АЛГОРИТМ ВСТРАИВАНИЯ ИНФОРМАЦИИ В СЖАТЫЕ ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ НА ОСНОВЕ ОПЕРАЦИИ ЗАМЕНЫ С ПРИМЕНЕНИЕМ ОПТИМИЗАЦИИ

О.О. Евсютин[1], А.А. Шелупанов[1], Р.В. Мещеряков[1], Д.О. Бондаренко[1]
[1]Томский государственный университет систем управления и радиоэлектроники, Томск, Россия

Аннотация

В данной работе рассматривается одно из направлений цифровой стеганографии – встраивание информации в сжатые JPEG-изображения. Введена схема встраивания информации на основе операции замены ДКП-коэффициентов. Предложены и исследованы варианты алгоритмической реализации данной схемы. Для повышения качества встраивания, характеризуемого значением PSNR, использован генетический алгоритм. Основным результатом исследования является стеганографический алгоритм встраивания информации в сжатые JPEG-изображения, отличающийся возможностью неравномерного распределения битов сообщения по блокам ДКП-коэффициентов. Выбор оптимальной области встраивания осуществляется с помощью генетического алгоритма.

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

Цитирование: **Евсютин, О.О.** Алгоритм встраивания информации в сжатые цифровые изображения на основе операции замены с применением оптимизации / О.О. Евсютин, А.А. Шелупанов, Р.В. Мещеряков, Д.О. Бондаренко // Компьютерная оптика. – 2017. – Т. 41, № 3. – С. 412-421. – DOI: 10.18287/2412-6179-2017-41-3-412-421.

Введение

Цифровая стеганография представляет собой одно из современных направлений информационной безопасности. Стеганографические методы защиты информации позволяют решать такие задачи, как обеспечение конфиденциальности информации и обеспечение аутентификации цифровых объектов. Общим для всех стеганографических методов является скрытое встраивание дополнительной информации в цифровые объекты за счёт внесения некоторых изменений в элементы данных, составляющие цифровой объект. Свойства, которыми должен обладать данный процесс, зависят от конкретной задачи [1, 2].

В настоящем исследовании в качестве цифровых объектов-контейнеров рассматриваются сжатые JPEG-изображения. При работе с такими изображениями встраивание осуществляется посредством внесения изменений в квантованные коэффициенты дискретного косинусного преобразования (далее ДКП-коэффициенты или просто коэффициенты).

Можно выделить два основных подхода к встраиванию частей секретного сообщения в ДКП-коэффициенты JPEG-изображений:

1. Непосредственное встраивание битов в выбранные коэффициенты.
2. Изменение групп выбранных коэффициентов таким образом, чтобы они удовлетворяли определённым соотношениям в зависимости от встраиваемых битов [3].

Первый подход позволяет обеспечить бо́льшую ёмкость встраивания по сравнению со вторым подходом. Алгоритмы, работающие с отдельными ДКП-коэффициентами, могут использоваться как для встраивания в изображения цифровых водяных знаков, так и для встраивания произвольных сообщений, в то время как алгоритмы, работающие с группами ДКП-коэффициентов, преимущественно используются для встраивания цифровых водяных знаков.

Настоящее исследование развивает первый из указанных подходов. В статье вводится и исследуется схема встраивания информации в JPEG-изображения на основе операции замены отдельных ДКП-коэффициентов.

Данная статья организована следующим образом. В параграфе 1 представлен обзор и анализ методов и алгоритмов встраивания информации в сжатые JPEG-изображения. В параграфе 2 описана предлагаемая схема встраивания информации в сжатые JPEG-изображения на основе операции замены ДКП-коэффициентов. В параграфе 3 приведены варианты алгоритмической реализации данной схемы, построенные с применением генетического алгоритма (ГА). Результаты вычислительных экспериментов с полученными алгоритмами и их обсуждение представлены в параграфе 4. Заключение подводит итоги работы и указывает направления будущих исследований.

1. Обзор методов встраивания информации в JPEG-изображения

Известно достаточно много стеганографических методов и алгоритмов, работающих с JPEG-изображениями. Основное отличие между ними заключается в способах формирования пространства сокрытия – множества ДКП-коэффициентов, непосредственно используемых для записи битов встраиваемого сообщения.

В некоторых алгоритмах такого рода пространство сокрытия формируется из ДКП-коэффициентов, принимающих значения из заранее определённого множества.

Например, алгоритмы, представленные в [3, 4], используют для встраивания сообщения все ненулевые ДКП-коэффициенты блоков изображения-контейнера. Данные алгоритмы основаны на методе PM1, согласно которому в один коэффициент встраивается один бит сообщения. Встраивание заключается в уменьшении или увеличении коэффициента на единицу в зависимости от значения встраиваемого бита [1].

В статье [3] описывается алгоритм GA-PM1, в котором для выбора одного из двух возможных способов изменения каждого коэффициента используется ГА, что позволяет незначительно повысить эффективность встраивания. Алгоритм, представленный в [4], отличается бо́льшей эффективностью встраивания за счёт оригинального подхода к формированию стегопути с учётом свойств ДКП. Однако он не обладает способностью адаптироваться к свойствам конкретного изображения-контейнера.

В работе [5] для уменьшения искажений, вносимых в изображение при встраивании данного объёма информации, применяется свёрточное кодирование. Оно служит для предварительного преобразования сообщения в вид, обеспечивающий минимальное число изменений элементов данных изображения-контейнера. Непосредственное встраивание преобразованного сообщения осуществляется посредством сложения ДКП-коэффициентов со значениями из множества $\{-1, 0, 1\}$, поэтому данный алгоритм также можно считать разновидностью PM1.

В статье [6] для записи битов сообщения используются только ДКП-коэффициенты, равные по модулю заранее заданной величине L. Данная величина является параметром соответствующего алгоритма. При встраивании единичного бита абсолютное значение коэффициента увеличивается на единицу, при встраивании нулевого бита — остаётся без изменений. При этом все прочие коэффициенты, не включённые в пространство сокрытия, также увеличиваются по модулю на единицу, чтобы при извлечении сообщения не возникло неоднозначности.

В отмеченных исследованиях, а также и в других схожих работах отсутствует возможность произвольного выбора коэффициентов для встраивания независимо от их исходных значений, поскольку это приведёт к неоднозначности при извлечении сообщения.

Другой широкий класс алгоритмов основан на использовании определённой частотной области в блоке ДКП-коэффициентов, одинаковой для разных блоков и не зависящей от конкретного изображения-контейнера.

