УДК 004.056.5

**О.О. Евсютин, Е.В. Негачева**

# Стеганографическое встраивание информации в цифровые изображения, сжатые с помощью блочных клеточных автоматов

Исследуется возможность использования цифровых изображений, сжатых с помощью метода, построенного на основе блочных клеточных автоматов, в качестве стегоконтейнеров. Производится оценка дополнительного шума, проявляющегося на восстанавливаемых после сжатия изображениях, в зависимости от параметров записи встраиваемой информации.

**Ключевые слова:** защита конфиденциальной информации, стеганография, цифровые изображения, сжатие, PSNR.

Цифровая стеганография – наука, занимающаяся вопросами скрытой передачи одних битовых последовательностей в других последовательностях, – наряду с криптографией позволяет решать задачи обеспечения конфиденциальности информации и аутентификации данных, а также задачу защиты авторских прав на цифровые объекты с помощью внедрения в последние так называемых цифровых водяных знаков [1–5].

Чаще всего в качестве контейнеров для сокрытия битовых последовательностей выбираются цифровые изображения, что связано с их повсеместным использованием в современном мире и значительной избыточностью, присущей составляющим их элементам данных [6]. При этом необходимо отметить, что несмотря на существование значительного количества стеганографических методов и алгоритмов, направленных на работу с цифровыми изображениями без сжатия, когда стеганографическое кодирование осуществляется в пространственной области посредством изменения значений отдельных пикселей, использование подобных методов зачастую оказывается затруднительным, поскольку на практике в основном применяются сжатые цифровые изображения.

В этом случае стеганографическое кодирование из пространственной области перемещается в частотную – так как наиболее эффективные методы сжатия цифровых изображений основываются на ортогональных преобразованиях, служащих для декорреляции элементов данных, то соответствующие алгоритмы встраивания оперируют коэффициентами этих преобразований, используя их для записи встраиваемой информации [1, 2].

В [7] рассматривается метод сжатия цифровых изображений с потерями, построенный с применением блочных клеточных автоматов. В настоящей работе предлагается использовать сжатые с помощью указанного метода цифровые изображения в качестве стегоконтейнеров и приводятся результаты соответствующего исследования.

**Метод сжатия цифровых изображений на основе блочных клеточных автоматов.** Данный метод построен в соответствии с той же моделью, что и классические методы JPEG и JPEG 2000, когда сжатие цифрового изображения осуществляется за счет устранения пространственной избыточности из элементов данных с помощью ортогонального декоррелирующего преобразования, последующего отбрасывания некоторой малозначимой информации об изображении посредством квантования преобразованных элементов данных и завершающего устранения статистической избыточности из квантованных элементов данных с помощью энтропийного кодирования, как это показано на рис. 1. Однако особенностью рассмотренной модели является использование для декорреляции элементов данных декоррелирующих клеточных преобразований (ДКлП), получаемых с помощью динамики блочных клеточных автоматов [8].

Алгоритмы получения такого рода преобразований рассматриваются в работе [9].

Произвольное ДКлП определяется ортогональным базисом, который в общем случае является представителем некоторого подсемейства семейства базисов $\mathbf{\Sigma}(\mathrm{CA}, \mathbf{B})$, полученных из состояний развития заданного клеточного автомата CA при использовании кодового множества $\mathbf{B}$ [7]. Существуют семейства базисов, преобразования на основе которых совпадают с известными ранее ортогональными преобразованиями или являются их аппроксимациями. В частности, рассматриваемое в

[10] дискретное псевдокосинусное преобразование может быть описано в терминах клеточных автоматов как ДКлП, являющееся представителем подсемейства преобразований, частотные спектры которых содержат только одну низкочастотную составляющую среди преобразованных элементов данных.

