**УДК 681.3**

# СКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ НА ОСНОВЕ СПЕКТРАЛЬНЫХ ПРЕОБРАЗОВАНИЙ

***канд. техн. наук, доц. Р.П. БОГУШ***
***(Полоцкий государственный университет)***

*Предлагается стеганографическая система скрытия информации, представленной в виде изображения, в цветных статических изображениях. Для сокрытия информации используется дискретное косинусное преобразование либо двумерное вейвлет-преобразование, адаптированные к современным алгоритмам сжатия изображений JPEG и JPEG2000 соответственно. Для повышения устойчивости к алгоритмам сжатия внедрение осуществляется в низкочастотную область цифрового контейнера. Криптостойкость системы обеспечивается применением ассиметричного алгоритма RSA при внедрении информации в изображение. Рассматриваются вопросы эффективности и робастности предлагаемой системы. Представлены результаты исследований, которые подтвердили эффективность применения данной стегосистемы и показали ее перспективность для использования в системах скрытой передачи информации, системах встраивания цифровых водяных знаков и идентификационных номеров.*

**Введение.** В настоящее время бурно развивается такое направление защиты информации от несанкционированного доступа, как цифровая стеганография. Это связано с развитием мультимедийных технологий, сети Internet, с непрерывным совершенствованием компьютерной техники, методов и алгоритмов обработки цифровой информации и с тем, что стеганография позволяет обеспечивать обмен конфиденциальной информацией таким образом, что скрывается сам факт передачи такой информации. В отличие от криптографии, где точно можно определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в открытые так, чтобы невозможно было определить существование встроенных секретных данных.

Цифровая стеганография включает следующие основные направления [1]:

- встраивание информации с целью ее скрытой передачи;
- встраивание цифровых водяных знаков;
- встраивание идентификационных номеров;
- встраивание заголовков.

В цифровой стеганографии используются следующие основные термины [1, 2]:

- стегосистема – система скрытия данных на основе стеганографии;
- цифровой контейнер – любая цифровая информация, предназначенная для сокрытия конфиденциальных сообщений;
- скрытое сообщение – сообщение, встраиваемое в контейнер;
- стегоконтейнер – контейнер с внедренным в него скрытым сообщением.

Значительное влияние на безопасность и удобство работы стегосистемы оказывает используемый цифровой контейнер. Среди ряда возможных стегоконтейнеров (звук, статические и динамические изображения) наиболее широко используются статические изображения. Это обусловлено наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации; слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержанию в нем шума, искажениям вблизи контуров; бурно развивающимися методами цифровой обработки изображений и т.д.

Стегосистема, использующая в качестве цифрового контейнера статическое изображение, должна удовлетворять следующим основным требованиям: свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле, что необходимо для обеспечения беспрепятственного прохождения стегоконтейнера по каналу связи, т.е. не должно привлекаться внимание атакующего; стегоконтейнер должен быть устойчив к искажениям, в том числе и преднамеренным, так как в процессе передачи он может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т.д. Кроме того, стегоконтейнер может быть сжат, в том числе и с использованием алгоритмов сжатия с потерей данных (JPEG, JPEG-2000). В настоящее время существует широкий спектр стеганографических систем [1 – 5], однако совершенствование методов обработки и сжатия изображений требует непрерывного развития и стегосистем, чтобы удовлетворять предъявляемым требованиям и обеспечивать робастность встраиваемой информации, так как чем более совершенными становятся методы сжатия, тем меньше остается возможностей для внедрения посторонней информации. Поэтому в данном направлении непрерывно проводятся исследования, а число публикаций по данной тематике достигает несколько сотен в год, и их количество постоянно возрастает. Как показал проведенный анализ, наиболее эффективны стегосистемы, реализующие скрытие данных в области спектральных преобразований с учетом особенностей алгоритмов сжатия изображений [3 – 5].

Целью данной работы является разработка и исследование алгоритмов скрытия данных в изображениях на основе дискретного косинусного преобразования и вейвлет-преобразования для стандартов сжатия JPEG и JPEG-2000.