В статье [7] представлен пример такого алгоритма, основанного на методе QIM [8, 9]. Данный метод использует два разных квантователя для встраивания нулевых и единичных битов секретного сообщения в ДКП-коэффициенты JPEG-изображения. В [7] встраивание осуществляется в низкочастотную область ДКП-блока, включающую 21 коэффициент, в том числе DC-коэффициент. Такое решение связано с тем, что метод QIM не рассчитан на работу с нулевыми коэффициентами, которые в большом количестве содержатся в высокочастотной области.

Во многих работах встраивание информации в жёстко заданную частотную область в ДКП-блоке дополняется использованием изменённой таблицы квантования.

В [10] элементы таблицы квантования, соответствующие области средних частот ДКП-спектра, уменьшаются с помощью деления на целое число k с последующим округлением. Секретное сообщение записывается как число k-ичной системы счисления, и разряды данного числа аддитивным образом встраиваются в среднечастотные ДКП-коэффициенты.

В [11] представлена модификация классического стеганографического алгоритма F5 [12], в которой для повышения ёмкости встраивания элементы таблицы квантования в области средних частот принимаются равными единице. Это позволяет увеличить количество ненулевых квантованных коэффициентов, которые используются для формирования пространства сокрытия. Встраивание как в алгоритме F5, так и в рассматриваемой модификации является аддитивным и заключается в уменьшении на единицу абсолютных значений отдельных коэффициентов.

В [13] представлен пример LSB-подобного алгоритма, осуществляющего встраивание в наименее значимые биты среднечастотных ДКП-коэффициентов. К среднечастотным коэффициентам блока 8×8 авторы данной работы относят 26 ДКП-коэффициентов, находящихся в четырёх диагоналях блока с номерами $5-8$. Квантователи этих коэффициентов принимаются равными единице. В данном случае это делается не для повышения ёмкости встраивания, как в [10], а для уменьшения искажений стегоизображения. В каждый из 26 коэффициентов встраивается два бита секретного сообщения.

Модификации данного алгоритма представлены в работах [14, 15]. В [14] отмечается, что количество изменений, вносимых в младшие биты ДКП-коэффициентов, зависит от порядка, в котором выбираются биты встраиваемой двоичной последовательности. Уменьшение количества изменений может быть достигнуто за счёт предварительного преобразования блоков секретного сообщения с помощью матрицы подстановок. Для поиска оптимальной матрицы в [14] используется алгоритм роящихся частиц. Алгоритм, представленный в [15], отличается от [13] использованием таблицы квантования нестандартного размера 16×16.

Необходимо отметить, что использование изменённой таблицы квантования является решением, не лишённым недостатков. Оно позволяет увеличить ёмкость и качество встраивания, однако компрометирует устойчивость перед стегоанализом. Поскольку таблица квантования хранится в JPEG-файле, изменённые значения квантователей указывают как на факт наличия стеговложения, так и на расположение встроенных битов в блоках ДКП-коэффициентов.

Кроме того, жёсткое задание частотной области для встраивания битов сообщения приводит к невозможности управления ёмкостью ДКП-блоков. В каждый блок встраивается одинаковое количество битов. Однако встраивание равного количества информации в разные ДКП-блоки приводит к разным результатам. Целесообразно строить пространство сокрытия таким образом, чтобы биты сообщения могли быть неравномерно распределены по блокам изображения-контейнера.

Таким образом, следует отметить, что основным недостатком многих известных алгоритмов является невозможность адаптации к свойствам конкретной пары (*изображение–контейнер*, *сообщение*).

Невозможность выбора количества изменяемых коэффициентов в блоке характерна как для алгоритмов, работающих с определённой частотной областью, так и для алгоритмов, встраивающих информацию в ДКП-коэффициенты, принимающие значения из определённого множества. Во втором случае разные ДКП-блоки обладают разной ёмкостью, определяемой количеством коэффициентов с данными значениями, присутствующих в блоке. Однако увеличение или уменьшение ёмкости блока тем не менее является невозможным.

Основной целью настоящего исследования является получение алгоритма встраивания информации в сжатые JPEG-изображения, позволяющего добиться повышения PSNR при фиксированной длине сообщения за счёт адаптации стегопути к контейнеру и варьирования ёмкости в различных ДКП-блоках.

Схема встраивания, позволяющая синтезировать алгоритмы, обладающие указанным свойством, представлена в следующем параграфе настоящей статьи.

2. Предлагаемая схема встраивания информации в частотную область JPEG-изображений на основе операции замены

Введём общую схему встраивания информации в сжатые JPEG-изображения на основе операции замены квантованных ДКП-коэффициентов.

Пусть изображение-контейнер содержит K блоков квантованных ДКП-коэффициентов. Пространство сокрытия представляет собой некоторую подпоследовательность последовательности всех ДКП-коэффициентов, которую обозначим $C = c_1c_2\ldots c_L$, $L \le 64K$. Часть пространства сокрытия, образованную ДКП-коэффициентами одного блока, назовём областью встраивания данного блока. Будем считать, что нумерация коэффициентов блока осуществляется в порядке его «зигзагообразного» обхода. Секретное сообщение обозначим $M = m_1m_2\ldots m_L$, где $m_i \in \{0, 1\}$, $i = \overline{1, L}$. Количество битов, встраиваемых в один блок изображения, обозначим n. Если биты сообщения распределяются по блокам неравномерно, то можем записать $L = \sum_{j=1}^{K} n_j$, $n_j \ge 0$.

Значение, на которое будет заменён ДКП-коэффициент при встраивании в него бита секретного сообщения, назовём величиной замены и обозначим x.

Тогда схему встраивания информации в JPEG-изображения на основе операции замены опишем следующей формулой, где c_i' обозначает изменённое значение ДКП-коэффициента:

$$c_i' = \begin{cases} x, & \text{если } m_i = 1, \\ -x, & \text{если } m_i = 0. \end{cases} \quad (1)$$

Обозначим последовательность ДКП-коэффициентов изображения-контейнера, не входящих в пространство сокрытия, $D = d_1d_2\ldots d_{64K-L}$, и введём дополнительную операцию для изменения данных коэффициентов:

$$d_i' = \begin{cases} x+1, & \text{если } d_i = x, \\ -x-1, & \text{если } d_i = -x, \\ d_i, & \text{в противном случае.} \end{cases} \quad (2)$$

Дополнительная операция необходима, чтобы при извлечении опираться только на ДКП-коэффициенты, равные x и $-x$, которые будут соответствовать единичным и нулевым битам секретного сообщения.

