ИНВАРИАНТНОЕ ТРОИЧНОЕ КОДИРОВАНИЕ ИНФОРМАЦИИ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

М. В. Харинов♦

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<khar@iias.spb.su>

УДК 681.3

Харинов М. В. **Инвариантное троичное кодирование информации в цифровом изображении** // Труды СПИИРАН. Вып. 3, т. 2. — СПб.: Наука, 2006.

Аннотация. *В детерминированном комбинаторном подходе к понятию содержащейся в сигнале (изображении) информации решается задача обратимого встраивания в изображение сообщения в виде произвольной последовательности бинарных кодов. Решение достигается благодаря многоканальной троичной памяти, которая формально приписывается изображению и оказывается способной хранить записанные в нее коды сообщения независимо от предусмотренных преобразований сигнала в процессе передачи.* — Библ. 10 назв.

UDC 681.3

Kharinov M. V. **Invariant Ternary-Coded Storage of Information in Digital Image** // SPIIRAS Proceedings. Issue 3, vol. 2. — SPb.: Nauka, 2006.

Abstract. *The problem of reversible data embedding is solved in framework of deterministic approach to video-information interpretation. The embedding data is initialized as arbitrary bit series of some message. The solution is succeeded owing to simulation of abstract multi-channel ternary memory attributed to image. It appears that ternary memory is capable to memorize the message and to store it independently of prescribed transmission signal transformation.* — Bibl. 10 items.

1. Введение

В работе на примере решения задачи стеганографии (неявного встраивания в изображение произвольной последовательности битов некоторого сообщения) демонстрируется логика интерпретации понятия информации для компьютерных вычислений в троичной системе счисления или посредством вычислительных устройств с троичными запоминающими элементами. Проблема воссоздания и развития подобных устройств возникла в начале 70-х годов прошлого столетия с утилизацией серии универсальных ЭВМ «Сетунь» [1–2]. Сомнения в перспективности развития устройств с троичной логикой обосновывались утверждением, что информацию следует представлять исключительно в двоичной логике и системе счисления. Мы, развивая в задаче стеганографии детерминированный (не вероятностный) комбинаторный подход А. Н. Колмогорова к количественному представлению информации [3–4], приходим к иному заключению — варианты встраивания сообщения в двоичной логике и системе счисления воспроизводятся по результатам аналогичного встраивания в троичной логике и системе счисления, но не наоборот. При этом более общее троичное кодирование позволяет точнее и полнее отобразить формирование представлений информации, поскольку, в отличие от двоичного кодирования, исключает ошибки типа округления и предусматривает самостоятельный выбор значения кода для случая равноправных альтернатив.

♦Публикация результатов по теме настоящей работы в 2006 г. поддержана издательским грантом РФФИ № 06–07–95007.

Основное практическое преимущество применения троичного кодирования в задаче стеганографии заключается в упрощении алгоритмов встраивания кодов сообщения с наложением по координатам и повышении объема встраиваемых кодов сообщения до 20–30% от объема исходного изображения против обычных 10%, достигаемых традиционными методами [5–7].

Выполненные программные эксперименты дают основание формализовать встраивание и извлечение сообщения следующим образом.

2. Общая схема обратимого встраивания

Встраивание S_h сообщения h в изображение (контейнер) u достигается посредством преобразования W_h, которое при циклическом применении порождает некоторую последовательность представлений, сходящуюся к представлению $S_h u$:

$$S_h^2 = S_h \ : \quad S_h u = \lim_{n \to \infty} W_h^n u ,$$

где n — число повторений преобразования W_h.

Под *сходимостью* представлений, получаемых преобразованием (программой, отображением и пр.) W_h понимается существование предела $S_h u$ последовательности представлений $W_h^n u$, который не меняется под действием программы W_h и называется стего-изображением. Иными словами, предполагается, что процесс встраивания не зацикливается, и при достаточно большом числе N повторений достигается инвариантное относительно преобразования W_h представление v изображения u:

$$W_h v = v ,$$

где $v \equiv S_h u = W_h^N u$ — стего-изображение.

Хотя результат повторного выполнения встраивания S_h сообщения h в произвольный контейнер u совпадает с результатом однократного, условимся называть S_h *идемпотентным* встраиванием только тогда, когда встраивание сообщения h в произвольный контейнер u достигается за единственную итерацию и $N = 1$, а $S_h = W_h$. В общем случае, если преобразование S_h достигается за несколько итераций $N \geq 1$, называем его *итеративным* встраиванием.

