УДК 004.932

АЛГОРИТМ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ДАННЫХ В JPEG ИЗОБРАЖЕНИЯ, ОСНОВАННЫЙ НА ИСПОЛЬЗОВАНИИ ФУНКЦИЙ СВЕРТКИ

М. А. Дрюченко

Воронежский государственный университет

Поступила в редакцию 22.08.2018 г.

Аннотация. Рассматривается алгоритм стеганографического встраивания данных в изображения формата JPEG, основанный на использовании функции свертки при определении модифицируемых значений групп квантованных спектральных коэффициентов в процессе скрытия данных. Особенностями алгоритма являются высокая пропускная способность, минимальное искажение заполненного контейнера, а также возможность мультиплексирования скрытых каналов хранения информации. Исследуются показатели качества работы предложенного алгоритма в части оценки скрытой пропускной способности и уровня вносимых визуальных искажений носителя.
Ключевые слова: стеганография, функции свертки, хеш-функции.
Annotation. JPEG steganography embedding algorithm based on using convolution functions for determining the modified values of groups of quantized spectral coefficients is considered. The main features of the algorithm are high capacity, minimal distortion of the filled container, and the possibility of multiplexing hidden channels. The results of experiments which show the container distortion level and hidden capacity are presented.
Keywords: steganography, convolution functions, hash-functions.

ВВЕДЕНИЕ

На сегодняшний день одним из наиболее актуальных трендов в развитии методов обеспечения информационной безопасности является разработка, совершенствование и использование методов компьютерной и цифровой стеганографии как эффективных инструментов для защиты конфиденциальных данных, организации скрытного защищенного хранения и передачи гетерогенных данных по открытым каналам коммуникации, защиты прав авторства и скрытного маркирования объектов цифрового и аналогового контента. Стеганографические методы расширяют и дополняют возможности традиционных криптографических методов. К числу практически значимых задач, решаемых при разработке новых методов и алгоритмов стеганографического скрытия информации (ССИ) необходимо отнести повышение робастности, увеличение визуальной и статистической незаметности скрытых данных, а также повышение пропускной способности (ПС) стеганографических каналов. В данной работе основное внимание уделяется последней задаче – максимизации скрытой ПС при встраивании данных в графические контейнеры формата JPEG.

Стегоалгоритмы, работающие с JPEG, как правило, реализуют встраивание данных в коэффициенты дискретного косинусного преобразования (ДКП). При этом применяются два основных подхода:

1) встраивание элементов сообщения в отдельные значения выбранных спектральных коэффициентов путем перезаписи битами сообщения наименее значимых бит коэффициентов ДКП или путем прибавления/вычитания из коэффициентов ДКП заданных (малых по модулю) значений [1–5];

2) встраивание элементов сообщения за счет модификации групп значений выбранных коэффициентов ДКП таким образом, чтобы они удовлетворяли заданному соотношению [6, 7].

Для стегоалгоритмов первого класса, повышение ПС в большинстве случаев возможно за счет увеличения числа задействованных в процессе ССИ элементов контейнера или за счет модификации нескольких младших двоичных разрядов коэффициентов ДКП. Стегоалгоритмы второго класса, как правило, применяются при создании цифровых водяных знаков и имеют строго фиксированную (низкую) ПС, которая может быть повышена за счет использования при скрытии дополнительных пар или троек спектральных коэффициентов. Стоит отметить, что подобные варианты повышения ПС для алгоритмов, модифицирующих коэффициенты ДКП напрямую или, использующих принцип относительной замены величин спектральных коэффициентов, неизбежно приведут к существенному снижению качества заполненных контейнеров.

В данной работе рассматривается высокопроизводительный алгоритм стеганографического скрытия в JPEG, реализующий «непрямое» встраивание сообщений путем итеративной модификации абсолютных значений групп квантованных коэффициентов ДКП контейнера до момента совпадения результата вычисления функции свертки над элементами модифицированной группы со значением встраиваемого сообщения. Главной отличительной особенностью алгоритма является реализованный принцип стеганографического кодирования, при котором обеспечивается встраивание бóльшего числа бит информации по сравнению с числом модифицируемых бит контейнера, что позволяет минимизировать его искажение. Сами элементы скрываемого сообщения при этом в явном виде в контейнер не добавляются.

