УЛУЧШЕННЫЙ АЛГОРИТМ ВСТРАИВАНИЯ ИНФОРМАЦИИ В СЖАТЫЕ ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ НА ОСНОВЕ МЕТОДА PM1

О.О. Евсютин, А.С. Кокурина, А.А. Шелупанов, И.И. Шепелев
Томский государственный университет систем управления и радиоэлектроники, Томск, Россия

Аннотация

В статье предлагается и исследуется новый алгоритм встраивания информации в JPEG-изображения, основанный на известном стеганографическом методе «плюс/минус один». Показывается, что при частичном заполнении стегоконтейнера предложенный алгоритм превосходит аналоги за счёт оригинального подхода к определению порядка обхода ДКП-коэффициентов при встраивании в них битов сообщения. В качестве метрики качества используется пиковое отношение сигнал/шум.

Ключевые слова: защита информации, стеганография, встраивание информации, цифровые изображения, JPEG.

Цитирование: **Евсютин, О.О.** Улучшенный алгоритм встраивания информации в сжатые цифровые изображения на основе метода PM1 / О.О. Евсютин, А.С. Кокурина, А.А. Шелупанов, И.И. Шепелев // Компьютерная оптика. – 2015. – Т. 39, № 4. – С. 572-581. – DOI: 10.18287/0134-2452-2015-39-4-572-581.

Введение

Известно множество методов стеганографического встраивания данных в цифровые изображения с целью решения различных задач обеспечения информационной безопасности [1].

Наибольшую практическую ценность представляют методы и алгоритмы, работающие со сжатыми изображениями, так как в сети Интернет, а также в локальных компьютерных сетях цифровые изображения хранятся и передаются прежде всего в сжатом виде. При этом наиболее популярным стандартом сжатия был и остаётся JPEG, построенный на основе дискретного косинусного преобразования (ДКП) [2].

Большинство известных методов стеганографического встраивания данных в сжатые JPEG-изображения оперирует квантованными коэффициентами ДКП (рис. 1), поскольку на этапе статистического кодирования, следующем за этапом квантования, отсутствуют потери информации, которые могли бы привести к повреждению встраиваемого сообщения.

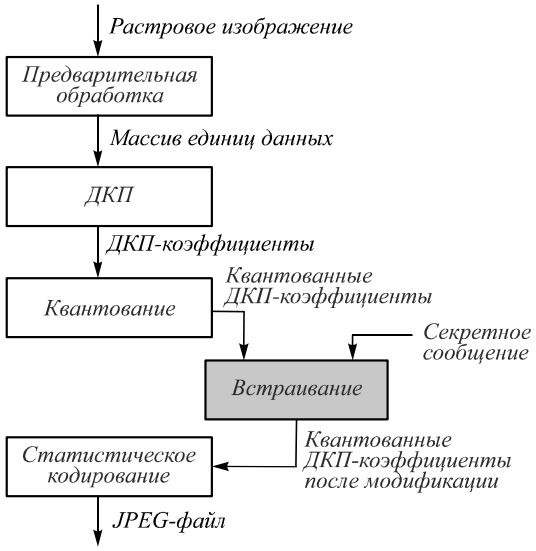


Рис. 1. Схема встраивания дополнительной информации в процессе сжатия цифрового изображения по методу JPEG

Можно выделить два основных подхода к встраиванию частей секретного сообщения в квантованные ДКП-коэффициенты JPEG-изображения (далее просто коэффициенты).

1. Непосредственное встраивание битов в выбранные коэффициенты.
2. Изменение групп выбранных коэффициентов таким образом, чтобы они удовлетворяли определённым соотношениям в зависимости от встраиваемых битов.

Стегосистемы, реализующие первый подход, в наибольшей степени пригодны для передачи больших объёмов секретной информации, однако отличаются слабой робастностью по отношению к искажающим воздействиям на изображения-стегоконтейнеры. При этом данный подход является достаточно гибким, поскольку позволяет управлять соотношением ёмкость/незаметность встраивания за счёт выбора того или иного количества коэффициентов для записи в них битов сообщения.

Под повышением незаметности встраивания подразумевается минимизация дополнительных потерь качества JPEG-изображения. Данные понятия: незаметность стеганографического встраивания и качество изображения-стегоконтейнера – будем считать эквивалентными. Оценка искажений цифровых изображений, содержащих вложения, относительно исходных изображений обычно производится с помощью стандартной метрики качества PSNR [2].

Второй из данных подходов применяется главным образом для встраивания цифровых водяных знаков (ЦВЗ). Соответствующие методы являются робастными за счёт значительного уменьшения ёмкости стегоконтейнеров по сравнению с первым подходом. Однако здесь необходимо отметить, что ЦВЗ допустимо извлекать с искажениями, поэтому наличие свойства робастности не подразумевает возможность точного восстановления таких стеговложений.

Далее будут рассмотрены основные алгоритмы стеганографического встраивания информации в

квантованные ДКП-коэффициенты сжатых цифровых изображений, представленные в литературе.

1. Обзор методов и алгоритмов встраивания информации в сжатые JPEG-изображения

Непосредственное встраивание в квантованные ДКП-коэффициенты

При непосредственном встраивании информации в квантованные ДКП-коэффициенты, составляющие пространство сокрытия, они складываются с некоторыми целочисленными значениями, либо изменения вносятся в наименее значащие биты.

Под пространством сокрытия понимается часть элементов данных цифрового изображения, непосредственно используемых для записи сообщения. Многие исследователи в своих работах основное внимание уделяют способам формирования пространства сокрытия из квантованных ДКП-коэффициентов, так чтобы для сообщения данной длины можно было обеспечить наилучшее качество изображения-стегоконтейнера.

Значительную ёмкость встраивания в частотной области ДКП позволяет обеспечить метод «плюс/минус один» (метод PM1) [3, 4], который будет подробно рассмотрен в следующем разделе настоящей статьи. Для записи битов сообщения используются все коэффициенты со значениями, отличными от нуля, и встраивание заключается в изменении их значений на единицу в большую или меньшую сторону, то есть является легко разрушаемым. Однако за счёт такого малого изменения незаметность встраивания сохраняется даже при максимальном заполнении стегоконтейнера.

Поэтому PM1 целесообразно использовать в тех приложениях, которые требует высокой ёмкости встраивания и позволяют пренебречь робастностью.

Алгоритм, подобный PM1, описан в [5]. В данной работе для записи битов используются только коэффициенты, равные по модулю заранее заданной величине L. В зависимости от встраиваемого бита коэффициент либо остаётся без изменений, либо увеличивается по модулю на единицу. При этом все прочие коэффициенты, не включённые в пространство сокрытия, также увеличиваются по модулю на единицу, чтобы при извлечении сообщения не возникло неоднозначности. Таким образом, при сравнимом качестве встраивания данный алгоритм обладает существенно меньшей ёмкостью по сравнению с PM1.