Под *сообщением* h понимается матрица ячеек троичной памяти, которые сопоставляются *пикселам* (элементарным клеточным полям) изображения и содержат последовательности *тритов*, т.е. запоминающих элементов со значениями $0, \pm 1$. Представление h получается обнулением некоторого множества тритов представления $\tilde{h}$ из одних ± 1, которое строится посредством записи в троичную память исходной последовательности битов встраиваемой информации и выполняется с повторениями по координатам и разрядам троичной памяти до ее заполнения.

Нулевые триты в сообщении h возникают из-за того, что, в зависимости от контекста контейнера u, некоторые триты представления $\tilde{h}$ при записи в троичную память не учитываются, а при чтении изображения из троичной памяти вычисляются как неопределенные и помечаются нулевыми значениями. Поскольку нулевые триты сообщения h предсказуемы при встраивании представ-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ления $\tilde{h}$, пропуска битов исходной встраиваемой информации можно избежать, например, за счет кодирования исходной последовательности битов с исключением ее элементов при достаточном числе повторений. Поэтому, не уменьшая общности, можно рассматривать в качестве начального троичного представления исходной последовательности встраиваемых битов сообщение h и не останавливаться далее на деталях практической реализации, чтобы не загромождать изложение.

Извлечение сообщения h состоит в его вычислении по стего-изображению из условия того, что W_h оставляет стего-изображение неизменным:

$$R : \quad R(W_h v = v) = h,$$

где R — программа извлечения сообщения, которая выполняет решение уравнения $W_h v = v$ относительно h и, фактически, представляет собой самостоятельное формирование и вывод файла сообщения, предусматриваемые в теле программы W_h. При этом в выписанной формуле аргумент отображения R трактуется двояко: как изображение v и как условие $W_h v = v$, которое рассматривается в качестве уравнения для нахождения h.

Считается, что любое изображение содержит некоторое сообщение, и в качестве стего-изображения v может быть взято произвольное изображение.

Главной особенностью описанной схемы является то, что существование точного предела v приближений $W_h^n u$ стего-изображения в процессе встраивания сообщения h позволяет обойтись при его извлечении обращением условия сохранения сообщения при однократном встраивании, которое выражается множеством независимых локальных уравнений по координатам и вложенным диапазонам яркости сигнала, как описывается в следующем разделе.

3. Модель многоканальной троичной памяти сигнала

В предлагаемом решении встраивание сообщения осуществляется как его запоминание в собственной *многоканальной троичной* памяти, которая приписывается изображению формально, но используется для записи и считывания произвольных кодов сообщения подобно или посредством реальной цифровой памяти. Полагается, что многоканальная троичная память состоит из запоминающих элементов, которые получаются в результате обобщения понятия битов.

Если отвлечься от строения ячейки памяти обычного компьютера, то биты, в которых хранятся значения яркости пикселов изображения, можно описать посредством вложенных диапазонов шкалы яркости, по величине равных степеням 2. Разряды сопоставляемой изображению многоканальной троичной памяти определяются последовательностью вложенных диапазонов шкалы яркости, которые, вообще говоря, по величине не кратны 2, поскольку вычисляются вне этого условия в алгоритме итеративного разделения гистограммы яркости на части с приблизительно равным числом пикселов. Итеративное разбиение яркостной шкалы продолжается до тех пор, пока все яркостные диапазоны очередного разбиения не вырождаются в элементарные диапазоны, содержащие единственную яркость, которая сопоставляется последовательности стягивающихся к ней диапазонов и на каждой итерации принадлежит одному из них. Алгоритм разбиения яркостной шкалы таков, что варьирование яркости каждого пиксела изображения внутри своего диапазона, хотя и влияет на гистограмму

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

яркости, но не влияет на вычисление текущего разбиения яркостной шкалы, а также на вычисление предыдущих ее разбиений на диапазоны яркости. При этом пикселы могут модифицироваться по яркости независимо друг от друга.

Полагается, что ячейки многоканальной троичной памяти сопоставляются пикселам изображения и состоят из последовательных запоминающих элементов. Значение очередного элемента ячейки многоканальной троичной памяти, в зависимости от номера итерации разбиения яркостной шкалы, определяется положением яркости пиксела относительно центра очередного диапазона яркости. При этом данному элементу ячейки многоканальной троичной памяти приписывается положительное, отрицательное, либо нулевое значение знака разности яркости пиксела и центральной яркости рассматриваемого диапазона, как на рис. 1.