1. АЛГОРИТМ СТЕГОСКРЫТИЯ ДАННЫХ

Пусть I – незаполненный JPEG-контейнер размером $W \times H$ пикселей, используемый для скрытия файла сообщения M, $\tilde{I}$ – заполненный JPEG-контейнер. Для встраивания и извлечения M используется ключ K. Алгоритм ССИ $E : I \times M \times K \to \tilde{I}$ должен одновременно удовлетворять двум противоречивым требованиям:

– максимизации пропускной способности (ПС) стегосистемы ($\left|M\right| \Big/ \sum_{i=1}^{N} \left|D_i\right| \xrightarrow[N \to \min]{} \max$, где $\left|M\right|$ – размер сообщения, $\sum_{i=1}^{N} \left|D_i\right|$ – суммарный размер элементов контейнера, пригодных для использования в процедуре встраивания данных, N – число используемых для ССИ элементов – коэффициентов ДКП);

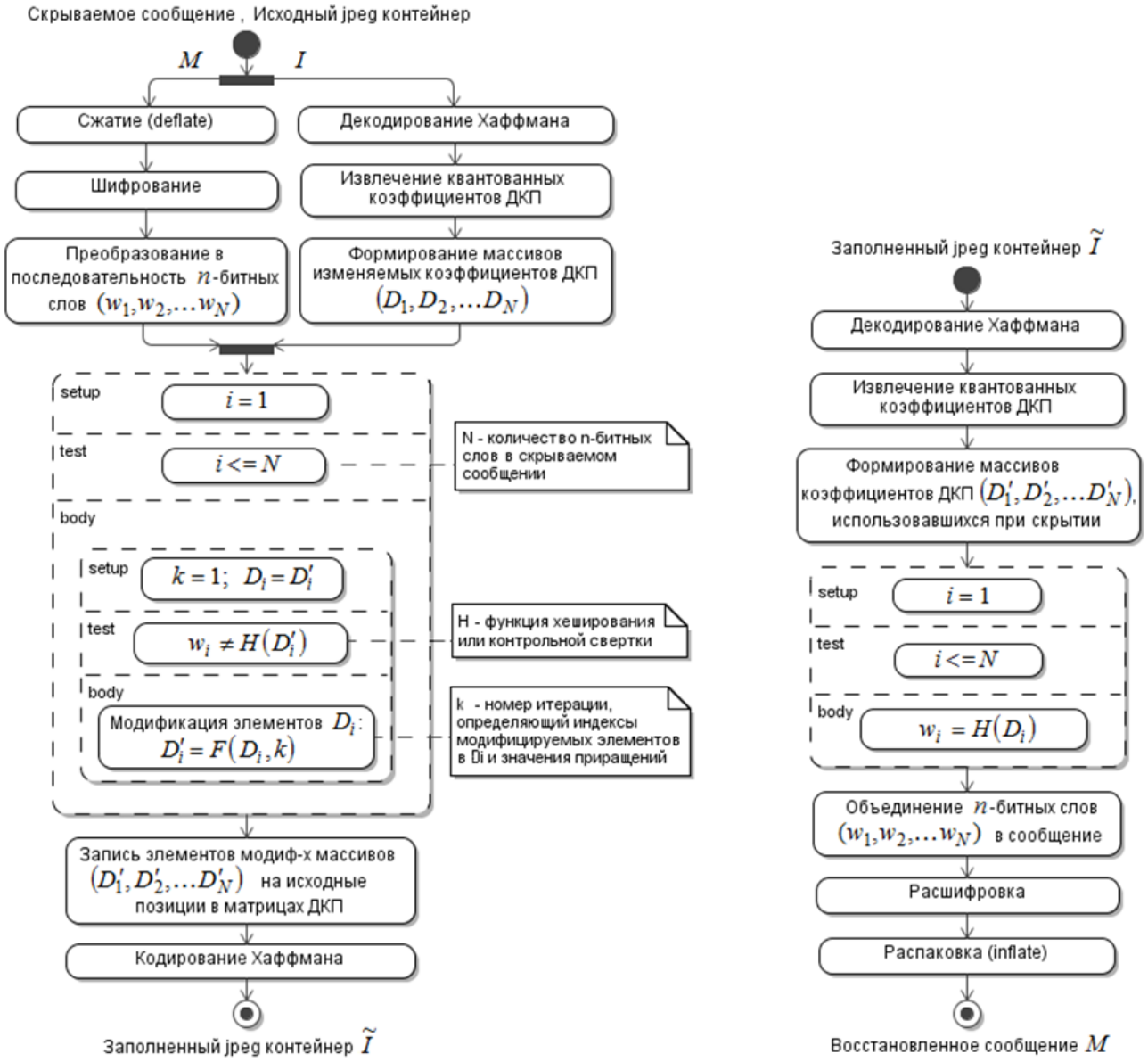
– минимизации визуальных искажений заполненного контейнера ($\left\| I - \tilde{I} \right\| \to \min$).

Предполагается, что заполненные контейнеры хранятся и используются в полностью цифровой среде без выполнения цифро-аналоговых и аналогово-цифровых преобразований, а также без внесения в них дополнительных искажений, поэтому дополнительные требования по обеспечению робастности скрытых данных в алгоритме ССИ не предъявляются.

Алгоритм извлечения информации $E^{-1} : \tilde{I} \times K \to M$ имеет строгий (не вероятностный) характер работы и позволяет безошибочно извлекать ранее скрытые данные. Для корректного извлечения сообщения необходимо знание стеганографического ключа K, компонентами которого могут являться ключ шифрования сообщения и параметры инициализации начального состояния генератора псевдослучайных числовых последовательностей, используемых при выборе элементов контейнера для стегоскрытия.