**1. Дискретные преобразования в алгоритмах сжатия изображений**

Для сжатия изображений можно использовать такие двухмерные дискретные преобразования, как преобразование Фурье, преобразование Уолша – Адамара, дискретное косинусное преобразование, дискретные преобразования Хартли, Хаара и т.д. Однако широко распространенный в мире стандарт сжатия JPEG предполагает применение дискретного косинусного преобразования (ДКП) к блокам изображения размером 8×8 пикселей [6]. Одномерное ДКП описывается выражением [6]:

$$\begin{cases} C_0 = \dfrac{1}{\sqrt{N}} \sum\limits_{n=0}^{N-1} s_n, \\ C_k = \sqrt{\dfrac{2}{N}} \cdot \sum\limits_{n=0}^{N-1} s_n \cdot \cos\left[ \dfrac{2n+1}{2N} k\pi \right], \end{cases}$$

где $s_n$ – отсчеты входного сигнала; $C_0$, $C_k$ – спектральные коэффициенты ($k = \{1, 2,\ldots, N-1\}$).

Обратное ДКП можно записать как

$$s_n = \frac{1}{\sqrt{N}} \hat{C}_0 + \sqrt{\frac{2}{N}} \cdot \mathrm{Re}\left\{ \sum_{k=1}^{2N-1} \exp\left[ j \frac{k\pi}{2N} \right] \hat{C}_k \overline{W}^{kn} \right\},$$

где

$$\hat{C}_k = \begin{cases} C_k, \text{ для } k \in 1,2,....N-1 \ , \\ 0, \quad \text{для } k \in N, N+1,....2N-1 \ ; \end{cases}$$

$$\overline{W} = \exp\left( \sqrt{-1} \frac{2\pi}{2N} \right), \quad n \in 1,2,...., N-1 \ .$$

Двумерное прямое ДКП в матричной форме определяется следующим образом:

$$C_{k_1,k_2} = \varphi_{k_1,n_1} \ s_{n_1,n_2} \ \varphi_{k_2,n_2}{}^T,$$

где $C_{k1,k2}$ – матрица спектральных коэффициентов ДКП размером N×N; $k_1, n_1, k_2, n_2 \in 0, 1, ..., N-1$ ; $s_{n1,n2}$ – сигнальная матрица размером N×N; $\varphi_{k1,n1}$ – матрица ДКП размером N×N:

$$\varphi_{k_1,n_1} = \sqrt{\frac{2}{N}} \left[ \begin{array}{c} \dfrac{1}{\sqrt{2}} \\ \cos\left[ \dfrac{2n_1+1}{2N} \cdot k_1\pi \right] \end{array} \right],$$

$$k_1, \in 1, 2, ..., N-1 \ , \ n_1 \in 0,1, ..., N-1 \ ;$$

$\varphi_{k2,n2}$ – матрица ДКП размером N×N:

$$\varphi_{k_2,n_2} = \sqrt{\frac{2}{N}} \left[ \begin{array}{c} \dfrac{1}{\sqrt{2}} \\ \cos\left[ \dfrac{2n_2+1}{2N} \cdot k_2\pi \right] \end{array} \right],$$

$$k_2, \in 1,2, ..., N-1 \ , n_2 \in 0,1, ..., N-1 \ .$$

Базовая схема стандарта сжатия JPEG-2000 схожа со схемой алгоритма JPEG, но одним из основных отличий является использование вейвлет-преобразования вместо дискретного косинусного преобразования. Вейвлет-преобразование двумерного сигнала $s(x, y)$ определяется как корреляция между двумерным сигналом и семейством вейвлетов $\varphi_q(x, y)$ [7]:

$$W_s(q, t_x, t_y) = \left\langle s(x, y), \varphi_q(x, y) \right\rangle,$$

где вейвлеты $\varphi_q(x, y)$ являются масштабированными и сдвинутыми копиями материнского вейвлета $\varphi(x, y)$:

$$\varphi_{q,t}(x, y) = \frac{1}{\sqrt{q}} \cdot \varphi\left( \frac{x - t_x}{q}, \frac{y - t_y}{q} \right).$$

Здесь $q$ – параметр масштаба; $(t_x, t_y)$ – параметр сдвига.