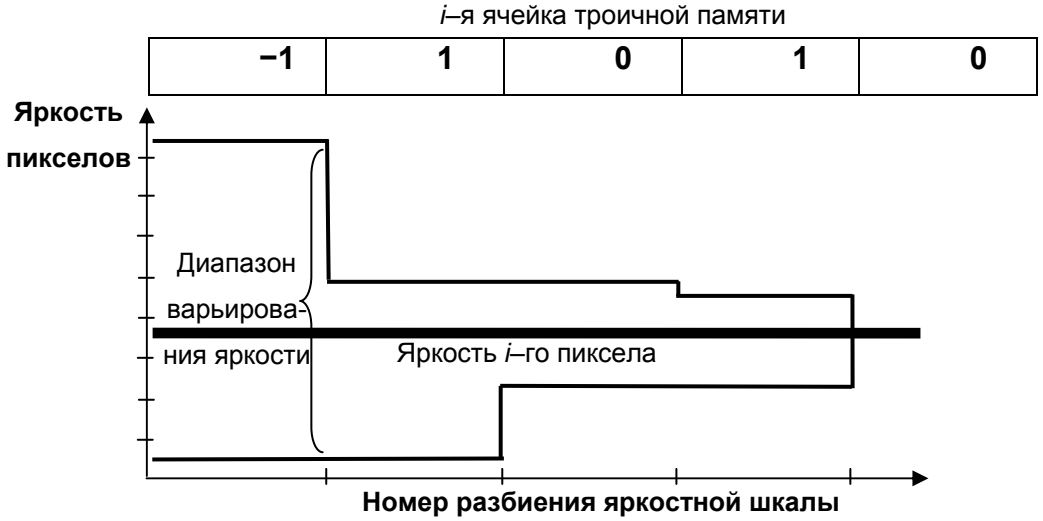

Рис. 1. Запоминание последовательности значений в *i*-й ячейке многоканальной троичной памяти.

Рисунок иллюстрирует содержание ячейки приписанной сигналу многоканальной троичной памяти, которая сопоставляется некоторому пикселу изображения с номером i.

Тем самым определяется считывание троичных единиц информации, которые согласно Н. П. Брусенцову называются тритами [1, 2]. Триты, вычисленные для данного разбиения шкалы яркости, составляют каналы троичной памяти и считаются упорядоченными по уменьшению вложенных диапазонов яркости. При этом самый старший трит каждой ячейки троичной памяти вычисляется для рабочего диапазона яркости, который содержит яркости всех пикселов изображения.

Запись сообщения в триты многоканальной троичной памяти связывается с отражением яркостного значения пиксела относительно центра соответствующего диапазона и выполняется последовательно от старших тритов — к младшим. Яркостное значение, оказавшееся в центре диапазона, очевидно, при отражении не меняется. Поэтому триты с нулевыми значениями при записи сообщения не подлежат модификации и считаются неактивными. К неактивным относят также триты, которые сопоставляются яркостям, ограничивающим допустимые диапазоны варьирования яркости, и триты, изменение которых влечет модификацию предшествующих тритов.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Основные принципы встраивания сообщения в многоканальную троичную память включают три требования инвариантности:

- инвариантность стего-изображения относительно повторного встраивания сообщения;
- инвариантность контейнера относительно обратного встраивания извлеченного сообщения;
- инвариантность сообщения относительно линейных и нелинейных изоморфных преобразований стего-изображения.

Здесь имеется в виду, что повторная запись сообщения не влияет на стего-изображение, любое изображение сохраняется при обратном встраивании извлеченного из него сообщения, а также, что предусмотрен режим, в котором стандартные преобразования стего-изображения (упаковка, растяжение рабочего диапазона, эквидистантное перераспределение яркостей стего-изображения по рабочему диапазону и пр.) не влияют на сообщение.

Компоненты цветового изображения при вычислении троичной памяти рассматриваются независимо друг от друга. Избыточность изображения выражается повторениями тритов по координатам, каналам троичной памяти и цветам. Искажение кодов сообщения в процессе передачи изображения компенсируется их простым суммированием с последующим вычислением знака полученной суммы. Для учета случая равновесного распределения альтернативных значений битов сообщения, в качестве запоминающих элементов ассоциированной с сигналом памяти удобно использовать именно триты, а не биты.

Таким образом, триты позволяют исключить систематические ошибки округления при вычислении ассоциированной с сигналом многоканальной памяти и точнее формализовать избыточность видеоинформации. Особенности единиц представления информации в многоканальной троичной памяти по сравнению с исходным представлением в компьютерной памяти отражены (для байтовых изображений) в табл. 1.