Основные этапы алгоритма ССИ отражены на обобщенных схемах встраивания и извлечения информации [8], приведенных в нотации языка UML на рис. 1. Далее рассмотрим каждый этап более подробно.

На первом этапе работы алгоритма встраивания реализуется подготовка скрываемых данных, включающая сжатие и шифрование файла-сообщения $W = AES_{K256}\left(DEFLATE\left(M\right)\right)$. Сжатие реализуется по алгоритму DEFLATE (библиотека zlib), а шифрование по алгоритму AES на 256-битном ключе. Использование процедур сжатия и шифрования позволяет не только повысить пропускную способность



а) *б)*

Рис. 1. Обобщенные схемы встраивания (а) и извлечения (б) данных из jpeg-контейнера

алгоритма и реализовать дополнительный уровень защиты скрываемых данных, но также способствует увеличению их стохастичности, что является немаловажным аспектом для последующих этапов работы алгоритма.

В начало W добавляется четырехбайтное значение $len = sizeof(W)$, хранящее размер самого сжатого и зашифрованного сообщения $W = len \| W$. Далее W представляется в виде последовательности n-битных слов (блоков) $\{w_1, w_2, \dots w_N\}$, $W = w_1 \| w_2 \| \dots w_N^*$, где w_N – добавленное необходимым числом нулей до кратности n содержимое последнего блока $w_N^* \in W$. Значение n определяет длину битовой последовательности, встраиваемой в контейнер за один шаг работы алгоритма и задается параметрически. Для простоты реализации n рассматривалось равным 4, 8, 16.

Параллельно с подготовкой скрываемых данных из сжатого JPEG-контейнера выделяются квантованные коэффициенты ДКП, используемые для ССИ. Для этого к I применяется декодирование по Хаффману и декодирование серий. Далее среди множества извлеченных коэффициентов формируются массивы $\{D_1, D_2, \dots D_N\}$, содержащие по L значений выбранных квантованных коэффициентов ДКП $D_i = (d_1, d_2, \dots d_L)_i$, $i = \overline{1, N}$. Обяза-

тельным условием при формировании массивов D_i является уникальность всех входящих в них коэффициентов. Это значит, что ни один из коэффициентов d_{ji}, $j=\overline{1,L}$, $i=\overline{1,N}$, не должен использоваться в процедуре ССИ более одного раза при скрытии любой пары n-битных слов из $\{w_1, w_2, \dots w_N\}$. С целью повышения защищенности процедуры скрытия и затруднения возможного анализа $\tilde{I}$, для наполнения массивов D_i спектральные коэффициенты могут выбираться не локально в блоках, а в псевдослучайном порядке равномерно по всему изображению.

На следующем шаге реализуется встраивание каждого n-битового слова w_i в соответствующий ему массив коэффициентов D_i, $i=\overline{1,N}$. Главная отличительная особенность предложенного алгоритма встраивания состоит в том, что элементы скрываемого сообщения напрямую не участвуют в преобразованиях с элементами контейнера (аддитивно, мультипликативно или путем перезаписи отдельных бит), а «кодируются» в D_i путем итеративного изменения отдельных его значений до того момента пока не будет получено совпадение значений w_i и результата вычисления функции-свертки H над модифицированным D_i.

Для модификации коэффициентов ДКП в D_i применяется функция F вида

$$D_i' = F(D_i, k) = \left(d_1 + s_{1,k}, d_2 + s_{2,k}, \dots d_L + s_{L,k}\right)_i, \quad (1)$$

которая, в зависимости от текущего значения переменной счетчика k, добавляет к коэффициентам d_j, $j=\overline{1,L}$ элементы вектора $S_k = \left(s_{1,k}, s_{2,k}, \dots s_{L,k}\right)^T$, где $s_{j,k}$ могут принимать значения $\{0, \pm1, \pm2, \dots \pm\nu\}$, ν – максимальное значение, добавляемое к одному коэффициенту (обычно $\nu \le 4$). Векторы S_k, $k=\overline{1,R}$ формируются таким образом, чтобы при малых k количество и уровень вносимых изменений в D_i были минимальными. С возрастанием k число одновременно модифицируемых коэффициентов в D_i, а также абсолютные значения приращений $s_{j,k}$ постепенно увеличиваются. Отметим, что для успешной работы алгоритма встраивания данных, количество векторов S_k, определяемое числом возможных неповторяющихся комбинаций значений приращений, должно быть много больше размерности пространства решений $R >> 2^L$. С целью уменьшения визуальной заметности факта ССИ при встраивании данных целесообразно пропускать блоки коэффициентов ДКП, соответствующие гладким областям изображения-носителя. Такие блоки характеризуются малым числом ненулевых коэффициентов в D_i.