Основное преимущество, которое даёт представленная схема встраивания по сравнению с другими схемами, заключается в возможности произвольного выбора ДКП-коэффициентов, в которых будут размещены биты встраиваемого сообщения. При этом количество изменяемых коэффициентов для разных блоков изображения-контейнера может быть различным. Это позволит формировать пространство сокрытия для каждого конкретного контейнера наилучшим образом.

Устойчивость введённой схемы встраивания перед стегоанализом будет зависеть от статистических характеристик сообщения, объёма стеговложения и качества сжатия изображения-контейнера.

Распределение квантованных ДКП-коэффициентов JPEG-изображения близко к обобщённому нормальному распределению [3]. Если распределение нулей и единиц в сообщении будет отлично от равномерного, то столбцы гистограммы ДКП-коэффициентов со значениями x и $–x$ будут иметь вид, не соответствующий нормальному распределению, что послужит демаскирующим признаком. Для предупреждения данной уязвимости сообщение перед встраиванием должно быть сжато или зашифровано. В этом случае столбцы со значениями x и $–x$ на гистограмме ДКП-коэффициентов будут иметь симметричный вид (с некоторой допустимой погрешностью), что соответствует модели исходного изображения.

Другим демаскирующим признаком может послужить изменение высоты данных столбцов. Для предупреждения данной уязвимости длину сообщения следует задавать такой, чтобы она совпадала с количеством ДКП-коэффициентов, по абсолютному значению соответствующих величине замены для данного качества JPEG-сжатия изображения-контейнера. При встраивании сообщения малого объёма следует добавить в него поле, хранящее длину, и использовать только часть пространства сокрытия.

Таким образом, устойчивость перед стегоанализом может быть достигнута за счёт подстройки параметров встраивания под длину секретного сообщения или характеристики конкретного изображения-контейнера.

Отдельно необходимо отметить, что введённая схема встраивания не содержит секретного ключа. Величину замены x можно держать в секрете, однако это не даёт полноценного ключевого пространства. Поэтому следует рассмотреть возможные подходы к дополнению введённой схемы ключом.

1. Встраивание двоичной последовательности, содержащей биты секретного сообщения, некоторым образом перемешанные со случайно сгенерированными битами. Ключом в этом случае будут позиции битов секретного сообщения во встраиваемой последовательности.
2. Варьирование величины замены для разных блоков изображения-контейнера. Ключом будет последовательность $X=(x_1, x_2,\ldots,x_K)$, где K — количество блоков.
3. Использование множества величин замены вместо единственной величины. Ключом будет отображение $\{x_1, x_2,\ldots,x_K\}\to\{0,1\}$. При этом количество значений, соответствующих нулевому и единичному биту, может быть различным.

Первый из приведённых подходов совместим с алгоритмами, представленными в следующем параграфе настоящей статьи, а другие два — являются предметом отдельного исследования.

3. Алгоритмы, реализующие введённую схему встраивания информации

В данном параграфе представлены алгоритмы, реализующие описанную в параграфе 1 схему. Первый алгоритм сформулирован для случая, когда для всех блоков значение n постоянно и имеет следующий вид.

Алгоритм 1

Вход:

сообщение $M=m_1m_2\ldots m_L,\ m_i\in\{0,1\},\ i=\overline{1,L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены x; размер области встраивания n.

Выход:

заполненный стегоконтейнер.

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

Шаг 2. Для $i=\overline{1,K}$ выполнить следующее:

Шаг 2.1. Случайно сгенерировать n неповторяющихся значений, $1\le p_j\le 63,\ j=\overline{1,n}$.

Шаг 2.2. ДКП-коэффициенты i-го блока изображения с номерами $p_1, p_2,..., p_n$ преобразовать по формуле (1), прочие ДКП-коэффициенты i-го блока, за исключением DC-коэффициента, преобразовать по формуле (2).

Шаг 3. Осуществить статистическое кодирование ДКП-коэффициентов, и завершить алгоритм.

Здесь и далее для упрощения будем считать, что встраиваемое сообщение прошло предобработку и включает поле, содержащее длину полезной части сообщения.

Данный алгоритм служит для оценки влияния величины замены и количества замен на качество встраивания при случайном выборе позиций встраиваемых битов в ДКП-блоках изображения-контейнера.

Случайный выбор ДКП-коэффициентов для встраивания является «наивным» решением и не позволяет обеспечить наилучшее качество стегоизображения при встраивании данного объёма информации, как это будет показано далее. Повышение качества встраивания в данной работе осуществляется посредством оптимизации с применением ГА.

Далее представлено два варианта применения ГА для повышения качества встраивания. Оптимизация производится для отдельных блоков ДКП-коэффициентов. В качестве целевой функции используется величина PSNR.

В первом случае ГА служит для выбора в каждом блоке оптимальных коэффициентов для встраивания. Количество коэффициентов одинаково для всех блоков. Соответствующий алгоритм представлен ниже.

Алгоритм 2

Вход:

сообщение $M=m_1m_2\ldots m_L,\ m_i\in\{0,1\},\ i=\overline{1,L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены x; размер области встраивания n; параметры ГА.

Выход:

заполненный стегоконтейнер.

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

Шаг 2. Для $i=\overline{1,K}$ выполнить следующее:

Шаг 2.1. Сгенерировать начальную популяцию ГА, состоящую из PS особей вида $\mathbf{p}^k=\left(p_1^k, p_2^k, \ldots, p_n^k\right)$, $p_u^k\in\{0,1\}^6$, причём $\forall u\ne v$ $p_u^k\ne p_v^k$, и рассчитать значение целевой функции для каждой особи.

Шаг 2.2. Осуществлять развитие популяции в течение SN итераций, исключая из неё особей с одинаковыми значениями отдельных элементов в случае их появления.

Шаг 2.3. Выбрать особь $\mathbf{p}^{\text{best}}=\left(p_1^{\text{best}}, p_2^{\text{best}}, \ldots, p_n^{\text{best}}\right)$ с максимальным значением целевой функции.

Шаг 2.4. ДКП-коэффициенты i-го блока изображения с номерами p_1^{best}, p_2^{best}, ..., p_n^{best} преобразовать по формуле (1), прочие ДКП-коэффициенты i-го блока преобразовать по формуле (2).