Для вейвлет-преобразования цифровых изображений применяют пирамиду Маллата [7]: для каждой строки цифрового изображения $s(i, j)$ выполняются операция фильтрации с помощью низкочастотного и высокочастотного фильтров и операция децимации. В результате формируются матрица низкочастотных коэффициентов $s^L(i, j)$ и матрица высокочастотных коэффициентов $s^H(i, j)$. Затем для каждого столбца полученных матриц выполняются операции фильтрации и децимации, в итоге формируются четыре матрицы (изображения): $s^{LL}(i, j)$, $s^{LH}(i, j)$, $s^{HL}(i, j)$ и $s^{HH}(i, j)$. Изображение $s^{LL}(i, j)$ представляет собой аппроксимацию изображения $s(i, j)$, а изображения $s^{LH}(i, j)$, $s^{HL}(i, j)$ и $s^{HH}(i, j)$ содержат детализирующую информацию.

Для того чтобы стегосистема обеспечивала робастность к компрессии изображений, в предлагаемой стегосистеме учитываются особенности алгоритмов сжатия JPEG и JPEG-2000 и предусмотрена возможность использования либо ДКП, либо вейвлет-преобразования на этапе внедрения скрываемого сообщения.

**2. Внедрение и восстановление скрываемой информации**

В разработанной стегосистеме сообщение, представляемое в виде изображения, внедряется в цифровой контейнер (статическое изображение) путем изменения амплитуд спектральных коэффициентов, полученных в результате прямого дискретного преобразования, на основе выражения:

$$E_{k,l} = S_{k,l} + \frac{A}{255} \cdot (W_{i,j} - 128), \quad (1)$$

где $S_{k,l}$ – амплитуда спектральной составляющей цифрового контейнера; $E_{k,l}$ – амплитуда спектральной компоненты стегоконтейнера; $W_{i,j}$ – компонента скрываемого сообщения; $A$ – весовой коэффициент, определяемый величиной энергии, которую можно добавить к изображению без его существенного искажения.

В связи с тем, что свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле, энергия, добавленная к изображению, должна быть очень мала. Пусть $E_s$ – максимально допустимое значение энергии, которую можно добавить к изображению без его существенного искажения, а $E_I$ – энергия контейнера. Введем обозначение: $k = \frac{E_s}{E_I}$. Тогда на основании равенства Парсеваля можно записать:

$$E_s = \frac{k}{N} \cdot \sum_{i=1}^{N} |S_i|^2,$$

где $N$ – общее число спектральных составляющих контейнера.

Пусть $N_1$ – общее число компонент скрываемого сообщения, тогда величина энергии, изменяемая в исходном изображении, может быть определена как

$$E_s = \frac{1}{N} \cdot \sum_{i=1}^{N_1} |\Delta S_i|^2 = \frac{1}{N} \cdot \sum_{i=1}^{N_1} \left( \frac{A}{255} \cdot 128 \right)^2 \approx \frac{A^2}{4 N_1 N}.$$

Отсюда можно определить весовой коэффициент $A$:

$$A = \sqrt{\frac{4 \cdot k}{N_1} \cdot \sum_{i=1}^{N \cdot M} |S_i|^2}. \quad (2)$$

Для обеспечения высокой криптостойкости стегосистемы при внедрении необходимо использовать криптографический алгоритм. В данной работе используется ассиметричный современный криптографический алгоритм RSA, безопасность которого основана на сложности разложения на множители больших чисел [8]. Для сокрытия в стегоконтейнере встроенного сообщения с помощью алгоритма RSA

и обеспечения быстродействия шифруются номера спектральных составляющих, в которых содержатся компоненты скрытого сообщения. При этом перед шифрованием каждый номер соответствующей спектральной составляющей дополняется строкой случайных бит длиной $M$ (в зависимости от длины выбранного модуля).

