электронный научно-технический журнал
ИНЖЕНЕРНЫЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51036. ISSN 2307-0595

Метод сокрытия информации в квантованных коэффициентах дискретного косинус преобразования

 # 08, август 2016

Филиппов М. В.[1], Балашова С. А.[1,*]

УДК: 519.688

[1]Россия, МГТУ им. Н.Э. Баумана
*balashovasofya@gmail.com

Введение

Информация является одним из важнейших предметов современной жизни. В настоящее время происходит активное развитие сетевых технологий. Как следствие этого большое количество информации передается по сетям [1-3]. При этом возрастает процент атак злоумышленников и попыток несанкционированного доступа к передаваемой информации. Поэтому появилась необходимость защиты информации от несанкционированного доступа.

Существует два подхода к решению данной проблемы: шифрование информации и стеганография.

Криптографическая защита информации (шифрование) не снимает проблему полностью. При этом подходе защищается само содержание сообщения. Наличие шифрованного сообщения вызывает подозрение и желание расшифровать передаваемое сообщение или же изменить его с целью сделать невозможным будущее дешифрование. К тому же в ряде стран действуют запреты на использование криптографических средств [1].

Второй подход – стеганография – основан на сокрытии самого факта передачи секретного сообщения. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания.

В большинстве случаев сокрытие информации осуществляется в графических и звуковых файлах [4]. Отличительной особенностью таких файлов является сжатие данных, что позволяет при сохранении качества информации сократить ее объем. Многие распространенные форматы файлов, в т.ч. формат JPEG, MP3, используют сжатие данных с потерей информации. Существующие методы сокрытия информации либо не устойчивы к сжатию, либо устойчивы при малых степенях сжатия [5-6]. Поэтому возникла необходимость создания метода во всех случаях устойчивого к сжатию.

В данной статье проведен анализ стеганографических методов сокрытия данных в изображениях формата JPEG. Показано преимущество частотных методов над пространственными с точки зрения устойчивости к сжатию. На основе частотных методов разрабо-

тан алгоритм сокрытия в спектральных коэффициентах файла формата JPEG, который обеспечивает 100% восстановление встраиваемых данных.

1. Обзор известных стеганографических методов

В настоящее время существует большое разнообразие стеганографических алгоритмов. Методы компьютерной стеганографии делятся на три основные группы:

1. Методы сокрытия, основанные на использовании специальных свойств компьютерных форматов;
2. Методы сокрытия в пространственной области;
3. Методы сокрытия в частотной области.

Достоинством методов 1-ой группы является простота использования. Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой [1,2]. Но такие методы обеспечивают низкую степень скрытности и слабую производительность. Объем передаваемых данных достаточно ограничен.

Методы 2-ой группы основаны на встраивании скрываемых данных в области первичного изображения. Преимущество таких методов заключается в том, что для встраивания информации не требуются сложные математические операции и длительные преобразования изображения [2].

Примером реализации такого подхода может выступать метод LSB (Least Significant Bit, наименьший значащий бит), наиболее распространенный среди методов замены в пространственной области. Суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека. Недостатком же метода LSB является неустойчивость его к обработке файла-контейнера, что делает невозможным его использование в сокрытии данных в файле, который в дальнейшем подвергается сжатию.

Более стойкими к искажениям, в том числе и компрессии, являются методы, использующие частотную область контейнера для сокрытия информации, так как они работают с уже преобразованными каналами данных.

Существует несколько способов представления изображения в частотной области. При этом используется определенная декомпозиция изображения, используемого в качестве контейнера. Например, существуют методы на основе дискретно косинусного преобразования (ДКП), дискретного преобразования Фурье (ДПФ), вейвлет-преобразования, преобразования Карунена-Лоева и т.д. [7]. Подобные преобразования могут применяться как к отдельным частям изображения, так и к изображению в целом.

Наибольшее распространение среди всех ортогональных преобразований в стеганографии получили вейвлет-преобразования и ДКП. Это объясняется значительным распространением их использования при компрессии изображений. Кроме того, для скрытия данных целесообразно применять именно то преобразование контейнера, которому он бу-

дет подвергаться в известных алгоритмах компрессии. Например, алгоритм ДКП является базовым в стандарте JPEG, а вейвлет-преобразования – в стандарте JPEG2000.