В простейшем случае, не учитывающем порядок выбора коэффициентов в рамках D_i, выполняемые на начальных итерациях преобразования в функции F могут быть представлены в виде

$$F(D_i, k) = \begin{cases} 0 \le k < K_1: & d_p' = d_p \pm 1, \\ & p = \overline{1,L}; \\ K_1 \le k < K_2: & d_p' = d_p \pm 1, \\ & d_q' = d_q \pm 1, \\ & p,q = \overline{1,L},\ p \ne q; \\ K_2 \le k < K_3: & d_p' = d_p \pm 2, \\ & p = \overline{1,L}; \\ K_3 \le k < K_4: & d_p' = d_p \pm 1, \\ & d_q' = d_q \pm 2, \\ & p,q = \overline{1,L},\ p \ne q; \\ K_4 \le k < K_5: & d_p' = d_p \pm 1, \\ & d_q' = d_q \pm 1, \\ & d_r' = d_r \pm 1, \\ & p,q,r = \overline{1,L}, \\ & p \ne q \ne r; \\ \dots & \end{cases} \quad (2)$$

В зависимости от числа одновременно модифицируемых коэффициентов в D_i, а также от выбранных на текущей итерации значений приращений (одинаковых или различных), границы изменения индексов K_j определяются с использованием формул комбинаторики – числа сочетаний $C_b^a = b!/\left[a!(b-a)!\right]$ и числа размещений $A_b^a = b!/(b-a)!$ без повторений. Так, в (2) $K_1 = 2A_L^1$, $K_2 = K_1 + \left(2C_L^2 + A_L^2\right)$, … $K_5 = K_4 + \left(2C_L^3 + 2C_L^2 C_L^1\right)$.

Для реализации функции свертки H, применяемой к D_i', рассматривались:

– хеш-функции с финализацией, обеспечивающей требуемую длину хеш-кода, равную длине встраиваемого слова;

– циклические избыточные коды (CRC) с различными степенями порождающих полиномов.

Фрагмент сообщения w_i считается успешно встроенным в контейнер в случае если для текущего, искаженного функцией F, массива D_i выполняется

$$w_i = H\left(D_i'\right). \quad (3)$$

Фактически в цикле внесения искажений в D_i с последующим вычислением функции свертки решается задача поиска подходящего решения методом полного перебора с той разницей, что результат на выходе функции свертки не контролируется и на промежуточных итерациях до нахождения искомого D_i', удовлетворяющего (3), теоретически возможно получение коллизий. С учетом известного (приближенного к равномерному) распределения элементов в w_i и $H\left(D_i'\right)$ для нахождения искомого решения D_i' потребуется в среднем $2^{n-1}\left(1+2\varepsilon\right)$ итераций вызова искажающей функции F. Здесь ε характеризует среднюю частоту появления коллизий для заданного типа функции свертки и заданной в битах длины скрываемого слова. Вопросы, связанные выбором наилучшей функции свертки, минимизирующей число вызовов функции искажения, в данной работе не рассматривались, однако, с точки зрения производительности алгоритма скрытия, при встраивании n-битных слов большой длины ($n > 8$) в качестве H целесообразнее использовать более простые в вычислительном отношении циклические избыточные коды [8].

На завершающем этапе работы алгоритма (после встраивания всех w_i) элементы модифицированных массивов коэффициентов $\left\{D_1', D_2', \ldots D_N'\right\}$ записываются на свои исходные позиции в матрицах квантованных коэффициентов ДКП изображения. Элементы матриц выстраиваются в зигзагообразном порядке в одномерные массивы, к которым применяется однопроходное кодирование Хаффмана. В результате формируется заполненный JPEG-контейнер $\tilde{I}$.

2. АЛГОРИТМ ИЗВЛЕЧЕНИЯ СКРЫТЫХ ДАННЫХ

Схема работы алгоритма извлечения скрытой информации приведена на рис. 1б. На первом шаге выполняется частичное декодирование заполненного JPEG-контейнера и выделение квантованных коэффициентов ДКП. Далее на основе общего множества коэффициентов ДКП, формируются первые $V = 32/n$ массивов $\left\{D_1', D_2', \ldots D_V'\right\}$, каждый из которых включает по L коэффициентов, ранее использовавшихся при встраивании целочисленного значения длины сжатого и зашифрованного сообщения. Порядок следования элементов в D_i' должен в точности соответствовать исходному – заданному при скрытии. Для каждого D_i', $i = \overline{1,V}$ далее вычисляются функции свертки и формируется множество n-битных слов $\left\{w_1, w_2, \ldots w_V\right\}$, конкатенация которых позволяет получить значение длины скрытых данных $len = w_1 \| w_2 \| \ldots w_V$.