В алгоритмах, представленных в [6, 7], пространство сокрытия формируется из коэффициентов, принадлежащих множеству $\{-T, ..., 0, \ldots, T\}$. Выбор конкретных коэффициентов для записи в них битов сообщения осуществляется с помощью вводимых в данных работах функций, учитывающих влияние изменения отдельно взятых коэффициентов на вносимые в изображение искажения. Данные алгоритмы сравнимы с PM1 по качеству встраивания при равной ёмкости, но требуют бо́льших вычислительных затрат на формирование пространства сокрытия.

В [8 – 10] встраивание основано на модификации таблиц квантования, которая заключается в том, что значения элементов данных таблиц в области средних частот ДКП уменьшаются. В результате потери информации при квантовании соответствующих ДКП-коэффициентов становятся минимальны, и эти коэффициенты образуют пространство сокрытия.

В [8, 9] для встраивания секретного сообщения используются два наименее значащих бита выбранных частотных коэффициентов. В [10] сообщение представляется в виде последовательности цифр системы счисления по модулю k, каждая из которых аддитивно встраивается в один коэффициент.

Однако если в [10] размер таблицы квантования является стандартным, то в [8, 9] использованы увеличенные таблицы квантования размером 16×16 и 32×32, получаемые из стандартных с помощью интерполяции. В отмеченных работах указывается, что это позволяет повысить качество изображений, однако из-за изменённых размеров блоков теряется совместимость со стандартными кодеками JPEG.

Кроме того, вследствие уменьшения потерь информации на этапе квантования увеличивается размер сжатого файла.

Алгоритм встраивания, описанный в [11], основан на методе QIM [12, 13], который вместо значений пикселей применяется к квантованным ДКП-коэффициентам. Пространство сокрытия формируется из коэффициентов низкочастотной области.

Таким образом, можно увидеть, что в большинстве своём стеганографические методы непосредственного встраивания информации в квантованные ДКП-коэффициенты основаны на аналогичных методах встраивания информации в пространственную область цифровых изображений.

Изменение соотношений между квантованными ДКП-коэффициентами

Как было отмечено ранее, встраивание информации в квантованные ДКП-коэффициенты за счёт изменения соотношений между ними чаще всего применяется в алгоритмах встраивания ЦВЗ, служащих для аутентификации цифровых изображений.

Отдельно отметим, что в случае встраивания ЦВЗ практической ценностью обладают не только методы и алгоритмы, работающие со сжатыми изображениями, но также и методы, работающие с цифровыми изображениями без сжатия и реализующие встраивание в пространственную область. При этом в качестве одного из возможных искажающих воздействий на стегоконтейнер рассматривается JPEG-сжатие. Примеры подобных алгоритмов представлены в [14, 15].

В [16, 17] представлен метод, согласно которому в каждый блок квантованных ДКП-коэффициентов JPEG-изображения встраивается один бит ЦВЗ. Для этого выбирается пара коэффициентов из области средних частот ДКП и в зависимости от значения встраиваемого бита они изменяются таким образом, чтобы модуль их разности был больше либо меньше некоторого числа D, составляющего вместе с номерами коэффициентов сте-

ганографический ключ. В другом варианте выбирается три коэффициента, и аналогичные соотношения устанавливаются для двух пар значений.

Можно увидеть, что размер пространства сокрытия в данном случае фиксирован и зависит только от размера изображения, но не от степени сжатия.

При этом изменения, которые описанный метод вносит в частотные коэффициенты, являются более значимыми по сравнению с методами, рассмотренными в предыдущем разделе, поэтому установленные между коэффициентами соотношения удаётся сохранить даже при некоторых модификациях цифрового изображения-стегоконтейнера.

Однако робастность достигается в ущерб ёмкости, поэтому данный метод и большинство его аналогов затруднительно использовать для передачи больших объёмов конфиденциальной информации.

Алгоритм на основе описанного метода, представленный в [18], использует пространство сокрытия переменного размера. Из него исключаются блоки ДКП-коэффициентов, соответствующие блокам пикселей с однотонным заполнением или, наоборот, с резкими перепадами, вследствие чего по сравнению с базовым алгоритмом ёмкость становится меньше.

В [19] ёмкость, наоборот, выше за счёт того, что в пару коэффициентов встраивается два бита секретного сообщения. Сначала встраивается первый бит, в зависимости от его значения между величинами коэффициентов устанавливается соотношение «больше–меньше». В зависимости от значения второго встраиваемого бита данные коэффициенты изменяются таким образом, чтобы их среднее арифметическое приняло определённый знак.

Рассмотренные методы обеспечивают робастность стеговложений за счёт внесения существенных изменений в малое число квантованных ДКП-коэффициентов. В [20] для этой цели используется избыточное встраивание: в разные области пространства сокрытия встраиваются специальные коды, выработанные рекуррентным образом из единственного сообщения. Пространство сокрытия формируется из коэффициентов со значениями 0, ±1.

В том случае, когда рассматриваемый подход используется для встраивания произвольных сообщений, а не ЦВЗ, это требует бо́льшей ёмкости, что, в свою очередь, достигается за счёт использования менее робастных операций.

Так, например, в [21, 22] представлен метод, основанный на изменении гистограмм значений среднечастотных коэффициентов, строящихся по отдельности для каждого блока. Для этого величины столбцов гистограмм изменяются в зависимости от встраиваемых битовых последовательностей. При этом встраиваемые биты кодируются не только значениями коэффициентов, но и взаимным порядком их расположения.

Это даёт существенно бо́льшую ёмкость по сравнению с методами из [14, 15]. Но при этом искажения стегоконтейнеров также намного более существенны, поскольку разница между коэффициентами, модифицированными при изменении гистограмм, и их исходными значениями может достигать нескольких единиц. Это негативным образом сказывается на качестве встраивания, но в то же время не обеспечивает должной робастности.

Таким образом, подытоживая настоящий обзор, отметим, что для задач передачи конфиденциальной информации в цифровых изображениях при отсутствии требований к робастности хорошо подходит метод PM1. И определим основную цель настоящей работы следующим образом: получение эффективной алгоритмической реализации стеганографического метода встраивания конфиденциальной информации в сжатые цифровые изображения PM1.

Критерием эффективности будем считать повышение незаметности встраивания при сравнимой ёмкости стегоконтейнера.