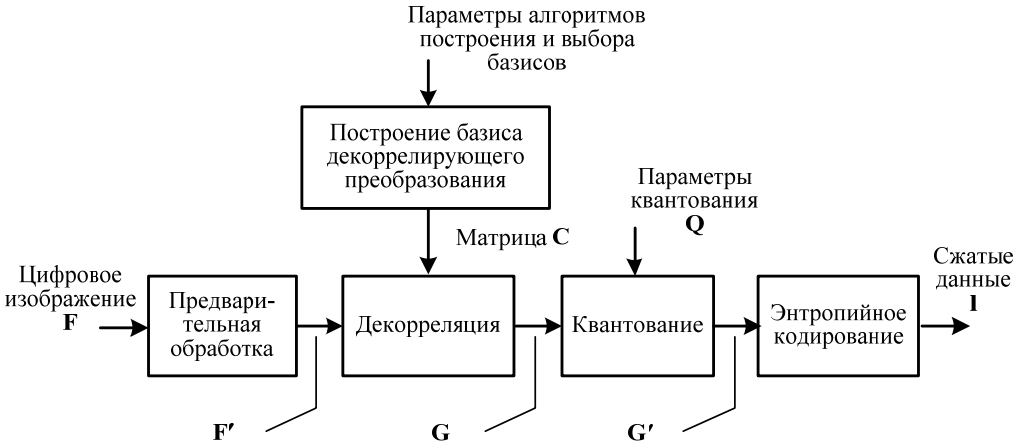


Рис. 1. Модель сжатия цифровых изображений на основе блочных клеточных автоматов

Особенностью же используемых в [7] ДКлП является наличие в их частотных спектрах равного количества низко- и высокочастотных составляющих, что дает аппроксимацию дискретного вейвлетного преобразования.

Таким образом, рассматриваемый метод сжатия цифровых изображений построен с использованием кратномасштабной обработки [6], когда декоррелирующее преобразование проводится в ряд итераций, в ходе каждой из которых преобразованные элементы данных группируются в четыре квадранта – квадрант низкочастотных составляющих и три квадранта высокочастотных, после чего квадрант низкочастотных составляющих подается на вход очередной итерации преобразования.

**Встраивание информации в сжатые изображения.** Перечислим основные подходы к встраиванию информации в сжатые цифровые изображения.

1. Внедрение цифровых водяных знаков в пространственную область изображения, с тем чтобы в случае сжатия изображения (или иного изменения исходных элементов данных) присутствие цифрового водяного знака сохранилось в измененном изображении и он мог быть извлечен. Подобные алгоритмы не используют сжатые цифровые изображения непосредственно в качестве стегоконтейнеров, а работают с несжатыми изображениями, учитывая возможность их дальнейшего сжатия.

2. Внесение изменений в значения элементов данных после дискретного ортогонального преобразования таким образом, чтобы эти изменения косвенным образом определяли значения встроенных битов. Указанные изменения могут производиться, в частности, так, чтобы наличие в блоке данных встроенного единичного бита определялось тем, что коэффициенты дискретного преобразования в пределах этого блока (8×8 в случае дискретного косинусного преобразования) удовлетворяют некоторому соотношению, не характерному для исходных данных.

3. Сложение коэффициентов дискретного ортогонального преобразования элементов данных цифрового изображения с коэффициентами аналогичного преобразования элементов данных встраиваемого цифрового водяного знака [1, 2].

Необходимо отметить, что большинство из известных стеганографических алгоритмов, работающих со сжатыми цифровыми изображениями, предназначены для встраивания в изображения цифровых водяных знаков, а не секретной информации, что позволяет задействовать для встраивания отдельных битов десятки и сотни пикселей. Мы же рассмотрим задачу обеспечения конфиденциальности информации, предполагающую возможность встраивания в стегоконтейнеры битовых последовательностей произвольной длины.

Касательно рассматриваемого метода заметим, что для него с учетом приведенного ранее описания характерной является следующая картина расположения элементов данных после завершения всех итераций этапов декорреляции и квантования: в правых верхних квадрантах всех уровней ДКлП малые величины с одинаковыми, а также близкими значениями образуют вертикально ориентированные полосы, в левых нижних квадрантах – горизонтально ориентированные. Расположение

величин в диагональных квадрантах в общем случае не позволяет выявить какую-либо закономерность, однако там содержится достаточное количество значений, равных $0$, $1$ или $-1$.

В качестве примера продемонстрируем расположение преобразованных элементов данных при слабом сжатии для классического тестового изображения «Lenna» после пяти итераций ДКлП с последующим квантованием (рис. 2). Для этого возьмем матрицу $\mathbf{G}'$ (см. рис. 1) и отобразим ее с помощью псевдоцветов, поставив в соответствие каждому из целочисленных значений, составляющих данную матрицу, некоторый цвет с соблюдением следующего правила: нулевое значение изображается белым цветом, и чем больше значение элемента данных по абсолютной величине, тем темнее соответствующий цвет.