Таблица 1

Единицы представления и запоминания видеоинформации

Единицы / Атрибуты	Биты	Триты
Порядковый номер	0, 1, 2, ..., 7	0, 1, 2, ..., *Ch*
Состояние	0, 1	±1, 0
Статус	*RW*	*R, RW*

где Ch — число каналов троичной памяти, *R* и *RW* — обозначения неактивных и активных тритов.

4. Интерпретация канала троичной памяти

Рис. 2 иллюстрирует интерпретацию понятия канала троичной памяти сигнала.

На рисунке сплошной темной линией для изображения (контейнера) $u\{x\}$ показана зависимость яркости u от координаты x.

Суть идеи выполнения обратимого встраивания посредством многоканальной троичной памяти без использования «ключа» [5] сводится к построению в окрестности изображения последовательности вложенных «коридоров» допустимой модификации изображения, один из которых обозначен на рис. 2 и

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ограничен пунктирными линиями. Коридоры сопоставляются разрядам ячеек приписываемой изображению троичной памяти и порождают каналы передачи кодов сообщения с наложением по координатам. Каждый коридор, с одной стороны, вычисляется по изображению, а, с другой стороны, не зависит от варьирования в своих пределах яркостей пикселов изображения.

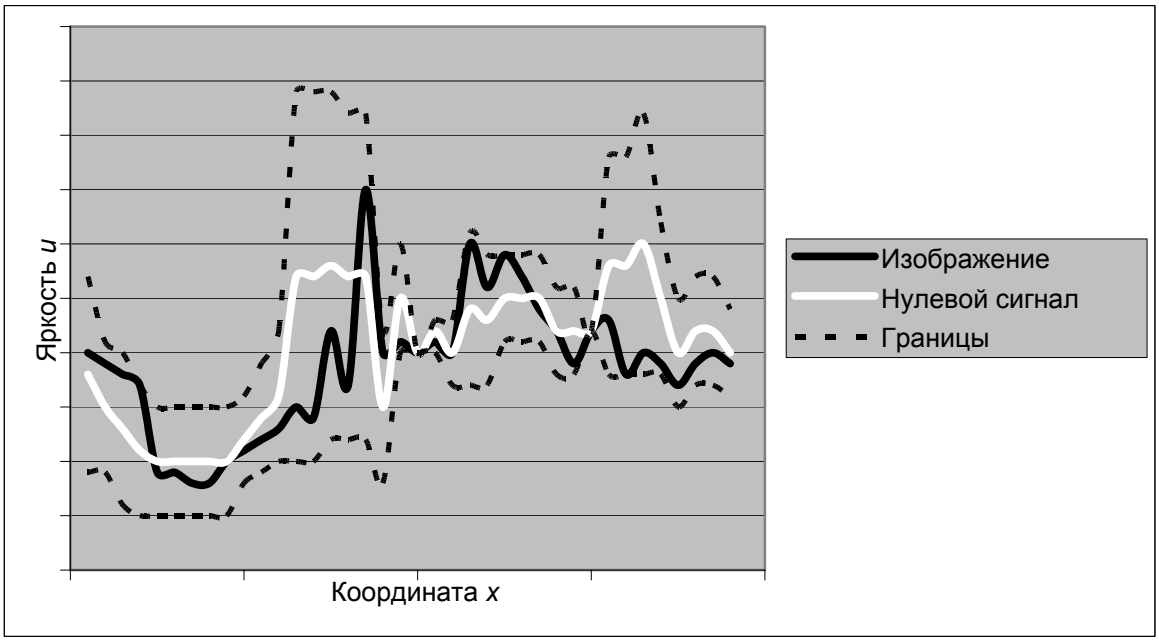

Рис. 2. «Коридор» варьирования яркостей изображения при обратимом встраивании сообщения на примере одномерного фрагмента изображения.

Границы натягиваются на яркости сохраняемых пикселов сигнала (контейнера или стего-изображения) и для каждого пиксела задают внутренний диапазон допустимого варьирования яркости, а также определяют обозначенные белым цветом центральные яркости допустимых диапазонов варьирования яркости. В принципе, в изображении может не встретиться ни одного пиксела, яркость которого совпадает с центром допустимого диапазона варьирования яркостного значения. Тем не менее, центральные яркости диапазонов, которые вычисляются одними и теми же по контейнеру и по стего-изображению, служат началом отсчета для кодов сообщения не хуже реальных яркостей и формально могут рассматриваться как яркости передаваемого *нулевого* сигнала.

Для точного и однозначного выполнения встраивания (записи) бита сообщения в изображение без использования округления мы записываем бит сообщения посредством зеркального отражения яркостного значения пиксела изображения относительно оси допустимого диапазона варьирования яркости.