2. Метод «плюс/минус один»

При встраивании информации в JPEG-изображения по методу PM1 для формирования пространства сокрытия используют ненулевые квантованные AC-коэффициенты всех составляющих модели YCbCr [3, 4]. Для данного изображения их количество зависит от степени сжатия. Пример соответствующей зависимости показан на рис. 2 для изображения «Lenna» разрешением 256×256.

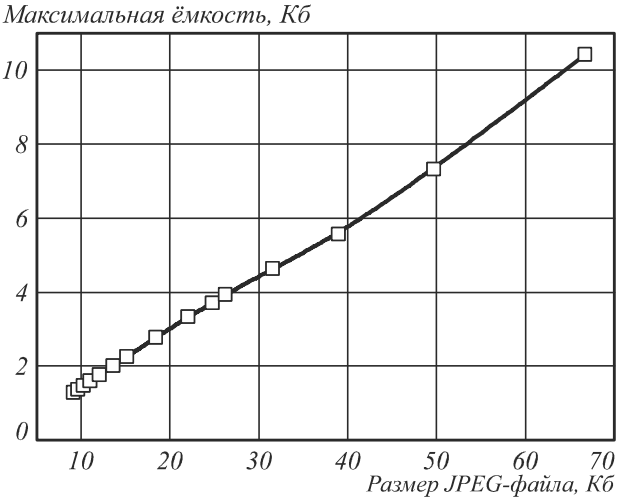


Рис. 2. Зависимость ёмкости JPEG-изображения от степени сжатия

Обозначим секретное сообщение и пространство сокрытия $M=m_1m_2\ldots m_L$ и $C=c_1c_2\ldots c_L$ соответственно, где $m_i\in\{0,1\}$, $0\neq c_i\in Z$, Z – множество целых чисел, $i=\overline{1,L}$. В простейшей алгоритмической реализации рассматриваемого метода пространство сокрытия формируется из первых L ненулевых AC-коэффициентов изображения при обходе его в некотором порядке.

Встраивание бита сообщения m_i в элемент пространства сокрытия c_i осуществляется по нижеприведённым формулам, где c_i' обозначает изменённое значение ДКП-коэффициента.

Если $m_i = 0$, то

$$c_i' \leftarrow \begin{cases} c_i, \text{ если } c_i < 0 \text{ и } c_i \equiv 1 \bmod 2, \\ c_i, \text{ если } c_i > 0 \text{ и } c_i \equiv 0 \bmod 2, \\ c_i + (-1)^r, \text{ в противном случае,} \end{cases} \quad (1)$$

если $m_i = 1$, то

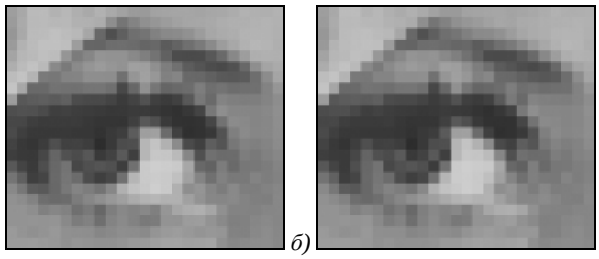
$$c_i' \leftarrow \begin{cases} c_i, \text{ если } c_i < 0 \text{ и } c_i \equiv 0 \bmod 2, \\ c_i, \text{ если } c_i > 0 \text{ и } c_i \equiv 1 \bmod 2, \\ c_i + (-1)^r, \text{ в противном случае,} \end{cases} \quad (2)$$

где $r \in \{0,1\}$ генерируется случайным образом, однако принимается равным нулю, если $c_i = 1$, и равным единице, если $c_i = -1$.

Таким образом, встраивание по методу PM1 основывается на изменении чётности ненулевых AC-коэффициентов JPEG-изображения, и извлечение сообщения тривиально.

Соответствующий алгоритм для краткости будем называть алгоритмом PM1 или базовым алгоритмом. Как было отмечено ранее, он позволяет обеспечить достаточно высокое качество встраивания даже при максимальном заполнении стегоконтейнера.

На рис. 3 представлен увеличенный фрагмент изображения «Lenna» до и после встраивания сообщения максимально возможной длины.



а) *б)*

Рис. 3. Артефакты встраивания алгоритма PM1 на примере изображения «Lenna»: фрагмент изображения до встраивания (а); фрагмент изображения после встраивания (б)

Визуальная оценка показывает отсутствие заметных артефактов встраивания.

Помимо высоких показателей ёмкости и качества стегоконтейнеров, достоинством базового алгоритма PM1 является также и то, что он не требует передачи пользователю каких-либо параметров встраивания.

Однако, несмотря на отмеченные достоинства рассматриваемого стеганографического метода, он обладает хорошими возможностями для улучшения.

3. Улучшение метода «плюс/минус один» на основе генетического алгоритма

В статье [3] описан алгоритм J-PM1, представляющий собой улучшенный алгоритм встраивания на основе метода PM1. Улучшение достигается за счёт управления процессом встраивания с помощью генетического алгоритма. Авторы данной работы отмечают следующий факт: существует два способа изменения отдельно взятого элемента пространства сокрытия при встраивании в него бита сообщения, и каждый такой выбор оказывает влияние на результирующие искажения цифрового изображения.

В формулах (1) и (2) способ изменения коэффициента c_i определяется значением r и, таким образом, может быть кодирован одним битом. В свою очередь, каждая из хромосом, которыми оперирует генетический алгоритм, кодирует способ встраивания всех битов сообщения в частотную область цифрового изображения, представляя собой двоичный вектор той же длины.

Кроме этого, в данной работе вводится секретный ключ, служащий для развёртывания подстановки, с помощью которой AC-коэффициенты перемешиваются перед началом встраивания. Использование подстановки позволяет распределить биты сообщения по всем блокам изображения и избежать ситуации, когда сообщение малой длины встраивается в локальную область цифрового изображения, что впоследствии может быть выявлено с помощью визуального или статистического анализа. Однако наличие секретного ключа требует обеспечить его безопасное хранение и передачу получателю стегоконтейнера, что связано с определёнными неудобствами.

Исследование описанного в работе [3] алгоритма позволило выявить следующие его особенности.

Использование генетического алгоритма требует значительных временных затрат, поскольку оценка приспособленности каждой хромосомы на каждой итерации работы алгоритма заключается в расчёте метрики качества стегоконтейнера, заполненного в соответствии с определяемым хромосомой способом встраивания сообщения.

Главным же недостатком алгоритма J-PM1 является незначительность улучшения по отношению к алгоритму PM1.

В табл. 1 представлены данные, отражающие зависимость величины PSNR между исходным изображением и изображением, содержащим встроенное сообщение, от длины сообщения (размера пространства сокрытия) для алгоритмов PM1 и J-PM1. Длина сообщения выражена в процентном отношении от общего количества ненулевых AC-коэффициентов изображения.