Шаг 3. Осуществить статистическое кодирование ДКП-коэффициентов, и завершить алгоритм.

Во втором случае ГА, кроме выбора оптимальных коэффициентов для встраивания, служит также для выбора количества битов, встраиваемых в отдельно взятый блок. Область встраивания выбирается в пределах заданной области частот ДКП-блока, ограниченной коэффициентами с номерами от s до e. Особь ГА представляет собой двоичный вектор $\mathbf{a}=(a_1, a_2,\ldots, a_{e-s+1})$, $a_i\in\{0,1\}$, где значение $a_i=1$ означает, что коэффициент с номером $s+i-1$ будет изменён по формуле (1), а значение $a_i=0$ означает, что данный коэффициент останется без изменений либо будет изменён по формуле (2). Очевидно, что

наилучшее качество встраивания будет достигнуто при наименьшем количестве замен, поэтому может наблюдаться вырождение популяции, заключающееся в появлении нулевых векторов. Обновлённую популяцию необходимо каждый раз проверять на наличие таких особей, и исключать их из неё.

Дополнительным параметром алгоритма встраивания является величина δ, представляющая собой пороговое значение PSNR для блока изображения. В случае, если в течение заданного количества итераций ГА будет найдено несколько особей, для которых значение целевой функции превышает пороговое, то в качестве лучшей особи будет принята та, которая обеспечивает наибольший объём вложения в данный ДКП-блок. Однако если найдётся такая особь, которая соответствует ненулевому объёму вложения, при том, что все коэффициенты остались без изменений, то лучшей будет считаться она.

Соответствующий алгоритм представлен ниже.

Алгоритм 3

Вход:

сообщение $M = m_1 m_2 \ldots m_L$, $m_i \in \{0, 1\}$, $i = \overline{1, L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены x; границы области встраивания s, e; параметр качества ДКП-блока δ; параметры ГА.

Выход:

заполненный стегоконтейнер.

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

Шаг 2. Для $i = \overline{1, K}$ выполнить следующее:

Шаг 2.1. Сгенерировать начальную популяцию ГА, состоящую из PS особей вида $\mathbf{a}^k = \left(a_1^k, a_2^k, \ldots, a_n^k\right) \neq \mathbf{0}$, $a_u^k \in \{0, 1\}$, $n = s–e+1$, и рассчитать значение целевой функции для каждой особи.

Шаг 2.2. Если в популяции есть особи, для которых значение целевой функции превышает δ, выбрать среди них особь с наибольшим количеством единичных генов и запомнить её как $\mathbf{a}^{\text{best}}$. В противном случае запомнить особь с наибольшим значением целевой функции как $\mathbf{a}^{\text{best}}$.

Шаг 2.3. Если в популяции есть особь, для которой значение целевой функции обращается в бесконечность, запомнить её как $\mathbf{a}^{\text{inf}}$. В противном случае присвоить $\mathbf{a}^{\text{inf}} = \mathbf{0}$.

Шаг 2.4. Для $j = \overline{1, SN}$ выполнить следующее:

Шаг 2.4.1. Сформировать новую популяцию, исключая из неё особи, не содержащие единичных генов, и рассчитать значение целевой функции для каждой особи.

Шаг 2.4.2. Обновить вектор $\mathbf{a}^{\text{best}}$.

Шаг 2.4.3. Обновить вектор $\mathbf{a}^{\text{inf}}$.

Шаг 2.5. Если $\mathbf{a}^{\text{inf}} \neq \mathbf{0}$, то перейти к шагу 2.1. В противном случае $\forall\, a_u^{\text{best}} = 1$ ДКП-коэффициенты i-го блока изображения с номерами u+s–1 преобразовать по формуле (1), прочие ДКП-коэффициенты i-го блока преобразовать по формуле (2).

Шаг 3. Осуществить статистическое кодирование ДКП-коэффициентов, и завершить алгоритм.

Оба представленных алгоритма встраивания, построенных с использованием оптимизации, обеспечивают значительное повышение качества встраивания по сравнению с алгоритмом 1. Однако алгоритм 3 из-за стремления популяции ГА к вырождению при варьировании количества изменяемых коэффициентов ДКП-блока в большинстве случаев уступает алгоритму 2, как это будет показано в следующем параграфе настоящей статьи. Поэтому для реализации неравномерного встраивания был предложен новый алгоритм, в котором ГА используется только для нахождения области встраивания ДКП-блока. Оптимальное количество встраиваемых битов определяется с помощью перебора возможных значений в заданном отрезке. Такое решение замедляет скорость встраивания, но позволяет избежать вырождения популяции ГА.

Соответствующий алгоритм представлен ниже.

Алгоритм 4

Вход:

сообщение $M = m_1 m_2 \ldots m_L$, $m_i \in \{0, 1\}$, $i = \overline{1, L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены x; минимальное и максимальное количество битов, встраиваемых в блок, $n_{\min}$ и $n_{\max}$; параметр качества ДКП-блока δ; параметры ГА.

Выход:

заполненный стегоконтейнер.

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

Шаг 2. Для $i = \overline{1, K}$ выполнить следующее:

Шаг 2.1. Для $n = \overline{n_{\min}, n_{\max}}$ выполнить следующее:

Шаг 2.1.1. Сгенерировать начальную популяцию ГА, состоящую из PS особей вида $\mathbf{p}^k = \left(p_1^k, p_2^k, \ldots, p_n^k\right)$, $p_u^k \in \{0, 1\}^6$, причём $\forall u \neq v$ $p_u^k \neq p_v^k$, и рассчитать значение целевой функции для каждой особи.

Шаг 2.1.2. Найти особь с наибольшим значением целевой функции и запомнить её как $\mathbf{p}^{\text{best}}$.

Шаг 2.1.3. Если в популяции есть особь, для которой значение целевой функции обращается в бесконечность, запомнить её как $\mathbf{p}^{\text{inf}}$. В противном случае присвоить $\mathbf{p}^{\text{inf}} = \mathbf{0}$.

Шаг 2.1.4. Осуществлять развитие популяции в течение SN итераций, исключая из неё особей с одинаковыми значениями отдельных элементов в случае их появления и обновляя на каждый итерации векторы $\mathbf{p}^{\text{best}}$ и $\mathbf{p}^{\text{inf}}$.