На следующем шаге с учетом полученной длины сообщения формируются массивы $\left\{D_{V+1}', D_{V+2}', \ldots D_N'\right\}$, включающие по L коэффициентов, ранее использовавшихся при встраивании сообщения. Для каждого D_i', $i = \overline{V+1, N}$ вычисляются функции свертки и формируется множество $\left\{w_{V+1}, w_{V+2}, \ldots w_N\right\}$, элементы которого последовательно объединяются, образуя промежуточное сообщение $W = w_{V+1} \| w_{V+2} \| \ldots w_N^*$ (w_N^* – скорректированное с учетом кратности len и n последнее извлеченное слово w_N). Далее W расшифровывается на секретном ключе и распаковывается по алгоритму INFLATE (библиотека zlib), в результате чего восстанавливается исходное сообщение $M = INFLATE\left(AES_{K256}^{-1}\left(W\right)\right)$.

В описанной схеме стеганографического кодирования число встраиваемых за один шаг битов сообщения n всегда превосходит число модифицируемых m в D_i (как правило $n >> m$), что позволяет существенно повысить ПС при сохранении визуальных искажений контейнера на низком уровне. На рис. 2а,б [8] приведен наглядный пример работы алгоритма. Для встраивания 16-битного слова w_i =0xC424 (11000100 00100100) использовался массив D_i из первых 28 коэффициентов ДКП,

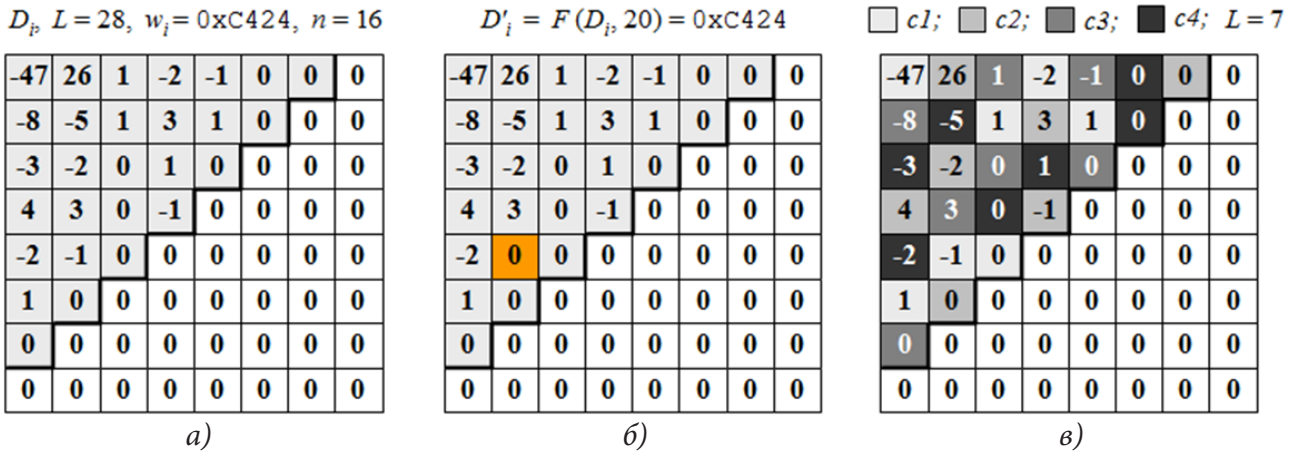


Рис. 2. Примеры блоков коэффициентов ДКП (а – блок до встраивания данных; б – блок после встраивания 16 бит данных; в – разметка блока при мультиплексировании каналов)

расположенных выше побочной диагонали и соответствующих низкочастотной (НЧ) и среднечастотной (СЧ) составляющей блока (рис. 2а). В качестве функции свертки H рассматривался циклический избыточный код CRC-16-CCITT. Искомые значения преобразованного по (2) массива коэффициентов D'_i, результат контрольной свертки которых совпадает со значением w_i, получаются на 20 итерации работы функции F. В данном примере для скрытия 16 бит информации потребовалась модификация лишь одного коэффициента из D_i (выделен цветом), что позволяет обеспечить минимальный уровень визуальных искажений в соответствующей данному блоку коэффициентов ДКП области на изображении.

3. МУЛЬТИПЛЕКСИРОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ

За счет реализуемых принципов встраивания информации предложенный алгоритм ССИ может успешно использоваться в режиме мультиплексирования нескольких скрытых каналов, обеспечивая высокий уровень ПС на канал при минимальных визуальных искажениях $\tilde{I}$. Применительно к задаче ССИ мультиплексирование скрытых каналов дает возможность одновременного использования одного контейнера несколькими независимыми пользователями. Для каждого пользователя выделяется свое непересекающееся с остальными множество элементов контейнера, используемое при встраивании и извлечении информации. Пример разметки блока коэффициентов ДКП при реализации четырех скрытых каналов $(c_1,\ldots c_4)$ приведен на рис. 2в. Здесь для встраивания пользовательской информации используются первые 28 коэффициентов ДКП каждого блока JPEG и на каждый канал выделяется по 7 коэффициентов, используемых при встраивании четырех n-битных слов. С учетом относительно небольшого числа доступных для модификации коэффициентов ДКП на один канал, для получения заполненного контейнера с минимальным уровнем визуальных искажений целесообразно выбирать малые значения n $(n \le 8)$. Выбор коэффициентов может осуществляться в соответствие с заранее сгенерированными случайными шаблонами, исключающими возможность пересечения значений из одного блока в разных каналах. Информация о конфигурации шаблона, т. е. о коэффициентах, с которыми работает пользователь, может являться компонентой стеганографического ключа.