Табл. 1. Зависимость величины искажений изображения от длины сообщения для алгоритмов PM1 и J-PM1

Уровень заполнения стегоконтейнера, %	PSNR, Дб	
	PM1	J-PM1
5	58,45	58,80
10	55,58	55,68
20	52,57	52,76
30	50,46	50,59
40	49,63	49,79
50	48,09	48,27
60	47,90	48,08
70	46,85	47,02
80	46,67	46,82
90	46,16	46,31
100	45,78	45,90

Приведённые значения были получены путём усреднения по выборке из 16 тестовых JPEG-

изображений разрешением 256×256 пикселей с уровнем качества 100 %: «Airplane», «Baboon», «Barbara», «Boats», «Cablecar», «Cornfield», «Fruits», «Flower», «Goldhill», «Lenna», «Monarch», «Pens», «Peppers», «Soccer», «Tiffany», «Yacht» [23].

Максимальная ёмкость выбранных стегоконтейнеров в среднем составила 10 Кб.

Встраиваемые сообщения представляли собой тексты на русском языке, сжатые с помощью программы-архиватора.

Значение PSNR рассчитывалось между изображением, восстановленным из исходного JPEG-файла, и изображением, восстановленным из JPEG-файла, содержащего вложение.

Можно увидеть, по качеству встраивания J-PM1 ненамного превосходит PM1. Достигаемое улучшение составляет не более 0,35 Дб, что нельзя считать существенным.

4. Предлагаемый алгоритм

В рамках данной работы было проведено исследование, позволившее получить более эффективный алгоритм встраивания на основе метода «плюс/минус один» по сравнению с базовым алгоритмом и алгоритмом J-PM1.

Встраивание информации в частотную область ДКП в общем случае обладает следующими свойствами:

1. Внесение изменений в среднечастотные и высокочастотные коэффициенты блока ДКП приводит к меньшим искажениям соответствующего блока цифрового изображения по сравнению с изменением низкочастотных коэффициентов.
2. Внесение изменений в блок ДКП, содержащий большее количество ненулевых коэффициентов, приводит к меньшим искажениям соответствующего блока цифрового изображения по сравнению с изменением блока ДКП с меньшим количеством ненулевых коэффициентов.

На рис. 4 показано, как меняется величина PSNR при выборе различных групп частотных коэффициентов для формирования пространства сокрытия. Данный график также получен путём усреднения по всей выборке тестовых изображений.

В рамках соответствующего эксперимента 63 АС-коэффициента каждого блока ДКП c_i, $i=\overline{2,64}$, были разделены на 32 частотные области следующим образом: $\Omega_1=\{c_2,c_3\}$, $\Omega_2=\{c_4,c_5\}$, ..., $\Omega_{31}=\{c_{62},c_{63}\}$, $\Omega_{32}=\{c_{63},c_{64}\}$. Приведённая нумерация коэффициентов соответствует зигзагообразному обходу блока ДКП, определённому в стандарте JPEG.

Встраивание сообщения фиксированного размера 0,1 Кб осуществлялось с помощью базового алгоритма PM1.

К наибольшим искажениям приводит встраивание сообщения в элементы низкочастотных областей Ω_1, Ω_2, Ω_3. Характеристики изменения величины PSNR при встраивании в другие частотные области в значительной степени зависят от изображения-стегоконтейнера. Однако если рассмотреть приведённый на рис. 4 график относительно среднего значения, то можно увидеть, что величина PSNR для областей $\Omega_4-\Omega_{15}$ в основном находится ниже среднего значения, для $\Omega_{16}-\Omega_{20}$ – колеблется в районе среднего значения и для $\Omega_{21}-\Omega_{32}$ – в основном находится выше среднего значения.

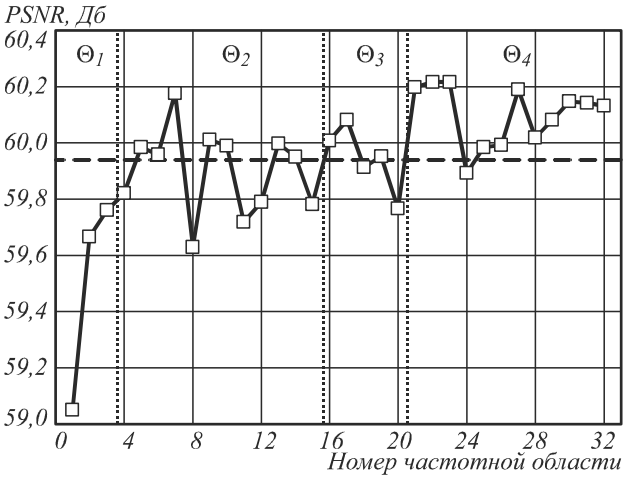


Рис. 4. Зависимость величины искажений изображения от выбора частотной области

Отмеченное поведение характерно как для представленного усреднённого графика, так и для графиков, получаемых для тестовых изображений по отдельности. Поэтому, исходя из этого эмпирического наблюдения, первичные частотные области малого размера Ω_i, $i=\overline{1,32}$, объединим в четыре укрупнённые частотные области: $\Theta_1=\{c_2,c_3,\ldots,c_6,c_7\}$, $\Theta_2=\{c_8,c_9,\ldots,c_{30},c_{31}\}$, $\Theta_3=\{c_{32},c_{33},\ldots,c_{40},c_{41}\}$, $\Theta_4=\{c_{42},c_{43},\ldots,c_{63},c_{64}\}$. Здесь области Θ_1, Θ_2 и Θ_4 естественным образом ассоциируются с низкими, средними и высокими частотами соответственно, а область Θ_3, в которую вошло меньше всего ДКП-коэффициентов, можно считать переходной между средними и высокими частотами.

Для уменьшения искажений область Θ_1 при встраивании предпочтительнее просматривать в обратном порядке, для прочих областей порядок обхода является менее значимым.

Второе из указанных свойств ДКП связано с тем, что наличие малого количества ненулевых коэффициентов (после квантования) в частотном спектре характерно для визуально однородных блоков изображения, не содержащих мелких деталей. На блоках подобного типа наиболее явно, как визуально, так и численно, могут проявляться искажения, вызванные встраиванием дополнительной информации.

При этом из двух блоков ДКП с равным количеством ненулевых коэффициентов для встраивания предпочтительнее использовать тот, в котором преобладают коэффициенты из областей Θ_3 и Θ_4.

На рис. 5 представлены примеры блоков изображения «Lenna», которым соответствуют блоки ДКП с разным количеством ненулевых коэффициентов.