Одним из самых известных стеганографических методов является метод Коха и Жао – метод относительной замены величин коэффициентов ДКП [8]. В данном алгоритме, происходит внедрение бит водяных знаков в блоки изображения размером 8 х 8 пикселей (1 бит на блок). При этом в качестве сообщения может использоваться как монохромное изображение, так и некая последовательность {0,1}, состоящая из произвольного количества чисел.

Данный алгоритм предусматривает, что получателю должны быть известны помимо контейнера со встроенными данными и его размерности алгоритм скрытия данных, размерность сегментов, на которые разбивался контейнер и матричные координаты коэффициентов косинусных функций, которые использовались для скрытия. При извлечении данных из изображения производится повторное ДКП и сравнение выбранных коэффициентов по правилу, использовавшемуся при сокрытии данных.

Таким образом, оригинальное изображение искажается за счет внесения изменений в коэффициенты ДКП, если их относительная величина не отвечает скрываемому биту. Чем больше значение P, тем сокрытие является более стойким к сжатию, однако качество изображения при этом значительно ухудшается. И наоборот, чем меньше P, тем менее заметно наличие информации в контейнере, но тем большее количество ошибок в извлеченной информации.

Другим распространенным стеганографическим методом является метод Фридрих. В отличие от предыдущего алгоритма Коха и Жао, в котором ДКП производится поблочно, в алгоритме Фридрих ДКП происходит для всего защищаемого изображения. Скрываемое сообщение представляет собой последовательность {-1, 1} [9-12].

В этом алгоритме данные встраиваются в изображение двумя различными способами в зависимости от того, в каких коэффициентах ДКП происходит сокрытие – в среднечастотных или в низкочастотных. В этом алгоритме имеет место тот же недостаток: стойкость алгоритма к сжатию уменьшается с увеличением емкости контейнера.

Аналогичный недостаток характерен и для других алгоритмов [1-3], использующих сокрытие в коэффициентах спектральных преобразований.

Следует также отметить присущее описанным выше алгоритмам значительное ухудшение точности восстановленных данных при увеличении степени сжатия.

2. Описание формата JPEG

Для того, чтобы выяснить принципы неустойчивости по отношению к сжатию описанных в предыдущем разделе алгоритмов, рассмотрим подробно стандартный метод JPEG.

Предназначенные для использования в электронных средствах массовой информации не анимированные полутоновые и полноцветные фотографии обычно сохраняют в цифровых форматах PNG и JPEG. К достоинствам этих форматов можно отнести кроссплатформенность, возможность обработки практически во всех графических редакторах, хорошие

показатели качества изображений. Изображения в формате JPEG за счёт возможности их сжатия с потерями имеют меньший размер по сравнению с аналогичными, сохранёнными в формате PNG. Следовательно, использование формата JPEG для сохранения и передачи изображений является более предпочтительным [2].

Процесс сжатия JPEG состоит из следующих этапов [13]:

1. Прореживание каналов. Эта стадия является необязательной, в разрабатываемом алгоритме она опускается.

2. Переход из системы RGB в систему YCrCb осуществляется по следующим соотношениям:

$$Y = 0 + 0.299 \cdot R + 0.587 \cdot G + 0.114 \cdot B$$
$$Cb = 128 - 0.168736 \cdot R - 0.331264 \cdot G + 0.5 \cdot B$$
$$Cr = 128 + 0.5 \cdot R - 0.418688 \cdot G - 0.081312 \cdot B$$

3. Дискретно-косинусное преобразование (далее ДКП) блока производится по следующей формуле:

$$DCT(u,v) = C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)v}{2M}$$
$$u = 0,1 \dots N-1; \quad v = 0,1 \dots M-1$$

$$C(u), C(v) = \begin{cases} \sqrt{\frac{1}{N}}, u = 0; \\ \sqrt{\frac{2}{N}}, \text{иначе} \end{cases}$$

В разрабатываемом алгоритме предполагается, что N=M=8.