Известно, что реальные изображения не являются случайным процессом с равномерно распределенными значениями величин и большая часть энергии изображений сосредоточена в низкочастотной части спектра. Низкочастотные субполосы содержат подавляющую часть энергии изображения. Высокочастотные составляющие наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие, низкочастотная (размытие) или медианная фильтрация. Поэтому для обеспечения устойчивости стегосистемы к алгоритмам сжатия используются низкочастотные компоненты контейнера.

Таким образом, алгоритм скрытия сообщения требует выполнения следующих основных шагов:

- выполнение прямого дискретного преобразования для контейнера – ДКП при использовании алгоритма JPEG и вейвлет-преобразования при использовании JPEG-2000;
- расчёт весового коэффициента по формуле (2);
- скрытие сообщения с использованием выражения (1) и алгоритма RSA;
- выполнение обратного дискретного преобразования.

Восстановление скрываемого сообщения требует наличие контейнера, стегоконтейнера и закрытого ключа алгоритма RSA. При этом требуется выполнить прямое дискретное преобразование для стегоконтейнера и извлечь сообщение с использованием закрытого ключа алгоритма RSA на основе выражения:

$$W_{i,j} = \frac{255}{A} \cdot (E_{k,l} - S_{k,l}) + 128,$$

где $S_{k,l}$ – амплитуда спектральной составляющей цифрового контейнера; $E_{k,l}$ – амплитуда спектральной компоненты стегоконтейнера.

**3. Экспериментальные исследования**

Для внедрения и извлечения информации разработано программное обеспечение, основой которого являются представленные алгоритмы. На базе разработанного обеспечения проведены практические эксперименты по внедрению сообщений, представленных в виде изображений, в цветные изображения.

На первом этапе экспериментов при скрытии информации использовалось дискретное косинусное преобразование, а стегоконтейнеры подвергались JPEG-сжатию и преобразованию в формат GIF и обратно. По результатам исследований установлено, что JPEG-сжатие приводит к более существенным искажениям встроенных сообщений по сравнению с преобразованием палитры стегоконтейнера (рис. 1 – 3).

Рис. 1. Контейнер

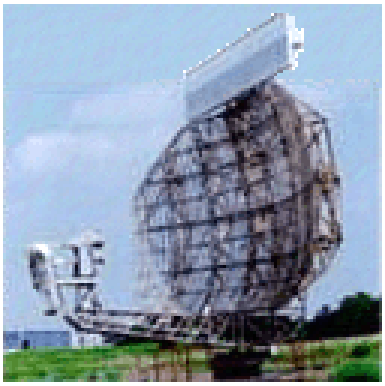


Рис. 2. Стегоконтейнер

а) б) в)

Рис. 3. Скрываемое изображение:
а – исходный вид; б – восстановленное после JPEG-сжатия стегоконтейнера;
в – восстановленное после преобразования цветовой палитры стегоконтейнера

На втором этапе экспериментов при скрытии информации использовалось вейвлет-преобразование, а стегоконтейнеры, полученные с различными весовыми коэффициентами, подвергались JPEG-2000-кодированию с разными степенями сжатия. По результатам исследований установлено, что для используемого стегоконтейнера необходим выбор оптимального весового коэффициента на основе визуального контроля стегоконтейнера при внедрении, а также установлено, что значительное увеличение степени сжатия все же приводит к потерям качества скрываемой информации. Поэтому дальнейшее совершенствование разработанной стегосистемы возможно путем применения помехоустойчивого кодирования.

Результаты экспериментов проиллюстрированы рисунком 4 и показаны в таблицах 1 – 2.


а) б) в)

Рис. 4. Результаты экспериментов:
а – цифровой контейнер (179 кб); б – стегоконтейнер (179 кб); в – скрытое сообщение (5 кб)

Размер цветного контейнера (24 бита на пиксель) составляет 305×200 пикселей. Внедряемое сообщение (рис. 4, в) размером 42×39 пикселей (на рисунке 4, в и далее представлено увеличенным в два раза) использовалось без рамки, она показана на рисунке для наглядности границ.