В табл. 2 приведены результаты встраивания сообщения фиксированного размера 1 байт в выбранные блоки с помощью алгоритма J-PM1. В данном случае оптимизация была использована, чтобы исключить влияние способа модификации коэффициентов при записи в них битов сообщения на итоговую величину искажений.

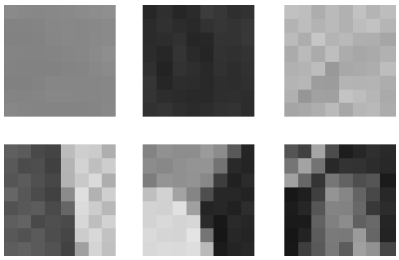


Рис. 5. Примеры укрупнённых блоков пикселей различного типа

Табл. 2. Оценка искажений при встраивании информации в блоки цифрового изображения различного типа

№ блока	Количество ненулевых ДКП-коэффициентов	PSNR, Дб
1	11	48,48
2	20	48,56
3	30	49,12
4	40	51,93
5	52	54,43
6	57	55,52

Нумерация блоков в таблице соответствует их обходу слева направо и сверху вниз.

Таким образом, при частичном заполнении стегоконтейнера управлять качеством встраивания можно за счёт выбора для записи битов секретного сообщения определённых АС-коэффициентов.

Псевдослучайный порядок обхода коэффициентов, реализованный в алгоритме J-PM1, позволяет распределить элементы секретного сообщения по всему изображению, однако не учитывает вышеописанные свойства дискретного косинусного преобразования.

Далее порядок обхода АС-коэффициентов при формировании из них пространства сокрытия будем называть стегопутём [1] и процесс встраивания информации в цифровое изображение определим состоящим из следующих двух этапов.

Этап 1. Построение стегопути.

Этап 2. Встраивание сообщения.

Предлагаемый алгоритм встраивания в изображение секретного сообщения на основе метода PM1 представлен ниже. Данный алгоритм сформулирован в предположении, что размер изображения достаточен для сокрытия в нём сообщения заданной длины.

Предварительно введём некоторые обозначения.

B_i – i-й блок квантованных ДКП-коэффициентов сжатого JPEG-изображения, $i=\overline{1,K}$, и K – значение, зависящее от установленных при сжатии параметров субдискретизации [2].

$c_j^{(i)}$ – j-й АС-коэффициент блока B_i, $i=\overline{1,K}$, $j=\overline{2,64}$.

$$V_i=\sum_{j=2}^{64}h_j^{(i)},\ \text{где}\ h_j^{(i)}=\begin{cases}1, & \text{если } c_j^{(i)}\neq 0,\\ 0, & \text{если } c_j^{(i)}=0.\end{cases}$$

$W_i=\sum_{j=2}^{64}h_j^{(i)}g_j$ – «частотный» вес блока B_i, где

$$g_j=\begin{cases}0, & \text{если } 2\le j\le 7,\\ 1, & \text{если } 8\le j\le 31,\\ 2, & \text{если } 32\le j\le 41,\\ 3, & \text{если } 42\le j\le 64.\end{cases}$$

Вход:

сообщение $M=m_1m_2\ldots m_L$, $m_y\in\{0,1\}$, $y=\overline{1,L}$; пустой стегоконтейнер – цифровое изображение разрешением $M\times N$ пикселей, сжатое по методу JPEG.

Выход:

заполненный стегоконтейнер.

Шаг 1. Восстановить из JPEG-файла блоки квантованных ДКП-коэффициентов для трёх компонент цветового пространства YCbCr.

Шаг 2. $\forall\, i=\overline{1,K}$ рассчитать значения V_i и W_i.

Шаг 3. Создать вектор $\mathbf{S}=(s_i)_{i=1}^{K}$ и $\forall\, i=\overline{1,K}$ присвоить $s_i\leftarrow i$.

Шаг 4. Осуществить перестановку значений вектора **S** таким образом, чтобы выполнялось следующее условие: $\forall\, p,q=\overline{1,K}$, если $p<q$, то либо $V_{s_p}>V_{s_q}$, либо $V_{s_p}=V_{s_q}$ и $W_{s_p}\ge W_{s_q}$.

Шаг 5. Создать матрицу $\mathbf{U}=\left(u_{xy}\right)_{x=1,\,y=1}^{2,\,L}$ и присвоить $n\leftarrow 1$, $\phi\leftarrow 64$, $y\leftarrow 1$.

Шаг 6. Пока $y\le L$ выполнять следующее:

Шаг 6.1. Если $c_\phi^{(s_n)}\neq 0$, то присвоить $u_{1y}\leftarrow s_n$, $u_{2y}\leftarrow\phi$, $y\leftarrow y+1$.

Шаг 6.2. Присвоить $n\leftarrow n+1$.

Шаг 6.3. Если $n>K$, то присвоить $n\leftarrow 1$, $\phi\leftarrow\phi-1$.

Шаг 7. Присвоить $y\leftarrow 1$.

Шаг 8. Пока $y\le L$ выполнять следующее:

Шаг 8.1. Если $m_y=0$, то перейти к шагу 8.3. В противном случае перейти к шагу 8.2.

Шаг 8.2. Если $c_{u_{2y}}^{(u_{1y})}<0$ и $c_{u_{2y}}^{(u_{1y})}\equiv 0 \bmod 2$, либо $c_{u_{2y}}^{(u_{1y})}>0$ и $c_{u_{2y}}^{(u_{1y})}\equiv 1 \bmod 2$, то присвоить $y\leftarrow y+1$ и перейти к шагу 8. В противном случае перейти к шагу 8.4.

Шаг 8.3. Если $c_{u_{2y}}^{(u_{1y})}<0$ и $c_{u_{2y}}^{(u_{1y})}\equiv 1 \bmod 2$, либо $c_{u_{2y}}^{(u_{1y})}>0$ и $c_{u_{2y}}^{(u_{1y})}\equiv 0 \bmod 2$, то присвоить $y\leftarrow y+1$ и перейти к шагу 8. В противном случае перейти к шагу 8.4.

Шаг 8.4. Если $\left|c_{u_{2y}}^{(u_{1y})}\right|>1$, то сгенерировать случайным образом $r\in\{0,1\}$ и перейти к шагу 8.6. В противном случае перейти к шагу 8.5.

Шаг 8.5. Если $c_{u_{2y}}^{(u_{1y})}=1$, то присвоить $r\leftarrow 0$. В противном случае присвоить $r\leftarrow 1$.

Шаг 8.6. Вычислить $c_{u_{2y}}^{(u_{1y})}\leftarrow c_{u_{2y}}^{(u_{1y})}+(-1)^r$ и присвоить $y\leftarrow y+1$.