Шаг 2.1.5. Если $n = n_{\min}$, то присвоить $\mathbf{a}^{\text{best}} = \mathbf{p}^{\text{best}}$, $\mathbf{a}^{\text{inf}} = \mathbf{p}^{\text{inf}}$. В противном случае присвоить $\mathbf{a}^{\text{inf}} = \mathbf{p}^{\text{inf}}$, и, если значение целевой функции для $\mathbf{p}^{\text{best}}$ больше δ, присвоить $\mathbf{a}^{\text{best}} = \mathbf{p}^{\text{best}}$.

Шаг 2.2. Если $\mathbf{a}^{\inf} \neq \mathbf{0}$, то перейти к шагу 2.1. В противном случае ДКП-коэффициенты *i*-го блока изображения с номерами a_1^{best}, a_2^{best}, ..., a_n^{best}, $n_{\min} \le n \le n_{\max}$ преобразовать по формуле (1), прочие ДКП-коэффициенты *i*-го блока преобразовать по формуле (2).

Шаг 3. Осуществить статистическое кодирование ДКП-коэффициентов, и завершить алгоритм.

Во всех представленных случаях для извлечения встроенного сообщения необходимо знать величину замены *x*. Прочие параметры встраивания служат для того, чтобы наилучшим образом разместить сообщение в ДКП –блоках изображения–контейнера, и при извлечении не требуются. Поэтому алгоритм извлечения для алгоритмов 1–4 будет одинаков. Он сформулирован ниже.

Алгоритм извлечения

Вход:

заполненный стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены *x*.

Выход:

извлечённое сообщение.

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

Шаг 2. Присвоить $i = 0$.

Шаг 3. Для $j = \overline{1, 64K}$ выполнить следующее:

Шаг 3.1. Если $|c_j| = x$, то присвоить $i = i+1$,

$$m_i = \begin{cases} 1, & \text{если } c_j = x, \\ 0, & \text{если } c_j = -x. \end{cases}$$

Шаг 4. Считать из первых *h* извлечённых битов значение *L*, и присвоить $M = m_{h+1}m_{h+2}\ldots m_{h+L}$.

Шаг 5. Вернуть извлечённое сообщение *M* и завершить алгоритм.

Максимальная ёмкость изображения-контейнера зависит от его разрешения. В экспериментах, результаты которых представлены в следующем параграфе, значение *h* было принято равным 16.

4. Вычислительные эксперименты и их обсуждение

Вычислительные эксперименты проводились на выборке из 8 полноцветных тестовых JPEG-изображений разрешением 512×512 пикселей: «Airplane», «Baboon», «House», «Lenna», «Peppers», «Sailboat», «Splash», «Tiffany» [16]. Встраиваемые сообщения представляли собой тексты на русском языке, сжатые с помощью программы-архиватора.

На рис. 1 представлены зависимости значения PSNR от длины встраиваемого сообщения, полученные для алгоритма 1 при различных значениях параметров встраивания. Здесь и далее графики строились посредством усреднения по всей тестовой выборке.

При малых значениях *x* и *n* алгоритм 1 позволяет обеспечить приемлемое качество встраивания. Однако в большинстве случаев случайный выбор ДКП-коэффициентов приводит к заметным искажениям изображения-контейнера.

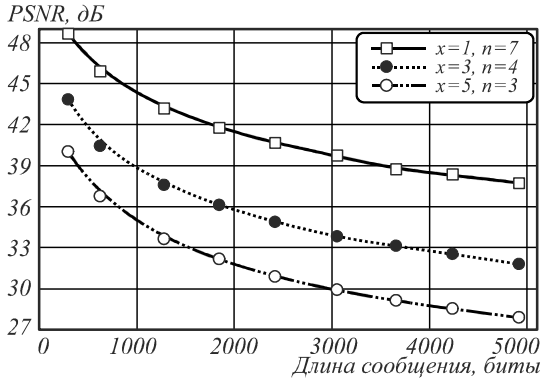

Рис. 1. Зависимость качества встраивания от длины сообщения для алгоритма 1

Алгоритм 2 основан на использовании ГА, поэтому эффективность встраивания в данном случае зависит от параметров оптимизации. Графики на рис. 2 отражают зависимость величины PSNR от параметров ГА при встраивании в изображение «Lenna» сообщения длиной 1200 битов (для $x = 3$, $n = 4$).

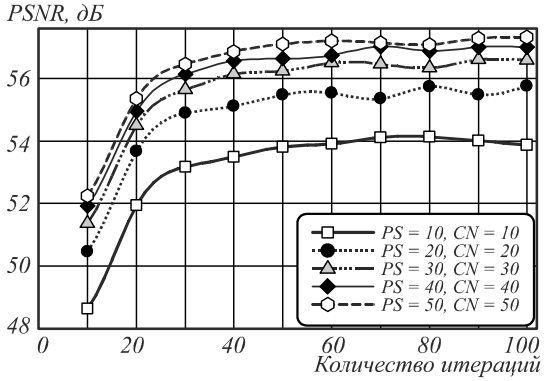

Рис. 2. Зависимость качества встраивания от параметров оптимизации для алгоритма 2

Можно увидеть, что при увеличении численности популяции ГА рост качества встраивания постепенно замедляется, причём при развитии каждой популяции наибольшую результативность показывают первые 30–50 итераций. Для других тестовых изображений данные зависимости имели аналогичный вид.

Зависимости значения PSNR от длины встраиваемого сообщения, полученные для алгоритма 2 при различных значениях параметров встраивания, представлены на рис. 3. В соответствующих экспериментах использовались следующие значения параметров ГА: $PS = 40$, $CN = 40$, $SC = 50$.

Алгоритм 2 очевидным образом значительно опережает по качеству встраивания алгоритм 1 за счёт использования ГА.

Алгоритм 3 реализует другой подход к использованию ГА для оптимизации встраивания. На рис. 4 представлены графики, отражающие зависимость качества и ёмкости встраивания от параметров ГА при встраивании в изображение «Lenna» сообщения длиной 1200 битов (для $x = 3$, $n = 4$, $\delta = 50$ дБ).

Из рис. 4*б* видно стремление популяции ГА к вырождению. Это выражается в уменьшении ёмкости встраивания до минимума, когда среднее количество

битов сообщения, приходящееся на один блок изображения-контейнера, стремится к единице.