4. Квантование коэффициентов ДКП. Процесс квантования играет ключевую роль в JPEG сжатии, так как в ходе него удаляются высокие частоты, представленные в исходном изображении и отвечающие за высокую детализацию. Этот шаг связан в тем, что глаз более чувствителен к низким частотам, чем к высоким. Таким образом, данная операция не ведет к заметному искажению изображения. Квантование – это процесс деления рабочей матрицы на матрицу квантования поэлементно:

$$R_{ij} = \left[\frac{DCT_{ij}}{Q_{ij}}\right], \; i,j = 1..8,$$

где $Q_{8\times8}$ - матрица квантования, $DCT_{8\times8}$ - блок коэфф-тов ДКП, квантованный блок - $R_{8\times8}$, квадратные скобки [ ] означают взятие целой части числа. Для каждой компоненты (Y, Cr и Cb), в общем случае, задается своя матрица квантования. Матрицы квантования для яркостной и цветовой компонент установлены стандартом JPEG для коэффициента сжатия 50%. Для произвольного коэффициента качества K каждый элемент q матриц квантования нужно преобразовать по следующим соотношениям:

$$\begin{cases} q = \frac{(100-K)}{50}, & \text{при } K \geq 50 \\ q = \frac{50}{K}, & \text{при } K < 50 \end{cases}$$

Ошибки восстановления в существующих методах, описанных в предыдущем разделе, появляются из-за того, что при квантовании теряется часть сокрытой в коэффициентах ДКП информации. Поэтому в представленном в данной статье алгоритме, встраивание данных будет производиться после этапа квантования в коэффициенты R_{ij} формулы. Так как изменение цветовой компоненты пиксела менее ощутима для органов восприятия человека, то сокрытие сообщения будет производиться в цветовых каналах изображения (Cr и Cb).

3. Принцип сокрытия информации

Как было отмечено ранее, алгоритм сокрытия информации в коэффициентах спектральных преобразований изображения должен отвечать двум критериям: стойкость к компрессии и незаметность [5].

Первое свойство достигается тем, что непосредственно встраивание данных происходит в квантованные коэффициенты ДКП, что предотвращает потерю информации. Обеспечение второго свойства сводится к задаче выбора коэффициентов ДКП для встраивания бит сообщения [8].

Пусть количество коэффициентов R_{ij} в формуле, отличных от 0, равно n. Выполнив однополяризацию матрицы R_{ij} алгоритмом «змейка» и оставив только ненулевые коэффициенты, получим последовательность $\{u_l\}$, где $l = 1,2, \dots, n$.

Положим, что отправитель хочет передать q бит сообщения $m = \{m_1, \dots m_q\}^T$. Отправитель и получатель договариваются о секретном ключе, который используется для создания псевдо-случайной бинарной матрицы D размерностью $q \times n$ где n - количество коэффициентов ДКП. Множество $C \subset \{1, \dots, n\}$ – индексы коэффициентов ДКП $u_j, j \in C$, в значения которых будут модифицироваться. Пусть количество таких коэффициентов равно $k < n$.

Отправитель определяет отображение $Q(u_i) = x_i$, переводящее последовательность коэффициентов u_j в последовательность бит $x_i \in \{0,1\}$. Закон преобразования Q сообщается получателю. Из n полученных бит $\{x_i\}$ k будут модифицированы согласно описанной ниже процедуре. В результате получим последовательность бит $\{y_i\}, i = 1,2, \dots, n$.

Для определения k модифицированных бит составим систему

$$Dy=m \quad (1)$$

из q линейных уравнений. Решение данной системы ищется в поле Галуа $GF(2)$, т.е. согласно двоичной арифметике по модулю 2. Это решение определяет значения бит, на которые изменяются соответствующие квантованные коэффициенты ДКП u_j.

В работе [9] показано, что система (1) имеет решение с вероятностью 1-$O(2^{q-k})$.

В результате получаем набор модифицированных коэффициентов u'_j, из которых формируется изображение-контейнер.

Декодирование представляет собой обратную операцию. Получатель знает бинарную матрицу D, составляет вектор u' и производит операцию умножения в $GF(2)$ по следующей формуле:

$$m = Du'$$

В процессе выполнения операций встраивания информации и извлечения происходит потеря дробной части в двух случаях. Во-первых, при выполнении операции квантования. Во-вторых, в процессе формирования контейнера после выполнения обратного ДКП. Возможность появления указанных погрешностей отмечена в работе [9].

Эти погрешности приводят к изменению значений пикселей исходного изображения. Для того, чтобы избежать ошибок восстановления скрытых сообщений, в работе предлагается при выборе коэффициентов ДКП для встраивания бит использовать пороговые значения: встраивание бит будет производиться только в тех коэффициентах, значение которых выше *B*. Таким образом, отбрасываются коэффициенты ДКП, значения которых после квантования малы. В каждом блоке ДКП выбирается два таких коэффициента.