Шаг 9. Осуществить статистическое кодирование квантованных ДКП-коэффициентов и завершить алгоритм.

Матрица **U** определяет стегопуть следующим образом: u_{1y} указывает на номер блока ДКП, u_{2y} – на номер ненулевого АС-коэффициента в данном блоке, в который должен быть встроен бит сообщения m_y, $y=\overline{1,L}$.

Результаты вычислительных экспериментов с предложенным алгоритмом представлены на рис. 6.

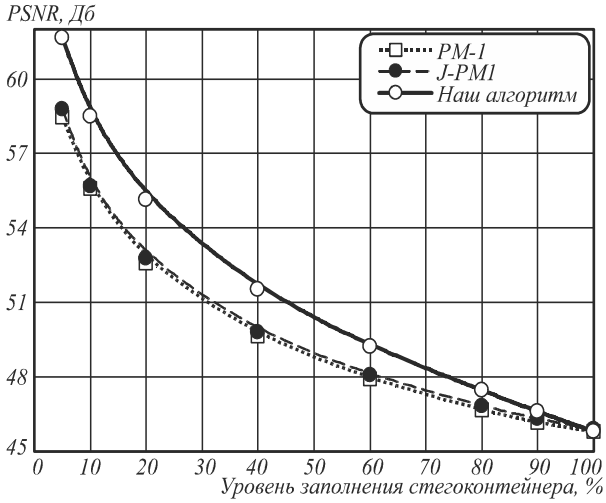


Рис. 6. Зависимость величины искажений изображения от длины сообщения для предложенного алгоритма и аналогов

Максимальное улучшение при частичном заполнении стегоконтейнера достигает 2,5 – 3,5 Дб относительно базового алгоритма и 2,25 – 3,25 Дб относительно алгоритма J-PM1.

При встраивании в цифровые изображения сообщений максимально возможной длины значимой разницы между значениями PSNR не наблюдается, поскольку в пространство сокрытия включены все возможные элементы. А как было показано ранее при анализе алгоритма J-PM1, способ модификации коэффициентов при записи в них битов сообщения определяет качество встраивания в меньшей степени, чем значения самих коэффициентов и их принадлежность той или иной частотной области.

Обратимость встраивания заложена в самом алгоритме: для извлечения встроенного сообщения не требуется передача каких-либо секретных параметров, поскольку при встраивании ни количество ненулевых коэффициентов, ни их распределение по частотным областям не изменяются.

Оценку стеганографической стойкости предложенного алгоритма проведём в сравнении с аналогами. Для этого рассмотрим два случая:

1. Стегоконтейнер содержит сообщение максимально возможной длины.
2. Длина встроенного сообщения меньше максимальной ёмкости стегоконтейнера.

В первом случае независимо от выбранного алгоритма для записи битов сообщения будут использованы все ненулевые АС-коэффициенты частотной области изображения, причём само стеганографическое преобразование каждый раз будет одно и то же. Таким образом, в данном случае все три алгоритма сравнимы по своей стеганографической стойкости.

Отдельно можно отметить, что J-PM1 и предложенный алгоритм обладают способностью изменять статистические характеристики встраиваемого сообщения за счёт нефиксированного порядка обхода ДКП-коэффициентов. Однако если сообщение уже имеет характеристики случайной последовательности, при максимальном заполнении стегоконтейнера данная способность не является существенно важной.

Для сообщений малой длины распределение встраиваемых битов по элементам частотной области изображения, осуществляемое предложенным алгоритмом, очевидным образом зависит от характерных особенностей самого изображения-стегоконтейнера.

При использовании изображений, содержащих значительное число областей с плавными цветовыми переходами (например, «Lenna», «Tiffany»), биты сообщений будут сосредоточены в тех блоках ДКП, которые соответствуют контурам объектов. В этом случае стегопуть не будет носить случайного характера.

Для изображений с большим числом мелких объектов и неоднородными текстурами (например, «Baboon», «Goldhill») стегопуть будет приближен к случайному.

Таким образом, по стеганографической стойкости в контексте степени случайности стегопути предложенный алгоритм опережает PM1, но в зависимости от характера изображения-стегоконтейнера в отдельных случаях может проигрывать J-PM1.

Для уменьшения корреляции между изображением и стегопутём без ухудшения качества встраивания в предложенный алгоритм допустимо ввести дополнительное перемешивающее преобразование всех подпоследовательностей последовательности значений вектора **S**, указывающих на блоки ДКП с одинаковыми значениями *V* и *W*.

Параметры данного перемешивающего преобразования могут быть использованы в качестве стеганографического ключа.

Заключение

В данной работе предложен новый алгоритм стеганографического встраивания информации в JPEG-изображения, построенный на основе метода «плюс/минус один» и отличающийся оригинальным подходом к формированию стегопути при встраивании сообщения. Сравнение с аналогами показало, что

данный алгоритм позволяет обеспечить более высокое качество цифровых изображений – стегоконтейнеров при равной ёмкости.

Предложенный алгоритм, как и другие алгоритмы подобного рода, можно использовать для организации скрытых каналов передачи данных ограниченного распространения в рамках решения задачи обеспечения конфиденциальности информации [24, 25].

Одно из возможных направлений развития данной работы заключается в применении нечёткой логики при формировании пространства сокрытия.

Благодарности

Работа выполнена при поддержке Минобрнауки России в рамках мероприятия 1.3 ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение о предоставление субсидии № 14.577.21.0153 от 28 ноября 2014 г.).