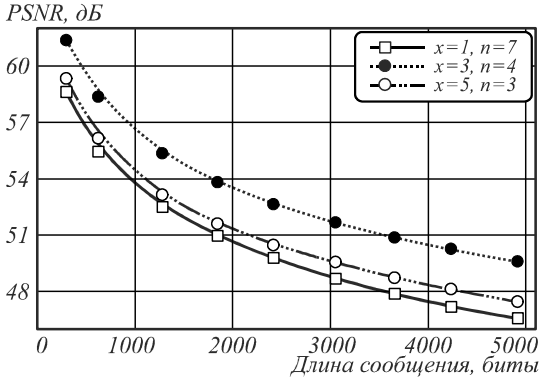

Рис. 3. Зависимость качества встраивания от длины сообщения для алгоритма 2

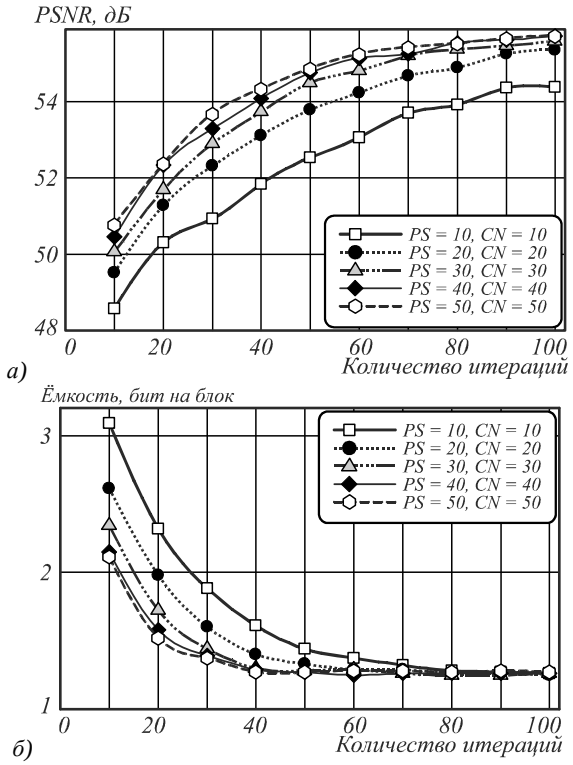

Рис. 4. Зависимость качества и ёмкости встраивания от параметров оптимизации для алгоритма 3

Зависимости значения PSNR от длины встраиваемого сообщения, полученные для алгоритма 3 при различных значениях параметров встраивания, представлены на рис. 5. В соответствующих экспериментах использовались следующие значения параметров ГА: $PS = 30$, $CN = 30$, $SC = 35$.

Алгоритм 3 также значительно опережает по качеству встраивания алгоритм 1, но при этом уступает алгоритму 2.

Последний из представленных в настоящей работе алгоритмов реализует объединение двух подходов к оптимизации встраивания с помощью ГА.

Можно увидеть, что алгоритм 4 отличается наибольшей эффективностью среди всех предложенных алгоритмов.

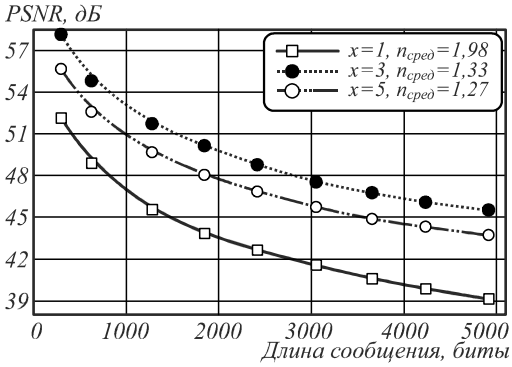

Рис. 5. Зависимость качества встраивания от длины сообщения для алгоритма 3

Зависимости значения PSNR от длины встраиваемого сообщения, полученные для алгоритма 4 при различных значениях параметров встраивания, представлены на рис. 6. В данных экспериментах использовались те же параметры ГА, что и для алгоритма 2.

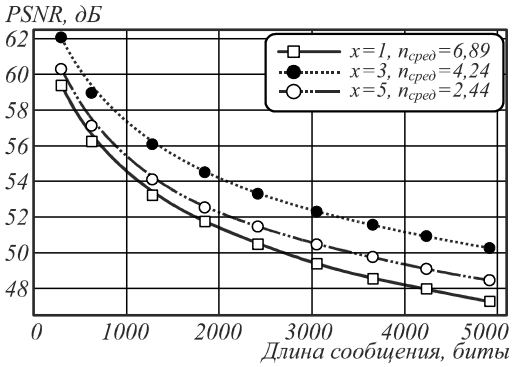

Рис. 6. Зависимость качества встраивания от длины сообщения для алгоритма 4

В табл. 1 приведено сравнение алгоритма 4 с алгоритмами, описанными в работах [6, 7, 10], которые в настоящем исследовании рассматриваются в качестве основных аналогов предложенных алгоритмов, так как сопоставимы с ними по ёмкости встраивания.

Табл. 1. Сравнение алгоритма 4 с аналогами

Ёмкость, биты	**PSNR, дБ**			
	Алгоритм [6]	**Алгоритм [7]**	**Алгоритм [10]**	**Алгоритм 4**
2000	47,11	—	—	54,20
5000	45,46	—	—	52,29
10000	43,77	—	—	46,29
36279	—	37,57	—	42,75
49128	—	—	35,39	40,60

Можно увидеть, что лучший из полученных в настоящей работе алгоритмов опережает по качеству встраивания алгоритмы-аналоги. Сравнение в каждом случае проводилось на той части описанной ранее тестовой выборки, для которой приведены результаты экспериментов в соответствующих статьях. Сравнение с алгоритмом [6] проводилось для $x = 3$, в остальных случаях использовалось значение $x = 1$.

Для исследования введённой схемы встраивания на предмет устойчивости перед стегоанализом был использован метод, основанный на законе Бенфорда [17]. Данный метод основан на сравнении частоты

появления цифры y на первом месте десятичной записи квантованных ДКП-коэффициентов в исследуемом изображении с величиной, рассчитанной по формуле

$$P(y) = N \cdot \log_{10}\left(1+1/(s+y^q)\right), \quad (3)$$

где N, s, q — параметры, зависящие от качества JPEG-сжатия. Если отклонение реальной величины от ожидаемой превышает некоторый порог, то принимается решение о наличии вложения в данном изображении.

Согласно [17], наиболее информативным признаком, свидетельствующим о наличии стеганографического вложения, является отклонение распределения цифры «2». Пороговое значение отклонения для качества JPEG-сжатия 90 % составляет 2,9.