Технология мультиплексирования стеганографических каналов дает возможность создавать скрытые электронные хранилища и системы скрытой передачи документов, доступные лишь авторизованным пользователям стеганографической системы. Для всех прочих пользователей скрытое электронное хранилище выступает в роли некоторого сервера, предоставляющего открытую информацию.

4. ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ АЛГОРИТМА ССИ

Экспериментальный анализ алгоритма ССИ проводился в части оценки пропускной способности и искажений, вносимых стогоалгоритмом, а также времени работы процедуры встраивания информации. Тестирование проводилось с использованием 30 JPEG-изображений фотографического качества размером 1200×1200 пикселей из тестового набора [9]. Согласно характеру содержимого тестовых изображений выборка была разбита на три группы по десять изображений в каждой. Первая группа $I_{(1)}$ включала гладкие изображения с большими участки плавного перехода цвета, вторая $I_{(2)}$ – изображения смешанного типа, содержащие контрастные и монотонные области, третья $I_{(3)}$ – контрастные, пестрые изображения. Для оценки уровня искажений использовался показатель пикового отношения сигнала к шуму (PSNR). Коэффициент скрытия определялся как отношение размера сжатого и зашифрованного скрываемого сообщения к размеру всего JPEG-контейнера $KC=|W|/|I|$. Зависимости усредненных по тестовым выборкам $I_{(1)}$–$I_{(3)}$ значений PSNR и KC от длины встраиваемых битовых слов n и числа коэффициентов ДКП L в модифицируемой группе D_i, приведены на рис. 3. При проведении тестирования встраивание данных реализовывалось в первые $V=28$ элементов каждого блока коэффициентов ДКП JPEG-контейнера (рис. 2а). Значения на графиках, соответствующие $n=8,\ L=7$ (по оси X), получены в режиме мультиплексирования скрытых каналов при одновременном встраивании четырех 8-битных слов в первые 28 коэффициентов ДКП блока.

Максимальные значения коэффициента скрытия (порядка 0.5) были получены в режиме мультиплексирования скрытых каналов, при этом значения $PSNR$ составили порядка 35 дБ, что свидетельствует о достаточно высоком качестве заполненных контейнеров. При встраивании 16-битных слов в группы из 28 коэффициентов без существенных визуально заметных искажений возможно скрытие сообщений размером порядка 20–30 % от размера самого JPEFG-контенйера. Наилучшее перцептивное качество заполненных контейнеров ожидаемо получается при скрытии битовых слов малой длины. Значения уровня искажений, полученные для гладких изображений из тестовой группы $I_{(1)}$, в среднем превышали аналогичные значения, полученные для контрастных кадров из $I_{(3)}$. Блоки квантованных коэффициентов ДКП на гладких участках кадра, характеризуются мень-

