим образом себя показал DM-QIM. Анализ различных конфигураций изменяемых коэффициентов ДКП по частотным зонам показал, что предпочтительным является встраивание информации в низкочастотные компоненты. Так, даже при встраивании 10 бит в НЧ-коэффициенты методом DM-QIM качество результирующего изображения оказывается выше, нежели при встраивании 1 бита в ВЧ-коэффициенты любым из четырёх методов.

6. Заключение

В работе проведено сравнительное исследование различных методов встраивания полухрупких цифровых водяных знаков, обладающих стойкостью к JPEG-сжатию в ограниченном диапазоне показателей компрессии. В эксперименте сравнивались следующие методы модификации информации: НЗБ; упрощённая версия QIM, использованная в статье [7] (Preda-QIM), версия QIM с добавлением остатка (MOD-QIM) на основе метода [18], а также DM-QIM [16]. Проверка работоспособности показала, что все рассмотренные методы могут использоваться для создания полухрупких ЦВЗ. Исследование качества формируемых в результате встраивания

ЦВЗ изображений показало преимущество метода DM-QIM. Кроме того, показано, что для снижения визуальных искажений, встраивание ЦВЗ, вне зависимости от метода, должно осуществляться в низкочастотные коэффициенты ДКП.

7. Литература

[1] Cox, I. Digital Watermarking and Steganography: Morgan Kaufmann / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker // Elsevier, 2008. – 624 p.
[2] Lin, C.-Y. Issues and solutions for authenticating MPEG video / C.-Y. Lin, S.-F. Chang // Proceedings of SPIE. – 1999. – P. 54-65. DOI: 10.1117/12.344703.
[3] Lin, C.-Y. Semifragile watermarking for authenticating JPEG visual content / C.-Y. Lin, S.-F. Chang. – 2000. – P. 140-151. DOI: 10.1117/12.384968.
[4] Ho, Ch.K. Semi-fragile watermarking scheme for authentication of JPEG images / Ch.K. Ho, Ch.-T. Li // Proceedings International Conference on Information Technology: Coding and Computing. – 2004. – Vol. 1. – P. 7-11. DOI: 10.1109/ITCC.2004.1286417.
[5] Huang, L.-Y. Authentication watermarking algorithm resisting JPEG compression based on preliminary quantization / L.-Y. Huang // Information Technology Journal. – 2013. – Vol. 12(16). – P. 3723-3728. DOI: 10.3923/itj.2013.3723.3728.
[6] Ye, S. A quantization-based image authentication system / S. Ye, Z. Zhou, Q. Sun, E. Chang, Q. Tian // Fourth International Conference on Information, Communications and Signal Processing, and the Fourth Pacific Rim Conference on Multimedia. – 2003. – Vol. 2. – P. 955-959. DOI: 10.1109/ICICS.2003.1292599.
[7] Preda, R.O. Watermarking-based image authentication robust to JPEG compression / R.O. Preda, D.N. Vizireanu // Electronics Letters. – 2015. – Vol. 51(23). – P. 1873-1875. DOI: 10.1049/el.2015.2522.
[8] Wang, H. A Novel Fast Self-restoration Semi-fragile Watermarking Algorithm for Image Content Authentication Resistant to JPEG Compression / H. Wang, A. Ho, X. Zhao. – 2011. – P. 72-85. DOI: 10.1007/978-3-642-32205-1_8.
[9] Fan, C.-H. A Robust Watermarking Technique Resistant JPEG Compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // J. Inf. Sci. Eng. – 2011. – Vol. 27. – P. 163-180.
[10] Fallahpour, M. Flexible image watermarking in JPEG domain / M. Fallahpour, D. Megias // IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). – 2016. – P. 311-316. DOI: 10.1109/ISSPIT.2016.7886055.
[11] Mursi, M. A DCT-based secure JPEG image authentication scheme / M. Mursi, G.M.R. Assassa, H. Aboalsamh, K. Alghathbar // World Academy of Science, Engineering and Technology. – 2009. – Vol. 53. – P. 681-687.
[12] Lin, E.T. Detection of image alterations using semifragile watermarks / E.T. Lin, C.I. Podilchuk, E.J. Delp // Security and Watermarking of Multimedia Contents. – 2000. – Vol. 3971. – P. 152-164. DOI: 10.1117/12.384969.
[13] Al-Mualla, M.E. Content-Adaptive Semi-Fragile Watermarking for Image Authentication / M.E. Al-Mualla // 14th IEEE International Conference on Electronics, Circuits and Systems. – 2007. – P. 1256-1259. DOI: 10.1109/ICECS.2007.4511225.
[14] Wong, P.H.W. Data hiding technique in JPEG compressed domain / P.H.W. Wong, O.C.L. Au, J.W.C. Wong. – 2001. – P. 309-320. DOI: 10.1117/12.435412.
[15] Xiao, J. A semi-fragile watermarking distinguishing JPEG compression and gray-scale-transformation from malicious manipulation / J. Xiao, Z. Ma, B. Lin, J. Su, Y. Wang // IEEE Youth Conference on Information, Computing and Telecommunications. – 2010. – P. 202-205. DOI: 10.1109/YCICT.2010.5713080.
[16] Chen, B. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding / B. Chen, G. Wornell // IEEE Transaction on Information Theory. – 2001. – Vol. 47(4). – P. 21.
[17] Wallace, G.K. The JPEG still picture compression standard / G.K. Wallace // IEEE Transactions on Consumer Electronics. – 1992. – Vol. 38(1). – P. XVIII–XXXIV. DOI: 10.1109/30.125072.

[18] Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – Т. 35. – С. 262-267.
[19] Image Repository. The Waterloo Fractal Coding and Analysis Group [Electronic resource]. – Access mode: http://links.uwaterloo.ca/Repository.html (20.10.2018).

Благодарности
Исследование выполнено за счет гранта Российского научного фонда (проект № 18-71-00052).

Comparative evaluation of semi-fragile JPEG watermarking methods

A.A. Egorova[1,2], V.A. Fedoseev[1,2]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086
[2]Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. One of the ways to protect images from tampering is embedding a digital watermark – additional information destroyed by unauthorized changes. The development of digital watermark embedding methods that are robust against allowable transformations the most typical example of which is lossy compression presents a challenging task. Such methods and watermarks embedded by them are called semi-fragile. The paper considers different semi-fragile watermarking techniques that resisting JPEG. Of particular interest is analyzing how watermark capacity, positions of spectral coefficients selected for embedding and specific algorithms of coefficients modification affect the quality of the resulting (secure) image. This study provides the best combinations of these parameters depending on the terms of use of a protected image.