Данный метод показывает хорошие результаты при стегоанализе известных стеганографических методов и при этом отличается низким уровнем ошибок первого рода.

В табл. 2 приведены результаты исследования алгоритма 4 с помощью метода стегоанализа на основе закона Бенфорда. Встраивание осуществлялось для $x = 3$.

Табл. 2. Результаты стегоанализа алгоритма 4

Длина сообщения, биты	**Среднее значение отклонения от $P(2)$**	**Доля выявленных стегоконтейнеров, %**
1000	0,59	0
3000	0,91	0
5000	1,49	0
10000	2,61	12,5

Можно увидеть, что с ростом объёма вложения отклонение рассчитанного распределения от ожидаемого возрастает, однако только при встраивании 10000 битов для одного стегоконтейнера из восьми наблюдается превышение порогового значения. При этом доля правильно определённых изображений без вложения в использованной выборке составила 100 %.

Таким образом, результаты экспериментов подтверждают эффективность введённой схемы встраивания информации и реализующих её алгоритмов.

Заключение

В данной работе введена схема встраивания информации в сжатые JPEG-изображения на основе операции замены, применяемой к квантованным ДКП-коэффициентам, предложены и исследованы варианты её алгоритмической реализации. Введённая схема встраивания предполагает использование произвольной величины замены, а предложенные алгоритмы позволяют обеспечить неравномерное распределение битов сообщения по блокам ДКП-коэффициентов изображения-контейнера. Данное решение позволяет адаптировать встраивание к свойствам изображения-контейнера.

Введённая схема встраивания информации может быть использована для синтеза алгоритмов встраивания сообщений, в том числе цифровых водяных знаков в сжатые JPEG-изображения.

Развитие данной работы будет заключаться в получении новых алгоритмических реализаций введённой схемы встраивания, основанных на более эффективных алгоритмах оптимизации расположения встраиваемых битов внутри блока ДКП-коэффициентов. Кроме того, дальнейшие исследования будут направлены на получение и исследование других схем стеганографического встраивания информации в сжатые цифровые изображения.

Благодарности

Данная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания ТУСУР на 2017–2019 гг. (проект № 2.3583.2017/4.6) и при поддержке РФФИ (проект № 16-47-700350 р_а). Кроме того, авторы выражают благодарность рецензентам за конструктивные замечания, которые помогли улучшить данную статью.

Литература

1. **Fridrich, J.** Steganography in digital media: Principles, algorithms, and applications / J. Fridrich. – Cambridge: Cambridge University Press, 2010. – 437 p. – ISBN: 978-0-521-19019-0.
2. **Федосеев, В.А.** Унифицированная модель систем встраивания информации в цифровые сигналы / В.А. Федосеев // Компьютерная оптика. – 2016. – Т. 40, № 1. – С. 87-98. – DOI: 10.18287/2412-6179-2016-40-1-87-98.
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. – DOI: 10.1007/s00500-008-0327-7.
4. **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.
5. **Li, F.** Adaptive JPEG steganography with new distortion function / F. Li, X. Zhang, J. Yu, W. Shen // Annals of Telecommunications. – 2014. – Vol. 69(7). – P. 431-440. – DOI: 10.1007/s12243-013-0415-2.
6. **Nikolaidis, A.** Low overhead reversible data hiding for color JPEG images / A. Nikolaidis // Multimedia Tools and Applications. – 2016. – Vol. 75(4). – P. 1869-1881. – DOI: 10.1007/s11042-014-2377-4.
7. **Noda, H.** High-performance JPEG steganography using quantization index modulation in DCT domain / H. Noda, M. Niimi, E. Kawaguchi // Pattern Recognition Letters. – 2006. – Vol. 27(5). – P. 455-461. – DOI: 10.1016/j.patrec.2005.09.008.
8. **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. – DOI: 10.1109/18.923725.
9. **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.
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. – DOI: 10.1016/j.jss.2013.03.083.

11. **Jiang, C.** A high capacity steganographic method based on quantization table modification and F5 algorithm / C. Jiang, Y. Pang, S. Xiong // Circuits, Systems, and Signal Processing. – 2013. – Vol. 33(5). – P. 1611-1626. – DOI: 10.1007/s00034-013-9703-3.
12. **Westfeld, A.** F5 – a steganographic algorithm. High capacity despite better steganalysis / A. Westfeld // Proceedings of the 4th International Workshop on Information Hiding (IH 2001), USA, PA, Pittsburgh. – 2001. – P. 289-302.
13. **Chang, C.-C.** A steganographic method based upon JPEG and quantization table modification / C.-C. Chang, T.-S. Chen, L.-Z. Chung // Information Sciences. – 2002. – Vol. 141(1-2). – P. 123-138. – DOI: 10.1016/S0020-0255(01)00194-3.
14. **Li, X.** A steganographic method based upon JPEG and particle swarm optimization algorithm / X. Li, J. Wang // Information Sciences. – 2007. – Vol. 177(15). – P. 3099-3109. – DOI: 10.1016/j.ins.2007.02.008.
15. **Jiang, C.** A high capacity steganographic method based on quantization table modification / C. Jiang, Y. Pang, L. Guo, B. Jing, X. Gong // Wuhan University Journal of Natural Sciences. – 2011. – Vol. 16, Issue 3. – P. 223-227. – DOI: 10.1007/s11859-011-0740-0.
16. The USC-SIPI image database [Электронный ресурс]. – URL: http://sipi.usc.edu/database/ (дата обращения 01.12.2016).
17. **Andriotis, P.** JPEG steganography detection with Benford's Law / P. Andriotis, G. Oikonomou, T. Tryfonas // Digital Investigation. – 2013. – Vol. 9(3-4). – P. 246-257. – DOI: 10.1016/j.diin.2013.01.005.

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 безопасности информационных систем ТУСУР. Область научных интересов: информационная безопасность, обработка цифровых изображений, приложения клеточных автоматов. E-mail: *eoo@keva.tusur.ru* .

Шелупанов Александр Александрович, 1954 года рождения, доктор технических наук, профессор, ректор ТУСУР. В 1976 году окончил Томский государственный университет по специальностям «Прикладная математика» и «Механика». Кандидат физико-математических наук (1991 год), доктор технических наук (1996 год). Область научных интересов: моделирование сложных технических систем, информационная безопасность, методы и системы защиты информации. E-mail: *saa@tusur.ru* .