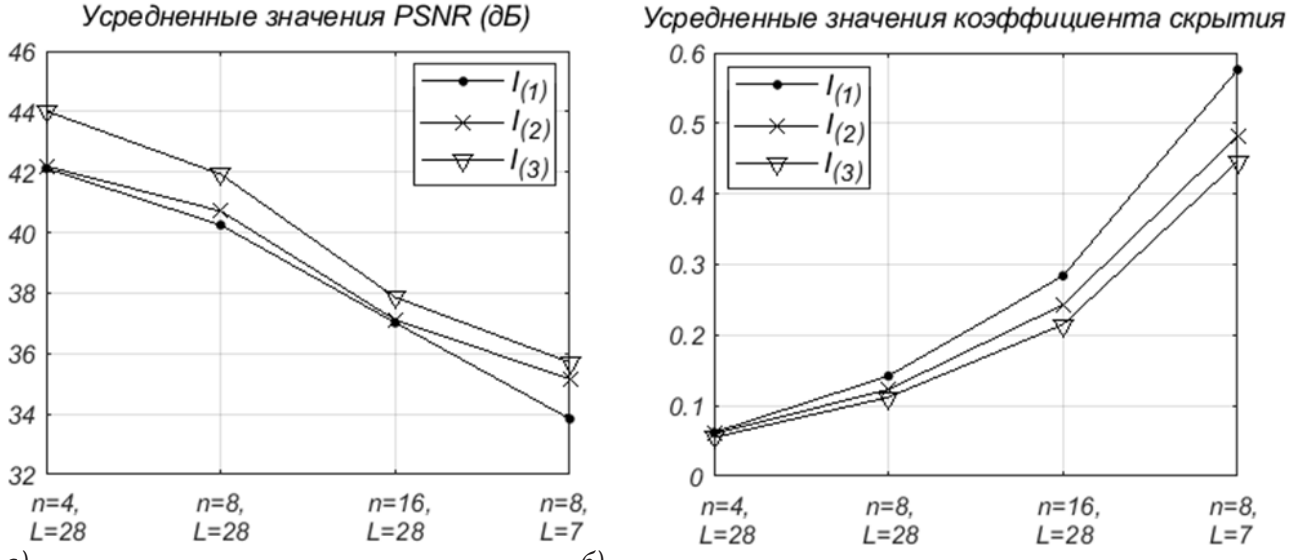


Рис. 3. Зависимости усредненных значений пикового отношения сигнал-шум (а) и коэффициента скрытия (б) от длины встраиваемых битовых слов n и числа коэффициентов ДКП L в модифицируемой группе ($V=28$)

шим числом отличных от нуля коэффициентов, поэтому вносимые функцией F модификации приводят к появлению более значимых локальных искажений при встраивании длинных битовых слов или мультиплексировании каналов.

С учетом специфики реализованного алгоритма скрытия, предусматривающего многократное применение искажающей функции F по отношению к массиву коэффициентов ДКП D_i при встраивании одного n-битного слова, важным оцениваемым показателем является время, затрачиваемое на создание заполненного контейнера $\tilde{I}$. На рис. 4а в логарифмическом масштабе приведены результаты оценки среднего числа вызовов функции искажения F необходимого для встраивания одного n-битного слова, а на рис. 4б приведены усредненные значения времени создания $\tilde{I}$ размером 1200×1200 пикселей. Для кадров из разных тестовых выборок $I_{(1)}-I_{(3)}$ значения среднего числа вызовов F и среднего времени скрытия были примерно одинаковыми, поэтому на рис. 4 приводятся усредненные значения по всем 30 кадрам тестового набора. Результаты получены при использовании в (3) функции свертки CRC-16-CCITT, а также при условии использования всего доступного пространства стегоскрытия каждого контейнера. Характеристики ЭВМ, использованной для тестирования: процессор Intel Core i5-2500 CPU @ 3.30 GHz 3.60 GHz, ОЗУ 4 ГБ.

При встраивании 8-битых слов среднее количество вызовов функции искажения F составило порядка 268, что соответствует модификации 2 бит для всех коэффициентов группы, при этом среднее время создания $\tilde{I}$ составляет 0.78 сек. При встраивании 16-битых слов среднее количество вызовов функции F составляет уже порядка 67320, что соответствует модификации 4–5 бит для коэффициентов группы, а среднее время создания $\tilde{I}$ составляет порядка 186 сек. В режиме мультиплексирования ($n=8,\ L=7$) создание $\tilde{I}$ происходит за 3.15 сек., при этом обеспечивается максимальный КС при сохранении высокого качества заполненного контейнера. Исходя из этого можно сделать вывод о нецелесообразности встраивания сообщений длинными ($n>16$) битовыми словами, а также о необходимости использования меньше-