Рис. 2. Расположение квантованных элементов данных после 5-уровневого ДКлП полутонового изображения «Lenna»

Поскольку малые значения преобразованных элементов данных не оказывают определяющего влияния на формирование восстанавливаемых после сжатия изображений, то будем использовать такие элементы для непосредственной записи битов встраиваемого сообщения. При этом в каждый элемент данных будем записывать не более одного бита сообщения.

Основной вопрос, на который теперь необходимо ответить, это то, какая часть преобразованных (квантованных) элементов данных цифрового изображения может быть использована для встраивания битов секретного сообщения так, чтобы это не привело к заметным искажениям на восстановленном после сжатия изображении.

**Определение допустимого размера пространства сокрытия в сжатых цифровых изображениях.** Введем три категории сжатых цифровых изображений с точки зрения произведенных в процессе сжатия потерь информации и осуществим такое разделение по следующей шкале значений пикового отношения сигнал/шум PSNR между исходным и восстановленным изображениями: $\mathrm{PSNR} \geq 36$ дБ – малые потери, $27\text{ дБ} \leq \mathrm{PSNR} < 36$ дБ – средние потери и $\mathrm{PSNR} < 27$ дБ – значительные потери.

Для определения величины дополнительного шума, вносимого в цифровые изображения встраиваемыми сообщениями, будем использовать формулу

$$\Delta\mathrm{PSNR} = \mathrm{PSNR}_{\text{исх}} - \mathrm{PSNR}_{\text{стего}}, \qquad (1)$$

где $\mathrm{PSNR}_{\text{исх}}$ – пиковое отношение сигнал/шум между исходным изображением и изображением, восстановленным после сжатия; $\mathrm{PSNR}_{\text{стего}}$ – пиковое отношение сигнал/шум между исходным изображением и изображением, восстановленным после сжатия со встраиванием некоторого сообщения.

Для проведения экспериментов был взят классический набор полутоновых и непрерывнотоновых изображений, используемый для демонстрации и сравнения между собой алгоритмов цифровой обработки изображений («Baboon», «Barbara», «Boat», «Goldhill», «Lenna», «Peppers» и т.д.). Все изображения в данном наборе имели размер 512×512 пикселей.

На рис. 3 представлена характерная зависимость значения $\Delta\mathrm{PSNR}$ от длины сообщения, встроенного в сжатое изображение при малых потерях информации, произведенных в процессе сжатия.

Здесь и далее биты встроенных сообщений, представляющих собой тексты на русском языке, последовательно без пропусков записывались в квантованные элементы данных со значениями 0 и 1.

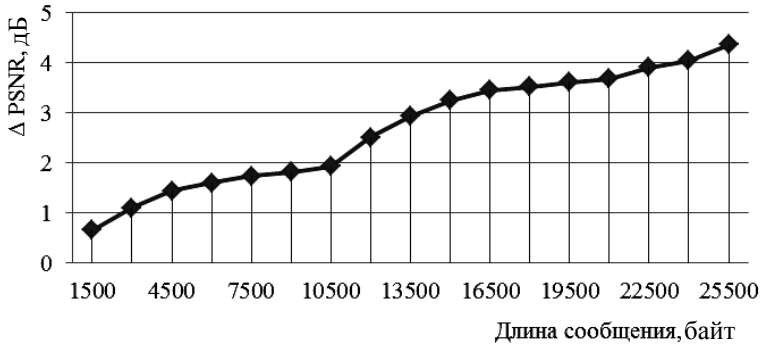


Рис. 3. Зависимость Δ PSNR от длины сообщения при малых потерях информации

Необходимо отметить, что размер пространства сокрытия при использовании описанного выше подхода к встраиванию информации в сжатые изображения не является постоянной величиной, поскольку количество малых значений среди преобразованных элементов данных зависит от использованного ДКлП и уровня произведенных потерь. Как можно увидеть из рис. 3, для использованных в данном случае непрерывно-тоновых цифровых изображений разрешением 512×512 пикселей размер пространства сокрытия составил приблизительно 25500 байт. Максимальное значение дополнительного шума, проявившегося при полном заполнении пространства сокрытия встроенным сообщением, достигло 4,4 дБ. При этом на восстанавливаемых после сжатия изображениях отсутствовали заметные артефакты.