Мещеряков Роман Валерьевич, 1974 года рождения, доктор технических наук, профессор, проректор ТУСУР по научной работе и инновациям. В 1997 году окончил Алтайский государственный технический университет им. И.И. Ползунова по специальности «Информационно-измерительная техника и технологии». Кандидат технических наук (2000 год), доктор технических наук (2011 год). Область научных интересов: обработка, анализ, синтез речевого сигнала и текста, системный анализ, информационная безопасность, математическое моделирование. E-mail: *mrv@tusur.ru* .

Бондаренко Дмитрий Олегович, 1993 года рождения, в 2016 году окончил ТУСУР по специальности «Информационная безопасность автоматизированных систем». Область научных интересов: информационная безопасность, стеганография, методы оптимизации. E-mail: *dima030793@gmail.com* .

ГРНТИ: 28.23.15
Поступила в редакцию 16 марта 2017 г. Окончательный вариант – 1 июня 2017 г.

AN ALGORITHM FOR INFORMATION EMBEDDING INTO COMPRESSED DIGITAL IMAGES BASED ON REPLACEMENT PROCEDURES WITH USE OF OPTIMIZATION

O.O. Evsutin[1], A.A. Shelupanov[1], R.V. Meshcheryakov[1], D.O. Bondarenko[1]
[1]Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia

Abstract

In the paper, we consider a particular direction of digital steganography — information embedding into the compressed JPEG images. A scheme of information embedding based on procedures of DCT-coefficients replacement is introduced. Variants of the scheme algorithmic implementation are offered and investigated. A genetic algorithm is used for the improvement of the embedding quality. The main result of the investigation is a steganographic algorithm of information embedding into the compressed JPEG images. This algorithm utilizes an unstable region of embedding at the level of one block of DCT-coefficients. The choice of an optimum region of embedding is performed by the genetic algorithm.

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

Citation: Evsutin OO, Shelupanov AA, Meshcheryakov RV, Bondarenko DO. An algorithm for information embedding into compressed digital images based on replacement procedures with use of optimization. Computer Optics 2017; 41(3): 412-421. DOI: 10.18287/2412-6179-2017-41-3-412-421.

Acknowledgements: The work was partially funded by the Russian Federation Ministry of Education and Science (grant 2.3583.2017/4.6) and the Russian Foundation of Basic Research (grant 16-47-700350 r_a).

References

[1] Fridrich J. Steganography in digital media: Principles, algorithms, and applications. Cambridge: Cambridge University Press; 2010. ISBN: 978-0-521-19019-0.

[2] Fedoseev VA. A unified model for information hiding systems [In Russian]. Computer Optics 2016; 40(1): 87-98. DOI: 10.18287/2412-6179-2016-40-1-87-98.

[3] Yu L, Zhao Y, Ni R, Zhu Z. PM1 steganography in JPEG images using genetic algorithm. Soft Computing 2009; 13(4): 393-400. DOI: 10.1007/s00500-008-0327-7.

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

[5] Li F, Zhang X, Yu J, Shen W. Adaptive JPEG steganography with new distortion function. Annals of Telecommunications 2014; 69(7): 431-440. DOI: 10.1007/s12243-013-0415-2.

[6] Nikolaidis A. Low overhead reversible data hiding for color JPEG images. Multimedia Tools and Applications 2016; 75(4): 1869-1881. DOI: 10.1007/s11042-014-2377-4.

[7] Noda H, Niimi M, Kawaguchi E. High-performance JPEG steganography using quantization index modulation in DCT domain. Pattern Recognition Letters 2006; 27(5): 455-461. DOI: 10.1016/j.patrec.2005.09.008.

[8] 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): 1423-1443. DOI: 10.1109/18.923725.

[9] Glumov NI, Mitekin VS. A new semi-fragile watermarking algorithm for image authentication and information hiding [In Russian]. Computer Optics 2011; 35(2): 262-267.

[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): 1965-1975. DOI: 10.1016/j.jss.2013.03.083.

[11] Jiang C, Pang Y, Xiong S. A high capacity steganographic method based on quantization table modification and F5 algorithm. Circuits, Systems, and Signal Processing 2013; 33(5): 1611-1626. DOI: 10.1007/s00034-013-9703-3.

[12] Westfeld A. F5 – a steganographic algorithm. High capacity despite better steganalysis. Proceedings of the 4th International Workshop on Information Hiding (IH 2001), USA, PA, Pittsburgh. 2001: 289-302.

[13] Chang C-C, Chen T-S, Chung L-Z. A steganographic method based upon JPEG and quantization table modification. Information Sciences 2002; 141(1-2): 123-138. DOI: 10.1016/S0020-0255(01)00194-3.

[14] Li X, Wang J. A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences 2007; 177(15): 3099-3109. DOI: 10.1016/j.ins.2007.02.008.

[15] Jiang C, Pang Y, Guo L, Jing B, Gong X. A high capacity steganographic method based on quantization table modification. Wuhan University Journal of Natural Sciences 2011; 16(3): 223-227. DOI: 10.1007/s11859-011-0740-0.

[16] The USC-SIPI image database. Source: ⟨http://sipi.usc.edu/database/⟩.

[17] Andriotis P, Oikonomou G, Tryfonas T. JPEG steganography detection with Benford's Law. Digital Investigation 2013: 9(3-4); 246-257. DOI: 10.1016/j.diin.2013.01.005.

Authors' information

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

Alexandr Alexandrovich Shelupanov (b. 1954) is Doctor in Engineering, professor, and rector of the Tomsk State University of Control Systems and Radioelectronics. 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. E-mail: *saa@tusur.ru* .

Roman Valeryevich Meshcheryakov (b. 1974) is Doctor in Engineering, professor, and vice-rector for research and innovation of the Tomsk State University of Control Systems and Radioelectronics. He is graduated (1997) from the Altai State Technical University majoring in Information Processing and Measurement Equipment and Technology. He received his Candidate in Engineering (2000) and Doctor in Engineering (2011) degrees. His current research interests include processing, analysis, synthesis of speech signals and texts, system analysis, information security, mathematical modeling. E-mail: *mrv@tusur.ru* .

Dmitry Olegovich Bondarenko (b. 1993), graduated from the Tomsk State University of Control Systems and Radioelectronics in 2016, majoring in Information Security of Computer Systems. His current research interests include information security, steganography, optimization methods. E-mail: *dima030793@gmail.com* .

Received March 16, 2017. The final version – June 1, 2017.