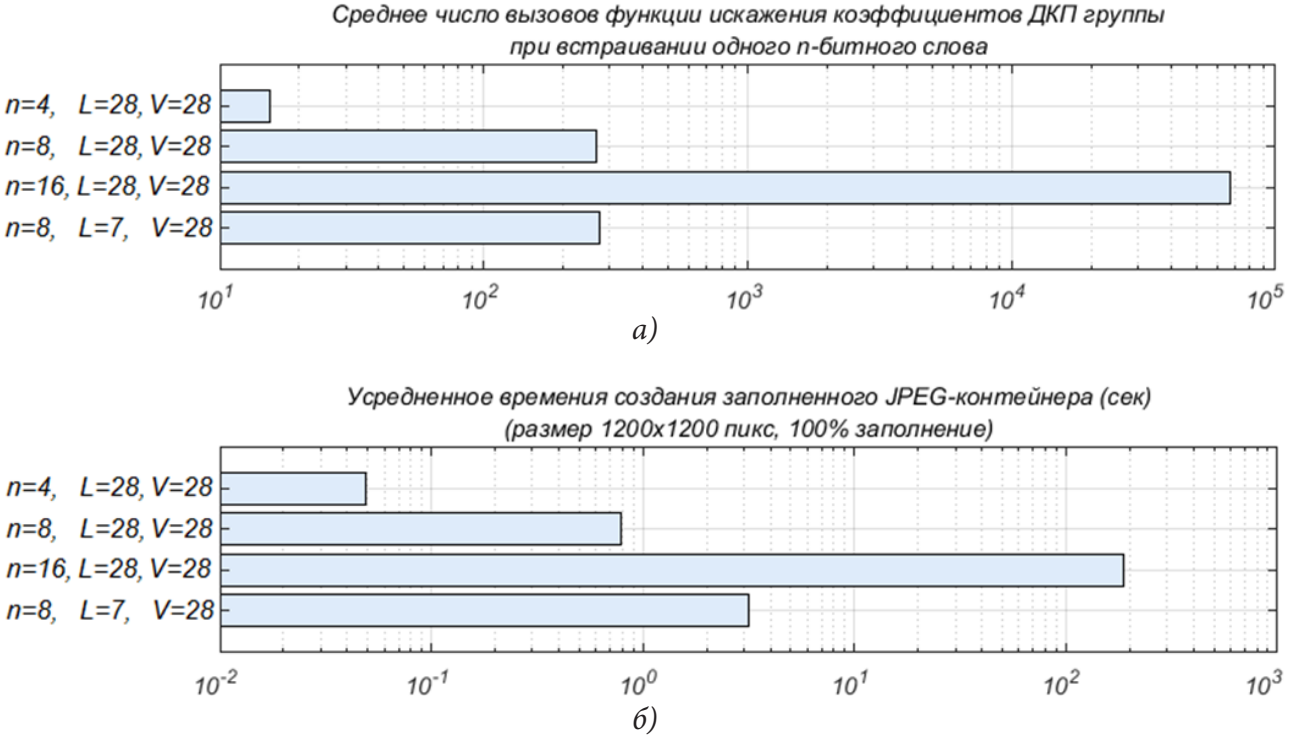


Рис. 4 Результаты оценки среднего числа вызовов функции искажения при встраивании одного n-битного слов (а) и усредненного времени создания заполненного контейнера для различных значений n и L

го числа коэффициентов ДКП в модифицируемых группах D_i при скрытии двух- трех-байтовых слов.

Усредненные значения времени встраивания были получены для нераспараллеленной версии алгоритма. Необходимо отметить, что специфика предложенного алгоритма ССИ позволяет эффективно организовать параллельную обработку на уровне CPU или GPU (вычисление функций искажения и свертки реализуется независимо для каждой группы коэффициентов D_i), что позволит многократно сократить общее время встраивания данных.

ЗАКЛЮЧЕНИЕ

В работе рассмотрен алгоритм ССИ в JPEG, совмещающий в себе два важных свойства – высокую пропускную способность и низкую визуальную заметность скрытых данных. Отличительной особенностью предложенного алгоритма является способ стеганографического кодирования данных, при котором элементы сообщения в явном виде (аддитивно, мультипликативно) не «подмешиваются» в структуру контейнера, что потенциально положительно отражается на статистической незаметности скрытых сообщений. При работе с JPEG-контейнерами алгоритм позволяет встраивать в них сжатые сообщения размером до 50–60 % от размера самих контейнеров, в то время как большинство известных JSteg-подобных алгоритмов способны скрывать сообщения размером лишь 5–15 % от размера контейнера. Реализуемые алгоритмом принципы встраивания информации позволяют успешно использовать его в режиме мультиплексирования нескольких скрытых каналов. Также предложенный алгоритм ССИ может быть использован в алгоритмах «самореконструирующей» стеганографии [10] с целью максимизации площадей искажаемых и реконструируемых областей.

СПИСОК ЛИТЕРАТУРЫ

1. *Westfeld, A.* High capacity despite better steganalysis (F5 – a steganographic algorithm) / A. Westfeld // in: Proceedings of the Fourth International Workshop on Information Hiding. – 2001 – Vol. 2137. – P. 289–302.

2. *Provos, N.* Defending against statistical steganalysis / N. Provos // in: Proceedings of the 10th USENIX Security Symposium. – 2001. – P. 323–336.

3. *Morsy, H. A.* JPEG Steganography System with Minimal Changes to the Quantized DCT Coefficients / Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer // International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307. – 2012. – Vol. 1(6).

4. *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.

5. *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.

6. *Koch, E.* Towards Robust and Hidden Image Copyright Labeling / E. Koch, J. Zhao // IEEE Workshop on Nonlinear Signal and Image Processing, Greece. –1995. – P. 123–132.

7. *Bansal, D.* An Improved DCT based Steganography Technique / D. Bansal, R. Chhikara // International Journal of Computer Applications. – 2014. –Vol. 102(14). – P. 46–49.

8. *Дрюченко, М. А.* Стегоалгоритм повышенной пропускной способности для скрытия данных в графические контейнеры с использованием функций свертки / М. А. Дрюченко // Математическое моделирование и информационные технологии в инженерных и бизнес приложениях : сб. тр. Междунар. науч. конф. (Воронеж, 6–7 сентября 2018 г.). – Воронеж, 2018. – С. 196–209.

9. Набор тестовых изображений «TEST-IMAGES». – Режим доступа: http://testimages.tecnick.com. – (дата обращения 27.09.2018).

10. *Дрюченко, М. А.* Принципы самореконструирующей стеганографии и защита цифровых изображений / М. А. Дрюченко // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2015. – № 3. – С. 51–61.

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

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