Аналогичная зависимость значения ΔPSNR от длины встроенного сообщения при средних потерях информации, произведенных в процессе сжатия, представлена на рис. 4.

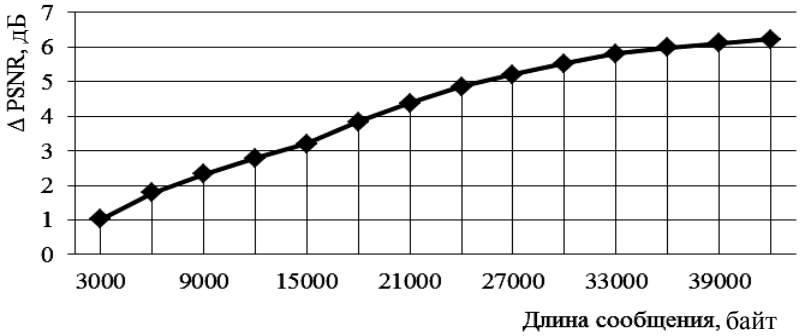


Рис. 4. Зависимость Δ PSNR от длины сообщения при средних потерях информации

В данном случае размер пространства сокрытия составил приблизительно 42000 байт, а максимальное значение шума, проявившегося при полном заполнении пространства сокрытия встроенным сообщением, достигло 6,2 дБ. Кроме того, при полном заполнении пространства сокрытия на восстанавливаемых после сжатия изображениях стали проявляться малозаметные артефакты.

После увеличения степени сжатия цифровых изображений была получена зависимость, представленная на рис. 5.

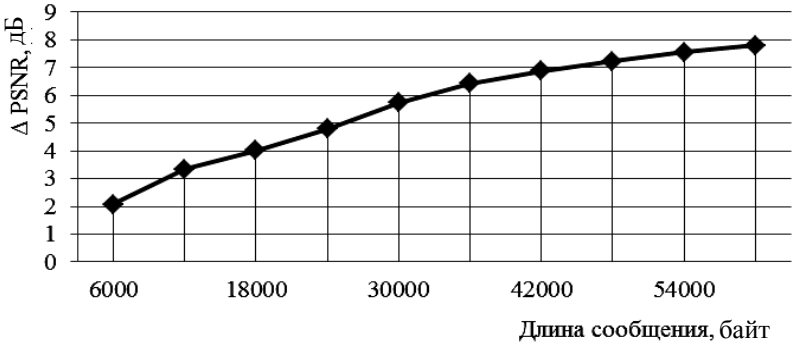


Рис. 5. Зависимость Δ PSNR от длины сообщения при значительных потерях информации

Размер пространства сокрытия естественным образом увеличился приблизительно до 60000 байт. Полное заполнение пространства сокрытия указанного размера привело к появлению значительных артефактов на восстановленных после сжатия изображениях, значение дополнительного шума увеличилось до 7,8 дБ.

При расширении множества значений, используемых для записи встраиваемых битов, до $\{0,1,-1\}$ была получена зависимость значения $\Delta$PSNR от длины сообщения при малых потерях информации, произведенных в процессе сжатия, представленная на рис. 6.

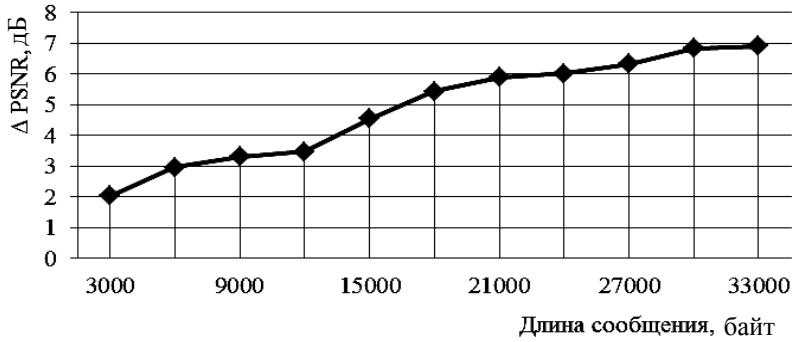


Рис. 6. Зависимость Δ PSNR от длины сообщения при малых потерях информации (при использовании элементов данных со значениями 0, 1 и −1)

Размер пространства сокрытия увеличился по сравнению со случаем, представленным на рис. 3, однако даже несмотря на малые потери информации, произведенные в процессе сжатия, включение в пространство сокрытия элементов данных со значением $-1$ привело к значительному увеличению дополнительного шума и появлению на восстанавливаемых изображениях заметных артефактов.