4. Разработанный алгоритм

Для проведения сокрытия данных входное изображение модифицируется согласно пунктам 1 - 4, описанных в разделе 2.

Алгоритм сокрытия данных основывается на методе, описанном выше.

Сокрытие производится поблочно, в каждом блоке скрывается два бита сообщения в двух коэффициентах ДКП блока соответственно. Для выбора набора подходящих для сокрытия коэффициентов используется пороговое значение. Выбор двух коэффициентов для сокрытия информации производится в соответствии с решением СЛАУ в $GF(2)$. Предварительно формируется бинарная матрица с использованием секретного ключа, известного получателю.

Непосредственно встраивание бит данных выполняется в отобранных коэффициентах ДКП с использованием алгоритма «Наименьшего значащего бита». Сокрытие производится в последнем бите числа.

Алгоритм извлечения ЦВЗ из каналов Cr и Cb изображения также основан на решении СЛАУ в $GF(2)$.

Извлечение производится поблочно, из каждого блока последовательно извлекаются два бита сообщения из двух коэффициентов ДКП блока. Соответствующие коэффициенты определяются решением СЛАУ. Предварительно формируется бинарная матрица с использованием секретного ключа, известного получателю. Та же матрица использовалась отправителем для сокрытия информации.

Данный алгоритм направлен на то, чтобы сделать схему сокрытия более разреженной. Так как методы определения факта сокрытия информации в файле основаны на статистическом анализе содержимого контейнера, для обеспечения его незаметности необходимо использовать методы, делающие модель менее регулярной. Тем самым обеспечивается малозаметность передачи сообщения.

5. Экспериментальное исследование

Для исследования работоспособности рассмотренного алгоритма была проведена серия испытаний для цветных изображений разного размера и скрываемых сообщений различной длины.

Первая группа этого эксперимента определяет степень неизменности встроенных сообщений. Исходное изображение цветное, размер его фиксирован. Исследована зависимость пикового отношения сигнал-шум (PSNR) от коэффициента качества сжатия при одинаковой длине сообщения.

Критерий PSNR наиболее часто используется для измерения уровня искажений изображений и определяется по формуле:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

где MAX_I – максимальное значение, принимаемое пикселем изображения (при разрядности 8 бит $MAX_I = 255$), а MSE – среднеквадратичная ошибка для изображений I и K размера $m \times n$, вычисляемая по формуле:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|I(i,j) - K(i,j)|^2$$

Результаты исследования приведены на рис. 1. Области на оси X соответствуют коэффициентам сжатия, значения оси Y соответствуют значениям PSNR.

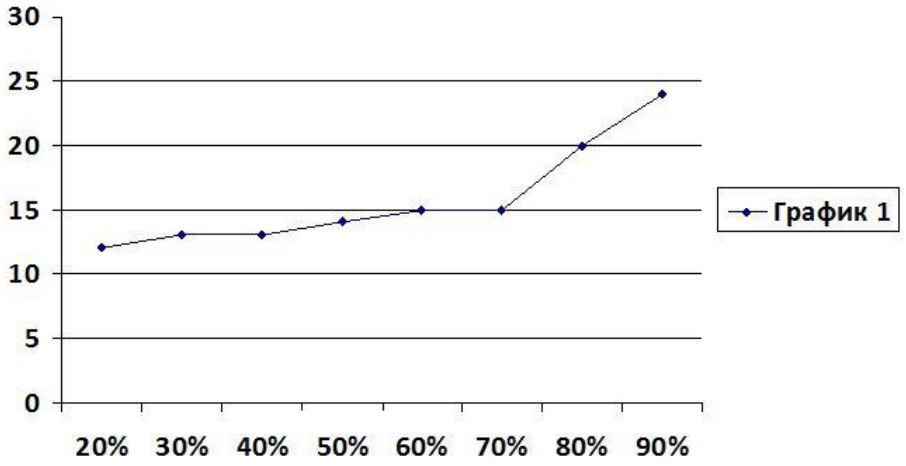

Рис. 1. Результаты эксперимента 1

Как видно из графика существует прямая зависимость между коэффициентом сжатия и значением оценки PSNR. Наилучшие результаты были достигнуты при использовании коэффициента выше 80%, а наихудшие – при 20% - 40%.