В ходе экспериментов рассчитывалась степень сходства восстановленного сообщения $D' = d'_{ij}$ и внедряемого $D = d_{ij}$ по формуле:

$$R^{SSD} = 1 - \frac{1}{256} \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(d_{ij} - d'_{ij})^2}{\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(d_{ij})^2}\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(d'_{ij})^2}}.$$

Таблица 1

Рассчитанные значения коэффициента схожести $R^{SSD}$ для скрываемой и восстановленной информации

| Весовой коэффициент | Размер файла стегоконтейнера, кб | | | | |
|---|---|---|---|---|---|
| | 115 | 45 | 21 | 12 | 8 |
| 50 | 0,996 | 0,995 | 0,989 | 0,958 | 0,899 |
| 100 | 0,996 | 0,995 | 0,989 | 0,965 | 0,916 |
| 200 | 0,996 | 0,995 | 0,989 | 0,973 | 0,942 |

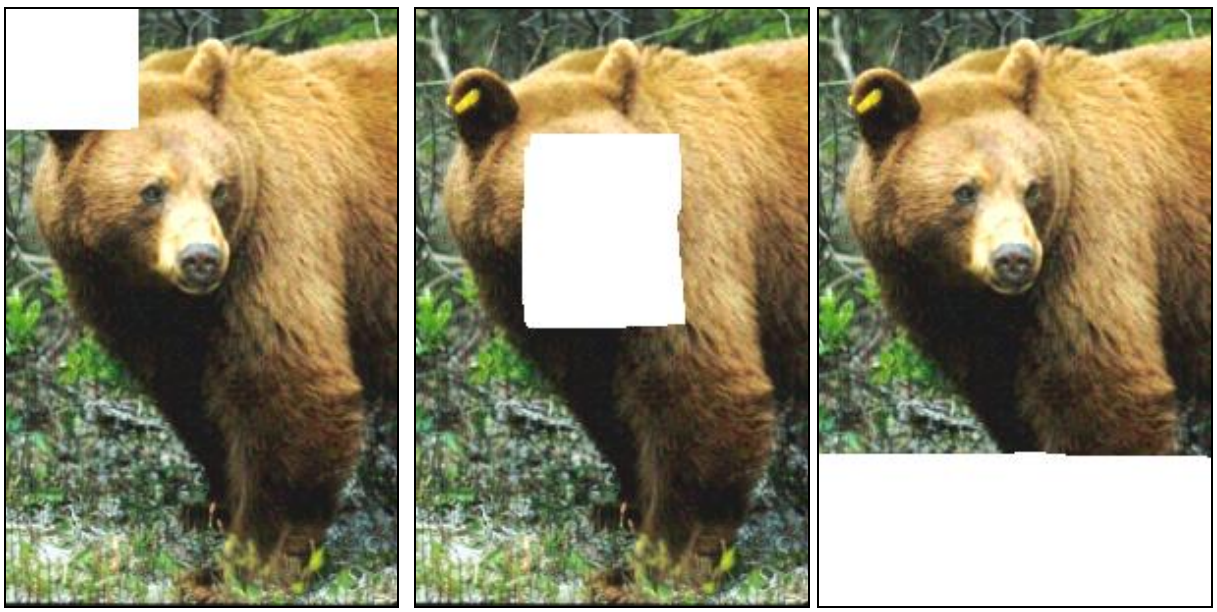
Визуальный анализ результатов (табл. 2) и анализ рассчитанных коэффициентов схожести (см. табл. 1) показывают, что при оптимальном значении весового коэффициента для заданного контейнера значительное увеличение степени сжатия приводит к потерям качества восстановленного сообщения, в то же время с увеличением весового коэффициента ухудшается качество стегоизображения.

Таблица 2

Восстановленные сообщения при различных степенях сжатия в формате JPEG-2000

| Весовой коэффициент | Размер файла стегоконтейнера, кб | | | | |
|---|---|---|---|---|---|
| | 115 | 45 | 21 | 12 | 8 |
| 50 |  |  |  |  |  |
| 100 |  |  |  |  |  |
| 200 |  |  |  |  |  |

На третьем этапе тестировалась робастность стегосистемы к потере или преднамеренной порче части стегоконтейнера при передаче или хранении. Стабильность стегосистемы проверялась следующим образом: в стегоконтейнере имитировалась потеря фрагмента изображения (до 26 %) в произвольном месте. Результаты экспериментов показаны на рисунке 5 и в таблице 3.