Литература

1. **Грибунин, В.Г.** Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-ПРЕСС, 2009. – 272 с.
2. **Salomon, D.** Data compression: the complete reference, 4th Edition. – London: Springer–Verlag, 2007. – 1111 p.
3. **Yu, L.** PM1 steganography in JPEG images using genetic algorithm / L. Yu, Y. Zhao, R. Ni, Z. Zhu // Soft Computing. – 2009. – Vol. 13(4). – P. 393-400. – ISSN 1433-7479.
4. **Fridrich, J.** Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fridrich. – Cambridge: Cambridge University Press, 2010. – 437 p.
5. **Nikolaidis, A.** Low overhead reversible data hiding for color JPEG images / A. Nikolaidis // Multimedia Tools And Applications. – 2014. – P. 1-13. – ISSN 1573-7721.
6. **Huang, F.** New channel selection rule for JPEG steganography / F. Huang, J. Huang, Y.-Q. Shi // IEEE Transactions on Information Forensics and Security. – 2012. – Vol. 7(4). – P. 1181-1191. – ISSN 1556-6013.
7. **Li, F.** Adaptive JPEG steganography with new distortion function / F. Li, X. Zhang, J. Yu, W. Shen // Annals of Telecommunications. – 2014. – Vol. 69(7-8). – P. 431-440. – ISSN 0003-4347.
8. **Almohammad, A.** High capacity steganographic method based upon JPEG / A. Almohammad, R.M. Hierons, G. Ghinea // Proceedings of the 3-th International Conference on Availability, Reliability and Security (ARES 2008). – Spain, Barcelona. – 2008. – P. 544–549.
9. **Vongurai, N.** Frequency-based steganography using 32×32 Interpolated quantization table and Discrete Cosine Transform / N. Vongurai, S. Phimoltares // Proceedings of the 5-th International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM). – Malaysia, Kuantan. – 2012. – P. 249-253.
10. **Wang, K.** A high capacity lossless data hiding scheme for JPEG images / K. Wang, Z.-M. Lu, Y.-J. Hu // The Journal of Systems and Software. – 2013. – Vol. 86(7). – P. 1965-1975. – ISSN 0164-1212.
11. **Velasco, C.** Adaptive JPEG steganography using convolutional codes and synchronization bits in DCT domain / C. Velasco, M. Nakano, H. Perez, R. Martinez, K. Yamaguchi // Proceedings of the 52-nd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS ‘09). – Mexico, Cancun. – 2009. – P. 842-847.
12. **Chen, B.** Quantization index modulation: a class of provably good methods for digital watermarking and information embedding / B. Chen, G.W. Wornell // IEEE Transactions on Information Theory. – 2001. –Vol. 47(4). – P. 1423-1443. – ISSN 0018-9448.
13. **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, № 2. – С. 262-267. – ISSN 0134-2452.
14. **Глумов, Н.И.** Алгоритм поблочного встраивания стойких ЦВЗ в крупноформатные изображения / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 3. – С. 368-372. – ISSN 0134-2452.
15. **Веричев, А.В.** Система встраивания цифровых водяных знаков на триангуляционной сетке опорных точек изображения / А.В. Веричев, В.А. Федосеев // Компьютерная оптика. – 2014. – Т. 38, № 3. – С. 555-563. – ISSN 0134-2452.
16. **Zhao, J.** Embedding robust labels into images for copyright protection / J. Zhao, E. Koch // Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies (KnowRight'95). – Austria, Vienna. – 1995. – P. 242-251.
17. **Burgett, S.** Copyright labeling of digitized image data / S. Burgett, E. Koch, J. Zhao // IEEE Communications Magazine. –1998. – Vol. 36(3). – P. 94-100. – ISSN 0163-6804.
18. **Holliman, M.** Adaptive public watermarking of DCT-based compressed images / M. Holliman, N. Memon, B.-L. Yeo, M. Yeung // Proceedings of SPIE – The International Society for Optical Engineering. – 1998. – Vol. 3312. – P. 284-295.
19. **Fujimura, M.** New data hiding scheme using method of embedding two bits data into two DCT coefficients / M. Fujimura, T. Takano, S. Baba, H. Kuroda // Proceedings of the International Conferences on Signal Processing, Image Processing and Pattern Recognition (SIP 2010) and Multimedia, Computer Graphics and Broadcasting (MulGraB 2010). – Korea Jeju, Island. – 2010. – P. 156-164.
20. **Chen, B.** Recursive code construction for reversible data hiding in DCT domain // Multimedia Tools and Applications. – 2013. – Vol. 72(2). – P. 1985-2009. – ISSN 1380-7501.
21. **Xuan, G.** Reversible data hiding for JPEG images based on histogram pair / G. Xuan, Y.Q. Shi, Z. Ni, P. Chai, X. Cui, X. Tong // Proceedings of the International Conference on Image Analysis and Recognition (ICIAR 2007). – Canada, Montreal. – 2007. – P. 715-727.
22. **Sakai, H.** Adaptive Reversible Data Hiding for JPEG Images / H. Sakai, M. Kuribayashi, M. Morii // Proceedings of the International Symposium on Information Theory and its Applications (ISITA2008). – New Zealand, Auckland. – 2008. – P. 1-6.
23. SIPI Image Database [Электронный ресурс]. – URL: http://sipi.usc.edu/database/ (дата обращения 1.08.2015).
24. **Крайнов, А.Ю.** Модель надёжности передачи информации в защищённой распределённой телекоммуникационной сети / А.Ю. Крайнов, Р.В. Мещеряков, А.А. Шелупанов // Известия Томского политехнического университета. – 2008. – Т. 313, № 2. – С. 60-63. – ISSN 1684-8519.
25. **Исхаков, С.Ю.** Гибридная система встраивания интерактивных услуг в цифровой телевизионный поток / С.Ю. Исхаков, А.А. Шелупанов, Р.В. Мещеряков, К.О. Беляков, В.А. Ширшин, А.Л. Шум, В.К. Сарьян // Телекоммуникации. – 2015. – № 1. – С. 11-19. – ISSN 1684-2588.

References

[1] Gribunin VG, Okov IN, Turincev IV. Digital steganography [in Russian]. Moscow: SOLON-PRESS; 2009.