Во второй группе экспериментов исследовалась зависимость критерия PSNR от длины встроенного сообщения. Исходное изображение является цветным, размер его фиксирован. Изменялась длина встроенного сообщения при фиксированном коэффициенте качества сжатия. В эксперименте был выбран коэффициент сжатия 80%.

Результаты исследования приведены на рис. 2. Области на оси X соответствуют длинам сообщения в символах, значения оси Y соответствуют значениям PSNR.

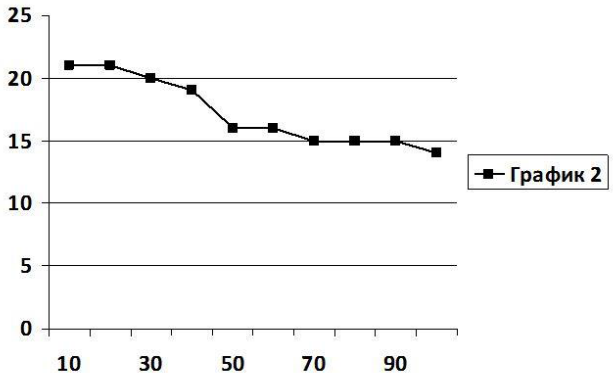

Рис. 2. Результаты эксперимента 2

Как видно из графика существует обратная зависимость между длиной сообщения и значением оценки PSNR. При встраивании небольшого сообщения (до 30 символов) достигается наилучшая оценка, а наихудшая – начиная от 70 символов.

Для определения точности извлечения данных использовался критерий BER - вероятность битовой ошибки, который показывает отношение числа битовых ошибок к числу переданных битов.

Реализованный алгоритм обеспечивает 100%-ную точность извлечения данных. Для ее определения использовалась оценка BER, определяемая по формуле

$$BER = \frac{N_e}{N}$$

где N_e – кол-во ошибочных бит, N – кол-во переданных бит.

Во всех случаях равно 0%. В случаях, когда размер сообщения превышает предельно допустимый, вычисление BER является некорректной задачей, так как размеры исходной и извлеченной строки не совпадают. Следовательно, такие случаи не рассматривались в ходе эксперимента.

В случае встраивания информации во все квантованные коэффициенты, в том числе, и меньшие порогового значения, точность извлечения составляла порядка 95%.

Также при оценке алгоритма оценивался визуальный критерий незаметности передачи сообщения [11]. На рисунках 3-7 представлены изображений, получавшиеся при сокрытии одного и того же сообщения, но при разной степени компрессии. Как видно из рисунков, при коэффициенте сжатия ниже 60% видны артефакты сокрытия сообщения.