а) б) в)

Рис. 5. Стегоконтейнер с потерей части контента:
а – с потерей 6,5 % контента в левом верхнем углу; б – с потерей 12,8 % контента в центральной части;
в – с потерей 26 % контента в нижней части

Таблица 3

Результаты экспериментов по робастности алгоритма к потере части информации стегоконтейнера

| Местоположение | в левом верхнем углу | в центральной части | в нижней части | в нижней части | в нижней части |
|---|---|---|---|---|---|
| Количество утерянного изображения стегоконтейнера, % | 6,5 | 12,8 | 3 | 13 | 26 |
| Восстановленное сообщение |  |  |  |  |  |
| $R^{SSD}$ | 0,982 | 0,972 | 0,994 | 0,985 | 0,961 |

Анализ полученных результатов показывает, что восстановленное изображение визуально распознаваемо даже при потере 25 % контента стегоконтейнера.

**Заключение**

В работе рассмотрена стеганографическая система скрытия информации, представленной в виде изображения, в цветных статических изображениях. Для обеспечения робастности стегосистемы к компрессии изображений в форматах сжатия JPEG и JPEG-2000 предусмотрена возможность использования ДКП или вейвлет-преобразования на этапе внедрения скрываемого сообщения. Разработанный алгоритм скрытия информации использует низкочастотные компоненты изображения, что также увеличивает его устойчивость к алгоритмам сжатия, при этом различие между стегоконтейнером и контейнером при оптимальном выборе параметров стегосистемы визуально установить достаточно сложно. Криптостойкость системы обеспечивается применением ассиметричного криптографического алгоритма RSA при внедрении информации в контейнер. Восстановление скрываемого сообщения требует наличие контейнера, стегоконтейнера и закрытого ключа алгоритма RSA.

Проведен ряд экспериментов, которые подтвердили эффективность данной стегосистемы и показали ее перспективность для использования в системах скрытой передачи информации, в системах встраивания цифровых водяных знаков и идентификационных номеров. Однако по результатам исследований установлено, что при оптимальном коэффициенте внедрения для заданного контейнера значительное увеличение степени сжатия или фильтрация стегоконтейнера приводит к потерям качества восстановленного сообщения. В связи с этим дальнейшее совершенствование разработанной стегосистемы возможно путем применения помехоустойчивых кодов на этапе внедрения информации в контейнер.

ЛИТЕРАТУРА


1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 261 с.
2. Кащеев, А.А. Стеганографическая защита цифровых изображений / А.А. Кащеев, С.Б. Саломатин // Изв. Белорус. инж. акад. – 2003. – № 1(15)/1. – С. 215 – 217.
3. Akansu, A.N. Data hiding in multimedia – theory and applications / A.N. Akansu // Doctoral Dissertation Department of ECE New Jersey Institute of Technology University Heights, Newark, NJ 07032, 1999.
4. Pereira, S. A framework for optimal adaptive DCT watermarks using linear programming / S. Pereira, T. Pun // Proc. of Tenth European Signal Processing Conf., EUSIPCO’2000, Tampere, Finland, Sep. 5 – 8, 2000. – Tampere, 2000. – P. 42 – 46.
5. Hassanien, A. Watermarking for copyright protection using discrete wavelet transform / A. Hassanien // Proc. of the 8 Int. Conf. Pattern Recognition and Information Processing, PRIP’2005, Minsk, May 18 – 20, 2005 / Belarusian State University of Informatics and Radioelectronics. – Minsk, 2005 – P. 185 – 191.
6. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин [и др.]. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с.
7. Chen, G. Applications of Wavelet Transforms in Pattern Recognition and De-noising / G. Chen. – Montreal, Concordia University, Canada, 1999. – 120 p.
8. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.


*Поступила 10.02.2009*