[2] Salomon D. Data compression: the complete reference, 4th Edition. London: Springer–Verlag; 2007.
[3] Yu L, Zhao Y, Ni R, Zhu Z. PM1 steganography in JPEG images using genetic algorithm. Soft Computing 2009; 13(4): 393-400.
[4] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge: Cambridge University Press; 2010.
[5] Nikolaidis A. Low overhead reversible data hiding for color JPEG images. Multimedia Tools And Applications 2014: 1-13.
[6] Huang F, Huang J, Shi YQ. New channel selection rule for JPEG steganography. IEEE Transactions on Information Forensics and Security 2012; 7(4): 1181-91.
[7] Li F, Zhang X, Yu J, Shen W. Adaptive JPEG steganography with new distortion function. Annals of Telecommunications 2014; 69(7-8): 431-40.
[8] Almohammad A, Hierons RM, Ghinea G. High capacity steganographic method based upon JPEG. Proceedings of the 3-th International Conference on Availability, Reliability and Security (ARES 2008). Spain, Barcelona. 2008: 544-9.
[9] Vongurai N, Phimoltares S. Frequency-based steganography using 32×32 interpolated quantization table and Discrete Cosine Transform. Proceedings of the 5-th International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM). Malaysia, Kuantan. 2012: 249-53.
[10] Wang K, Lu ZM, Hu YJ. A high capacity lossless data hiding scheme for JPEG images. The Journal of Systems and Software 2013; 86(7): 1965-75.
[11] Velasco C, Nakano M, Perez H, Martinez R, Yamaguchi K. Adaptive JPEG steganography using convolutional codes and synchronization bits in DCT domain. Proceedings of the 52-nd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '09). Mexico, Cancun. 2009: 842-7.
[12] Chen B, Wornell GW. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory 2001; 47(4): 1423-43.
[13] Glumov NI, Mitekin VS. A new semi-fragile watermarking algorithm for image authentication and information hiding [In Russian]. Computer Optics 2011; 35(2): 262-7.
[14] Glumov NI, Mitekin VS. The algorithm for large-scale images robust watermarking using blockwise [In Russian]. Computer Optics 2011; 35(3): 368-72.
[15] Verichev AV, Fedoseev VA. Digital image watermarking on triange grid of feature points. Computer Optics 2014; 38(3): 555-63.
[16] Zhao J, Koch E. Embedding robust labels into images for copyright protection. Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies (KnowRight'95). Austria, Vienna. 1995: 242-51.
[17] Burgett S, Koch E, Zhao J. Copyright labeling of digitized image data. IEEE Communications Magazine 1998; 36(3): 94-100.
[18] Holliman M, Memon N, Yeo BL, Yeung M. Adaptive public watermarking of DCT-based compressed images. Proceedings of SPIE – The International Society for Optical Engineering 1998; 3312: 284-95.
[19] Fujimura M, Takano T, Baba S, Kuroda H. New data hiding scheme using method of embedding two bits data into two DCT coefficients. Proceedings of the International Conferences on Signal Processing, Image Processing and Pattern Recognition (SIP 2010) and Multimedia, Computer Graphics and Broadcasting (MulGraB 2010). Koream Jeju Island. 2010: 156-64.
[20] Chen B. Recursive code construction for reversible data hiding in DCT domain. Multimedia Tools and Applications 2013; 72(2): 1985-2009.
[21] Xuan G, Shi YQ, Ni Z, Chai P, Cui X, Tong X. Reversible data hiding for JPEG images based on histogram pairs. Proceedings of the International Conference on Image Analysis and Recognition (ICIAR 2007). Canada, Montreal. 2007: 715-27.
[22] Sakai H, Kuribayashi M, Morii M. Adaptive Reversible Data Hiding for JPEG Images. Proceedings of the International Symposium on Information Theory and its Applications (ISITA2008). New Zealand, Auckland. 2008: 1-6.
[23] SIPI Image Database. Source: ⟨http://sipi.usc.edu/database/⟩.
[24] Krainov AY, Mescheryakov RV, Shelupanov AA. Reliability model of informaion transmission in protected distributed telecommunication network [In Russian]. Bulletin of the Tomsk Polytechnic University 2008; 313(2): 60-3.
[25] Iskhakov SY, Shelupanov AA, Meshcheryakov RV, Belyakov KO, Shirshin VA, Shum AL, Saryan VK. Hybrid system of embedding of interactive services in digital television stream [In Russian]. Telecommunications 2015; 1: 11-9.

AN IMPROVED ALGORITHM FOR DATA HIDING IN COMPRESSED DIGITAL IMAGES BASED ON PM1 METHOD

O.O. Evsutin, A.S. Kokurina, A.A. Shelupanov, I.I. Shepelev
Tomsk State University of Control Systems and Radioelectronics

Abstract

In this paper a novel algorithm of information embedding in JPEG images based on the known steganography method «plus minus 1» is proposed and researched. It is shown that the cover image partial filling allows the algorithm to surpass its counterparts due to an original approach to the determination of the DCT coefficients traverse order for message bits embedding. The peak signal-to-noise ratio is used as a quality metric.

Keywords: information security, steganography, data hiding, digital images, JPEG.

Citation: Evsutin OO, Kokurina AS, Shelupanov AA, Shepelev II. An improved algorithm for data hiding in compressed digital images based on PM1 method. Computer Optics 2015; 39(4): 572-81. DOI: 10.18287/0134-2452-2015-39-4-572-581.

Сведения об авторах

Евсютин Олег Олегович, 1987 года рождения, в 2009 году с отличием окончил Томский государственный университет систем управления и радиоэлектроники (ТУСУР) по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». Кандидат технических наук (2012 год), работает доцентом кафедры комплексной информационной безопасности электронно-вычислительных систем ТУСУР. Область научных интересов: информационная безопасность, обработка цифровых изображений, приложения клеточных автоматов.

E-mail: *eoo@keva.tusur.ru* .

Oleg Olegovich Evsutin (b. 1987) graduated with honours from the Tomsk State University of Control Systems and Radioelectronics in 2009, majoring in Complex Information Security of Computer Systems. He received his Candidate in Engineering (2012) degree from Tomsk State University. He is the associate professor at the TSUCSR's Complex Information Security of Computer Systems sub-department. His current research interests include information security, digital images processing, applications of cellular automata theory.

Кокурина Анна Сергеевна, 1994 года рождения, студент ТУСУР специальности «Информационно-аналитические системы безопасности». Область научных интересов: информационная безопасность, стеганография.

E-mail: *office@keva.tusur.ru* .

Anna Sergeevna Kokurina (b. 1994) is student of the Tomsk State University of Control Systems and Radioelectronics, majoring in Information and Analytic Security Systems. Her current research interests include information security, steganography.

Шелупанов Александр Александрович, 1954 года рождения, доктор технических наук, профессор, ректор ТУСУР. Лауреат премии Правительства РФ в области образования и премии Правительства РФ в области науки и техники. В 1976 году окончил Томский государственный университет по специальностям «Прикладная математика» и «Механика». В 1991 году стал кандидатом физико-математических наук, в 1996 защитил диссертацию на соискание учёной степени доктора технических наук. Область научных интересов: моделирование сложных технических систем, информационная безопасность, методы и системы защиты информации.

E-mail: *saa@tusur.ru* .

Alexandr Alexandrovich Shelupanov (b. 1954) is Doctor in Engineering, professor, and rector of the Tomsk State University of Control Systems and Radioelectronics (TSUCSR). He is the recipient of the RF government prize in Education and RF government prize in Science and Technology. He is graduated (1976) from the Tomsk State University, majoring in Applied Mathematics and Mechanics. He received his Candidate in Physics and Mathematics (1991) and Doctor in Engineering (1996) degrees. His current research interests include modeling of complex technical systems, information security, methods and systems of information security.

Шепелев Илья Игоревич, 1992 года рождения, в 2015 году окончил ТУСУР по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». Область научных интересов: информационная безопасность, стеганография.

E-mail: *office@keva.tusur.ru* .

Ilya Igorevich Shepelev (b. 1992), graduated from the Tomsk State University of Control Systems and Radioelectronics in 2015, majoring in Complex Information Security of Computer Systems. His current research interests include information security, steganography.

Поступила в редакцию 28 августа 2015 г.
Окончательный вариант – 30 сентября 2015 г.