Рис. 3. Изображение с коэффициентом сжатия 20%

Рис. 4. Изображение с коэффициентом сжатия 30%

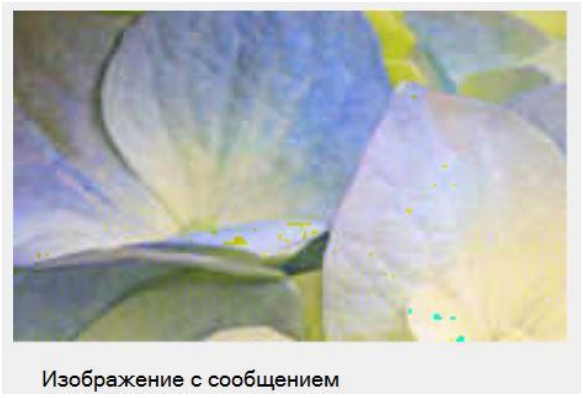

Рис. 5. Изображение с коэффициентом сжатия 50%

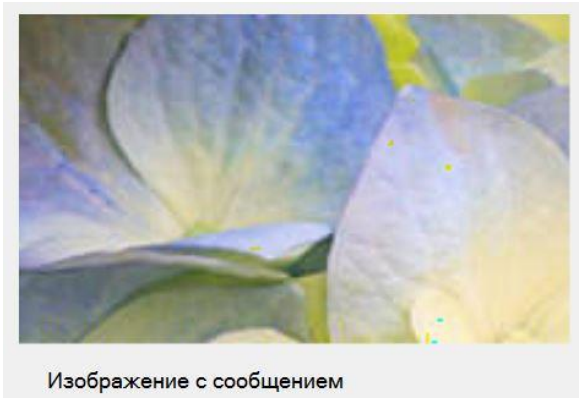

Рис. 6. Изображение с коэффициентом сжатия 60%

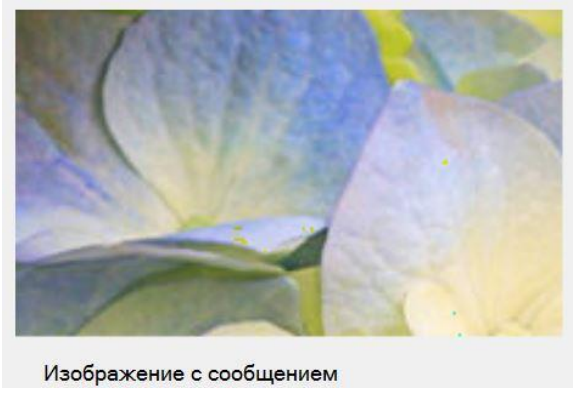

Рис. 7. Изображение с коэффициентом сжатия 80%

Заключение

В статье представлен разработанный алгоритм сокрытия информации в спектральных коэффициентах файла формата JPEG. Проведены исследования по критериям точности извлечения данных и незаметности передаваемого сообщения, которые показали, что разработанный алгоритм обеспечивает полное восстановление скрытой информации. В дальнейшем предполагается адаптация алгоритма для аудиофайлов, в частности к файлам формата MP3.

Список литературы

[1]. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс. 2009. 265 с.

[2]. Грибунин В.Г., Агрsuperновский А.В., Балакин А.В., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга. 2009. 220 с.

[3]. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс. 2006. 288 с.

[4]. Иконникова К.А., Филиппов М.В. Алгоритм сокрытия информации в коэффициентах МДКП WAV файлов. // Технология инженерных и информационных систем. 2016. № 1. С. 30-37

[5]. Михайличенко О.В. Методы и алгоритмы защиты цифровых водяных знаков при JPEG сжатии: дис. … канд. техн. наук. СПб.: Университет ИТМО. 2009. 115 с.

[6]. Коробейников А.Г., Прохожев Н.Н., Михайличенко О.В., Хоанг З. Выбор коэффициентов матрицы дискретно-косинусного преобразования при построении стеганографических систем. // Вестник компьютерных и информационных технологий. М.: Машиностроение. 2008. Вып.11. С.12-17.

[7]. Светов Л.А. Встраивание цифрового водяного знака в аудиосигнал с применением быстрого преобразования Фурье // Электронный журнал "Системный анализ в науке и образовании". 2013. № 2. Режим доступа: http://sanse.ru/download/168 (дата обращения: 4.07.2016)

[8]. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling // IEEE Workshop on Nonlinear Signal and Image Processing. (Neos Marmaras, Greece, June 20-22, 1995). 1995. P. 452-455. Режим доступа: https://scholar.google.ru/scholar?oi=bibs&cluster=16757936004491706508&btnI=1&hl=fi (дата обращения: 4.07.2016)

[9]. Fridrich J. Combining low-frequency and spread spectrum watermarking // Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption. San Diego, CA, USA. 1998. Vol. 3456. P. 2-12. DOI: 10.1117/12.330355. Режим доступа: http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=958610 (дата обращения: 4.07.2016)

[10]. Fridrich J., Goljan M., Soukal D. Efficient Wet Paper Codes. // Information Hiding. 7th International Workshop, IH 2005. (Barcelona, Spain, June 6-8, 2005. Revised Selected Papers, LNCS).

Berlin: Springer-Verlag Heidelberg. 2005. Vol. 3727. P. 204-218. DOI: 10.1007/11558859_16. Режим доступа: http://link.springer.com/chapter/10.1007%2F11558859_16 (дата обращения: 4.07.2016)

[11]. Fridrich J., Goljan M., Soukal D. Perturbed Quantization Steganography with Wet Paper Codes. // Proceedings ACM Multimedia Security Workshop. (Magdeburg, Germany, September 20-21). 2004. P. 4-15. Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/versions?doi=10.1.1.160.3462 (дата обращения: 4.07.2016)

[12]. Fridrich J., Goljan M., Soukal D. Steganography via codes for memory with defective cells. // Proceedings of the 43rd Annual Allerton Conference On Communication, Control, and Computing. 7th International Workshop, IH 2005. (Barcelona, Spain, June 6-8, 2005). 2005. Vol. 5681. P. 631-642. Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.160.4787 (дата обращения: 4.07.2016)

[13]. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера. 2005. 1072 с.