Дальнейшие эксперименты с записью встраиваемых битов в элементы данных со значениями из множества $\{0,1,-1\}$ показали, что при средних и значительных потерях информации, произведенных в процессе сжатия, величина дополнительного шума такова, что подобное расширение пространства сокрытия не имеет смысла.

В завершение настоящего исследования был проведен ряд экспериментов по записи битов встраиваемых сообщений не в подряд идущие элементы данных, а с некоторым периодом, поскольку, как отмечалось ранее, представленные на рис. 3–6 графики были получены в результате последовательной записи битов встраиваемых сообщений в элементы данных цифровых изображений. Однако увеличение периода встраивания при неизменном количестве встраиваемой информации не оказало какого-либо влияния на величину дополнительного шума и характер проявляющихся артефактов.

**Заключение.** Таким образом, в результате проведенного исследования было показано, что цифровые изображения, сжатые с помощью рассматриваемого метода, построенного на основе блочных клеточных автоматов, вполне пригодны к использованию в качестве стегоконтейнеров. При этом было установлено следующее:

1) при встраивании одной и той же битовой последовательности в изображение, сжатое с малыми, средними и значительными потерями информации, каждый раз наблюдается увеличение дополнительного шума, проявляющегося на восстановленном после сжатия изображении;

2) целесообразно использовать для записи встраиваемых битов элементы данных цифрового изображения, принимающие значения из множества $\{0,1\}$, в то время как добавление к указанному множеству значения $-1$ приводит к недопустимому увеличению дополнительного шума даже при малых объемах встраиваемой информации;

3) встраивание сообщения остается незамеченным при использовании в качестве пространства сокрытия до 20–25% элементов данных, составляющих цифровое изображение после завершения этапов декоррелирующего преобразования и квантования.

Работа выполнена при финансовой поддержке РФФИ (проект № 12-01-31378) и Министерства образования и науки Российской Федерации, проект 7.701.2011 (1/12).

*Литература*

1. Конахович Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2009. – 272 с.

3. Бондарчук С.С. Встраивание цифровых знаков для обеспечения защиты информации / С.С. Бондарчук, Е.М. Давыдова, Е.Ю. Костюченко // Доклады ТУСУРа. – 2011. – № 2(24), ч. 3. – С. 228–235.

4. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2/1. – С. 61–67.

5. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Специальный выпуск, № 1. – С. 51–61.

6. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.

7. Евсютин О.О. Метод сжатия цифровых изображений на основе блочных клеточных автоматов: дис. … канд. техн. наук / О.О. Евсютин. – Томск, 2012. – 174 с.

8. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 119–125.

9. Евсютин О.О. Разработка и тестирование вычислительного метода построения базисов декоррелирующих преобразований с использованием клеточных автоматов на разбиении / О.О. Евсютин, С.К. Росошек // Труды СПИИРАН. – 2012. – Вып. 23. – С. 324–342.

10. Умняшкин С.В. Алгоритм сжатия изображений на основе дискретного псевдокосинусного преобразования / С.В. Умняшкин, В.В. Курина // Цифровая обработка сигналов. – 2009. – № 3. – С. 2–7.

---

**Евсютин Олег Олегович**
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-403-09-21
Эл. почта: eoo@keva.tusur.ru

**Негачева Екатерина Викторовна**
Инженер каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: siluetalafelicidad@gmail.com

Evsutin O.O., Negacheva E.V.

**Steganographic embedding of information into digital images compressed with the use of block cellular automata**

We investigate the opportunity to use digital images, compressed according to the method based on block cellular automata, as containers. We estimate the additional noise, shown during the restoration of already compressed images, depending on the recording parameters of embedded information.

**Keywords:** protection of confidential information, steganography, digital images, compression, PSNR.

---