Обратимое встраивание битов сообщения в яркости пикселов с координатами x описывается соотношением:

$$P(Pu\{x\} + |h\{x\}|\,\mathrm{sign}(h\{x\})) = Pu\{x\}\ ,$$

где $h\{x\} \equiv |h\{x\}|\,\mathrm{sign}(h\{x\})$ — отклонение яркости стего-сигнала от центра диапазона; $|h\{x\}|$ — его абсолютная величина; sign — функция знака, принимающая значения $-1, 0, 1$ в зависимости от, соответственно, отрицательного, нулевого и положительного значения аргумента; $\mathrm{sign}(h\{x\})$ — коды исходного сообщения, установленные и неустановленные биты которого кодируются в переменных пикселах, соответственно, положительными и отрицательными единичными

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

значениями функции знака отклонения $h\{x\}$; $Pu\{x\}$ — нулевой сигнал, яркости которого лежат на осевой линии диапазонов допустимой яркостной модификации; P — идемпотентное преобразование контейнера u в нулевой сигнал Pu, а $Pu\{x\} + |h\{x\}|\,\mathrm{sign}(h\{x\}) \equiv Pu\{x\} + h\{x\}$ — стего-изображение.

Под идемпотентным преобразованием здесь, как обычно, понимается преобразование, повторное применение которого совпадает с однократным:

$$P = P^2 .$$

Результирующее изображение, полученное под действием идемпотентного преобразования, условимся называть *идемпотентным представлением*.

Программно–алгоритмическая реализация модели многоканальной троичной памяти выполняется посредством числовой иерархии гомоморфных представлений изображения и описывается в следующих разделах.

5. Иерархия гомоморфных представлений изображения

Под представлением, *изоморфным* изображению по яркостному порядку, понимается преобразованное в тех же координатах изображение, между яркостями которого сохраняются отношения меньше, равно, больше. Если в преобразованном изображении допускается переход неравенств в равенства, но отношения не замещаются альтернативными, то оно считается *гомоморфным* представлением исходного изображения. Преобразование изображения в изоморфное (гомоморфное) представление называется *изоморфным (гомоморфным)* преобразованием. Под *иерархией* представлений изображения, в рамках обсуждаемого решения, мы имеем в виду представления изображения, которые порождаются последовательностью разбиений яркостной шкалы на вложенные диапазоны яркости и определяются для каждого разбиения с точностью до изоморфного преобразования. При заданном разбиении шкалы яркости гомоморфные представления получаются посредством замещения яркостей пикселов изображения порядковыми номерами или иными последовательными индексами соответствующих диапазонов, которые содержат ту или иную яркость, а изоморфное представление получается, когда каждый элемент заданного разбиения шкалы яркости содержит единственное яркостное значение.

6. Числовая иерархия инвариантных идемпотентных гомоморфных представлений

Под *числовой* иерархией представлений изображения, понимается иерархия гомоморфных представлений, которая получается при итеративном преобразовании яркостей пикселов некоторого изоморфного представления изображения посредством применения арифметической функции (деления нацело и умножения на целое число), зависящей только от величины яркости. Иными словами, *числовая иерархия* — это иерархия вложенных разбиений изображения, которая задается величинами яркости пикселов изоморфного представления изображения и арифметическими действиями с ними, например, в простейшем случае, итеративным делением яркостей самого изображения нацело пополам.

Числовая иерархия считается *инвариантной*, если изоморфное представление, которое ее порождает, не зависит от стандартных преобразований изо-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

бражения (упаковки, линейного преобразования, эквидистантной нормировки по яркости, а также других линейных и нелинейных изоморфных преобразований).

На рис. 3 приведен пример инвариантного изоморфного представления стандартного изображения «Лена».

Рис. 3. Изображение «Лена» (слева) и его инвариантное изоморфное идемпотентное представление (справа), нормализованное на рабочий диапазон яркости (от 0 до 255).

Показанное на рисунке инвариантное изоморфное представление Hu изображения u, взятое в качестве исходного изображения, при повторном преобразовании под действием алгоритма H не меняется. Поэтому алгоритм H является идемпотентным:

$$H = H^2 ,$$

а полученное по алгоритму H изображение Hu является идемпотентным представлением исходного изображения u.

Инвариантные идемпотентные гомоморфные представления $H_\mu u\{x\}$ из одноименной иерархии идемпотентных представлений во всех координатах x выражаются через инвариантное идемпотентное изоморфное представление $Hu\{x\}$ рекуррентными соотношениями:

$$H_\mu{}^2 = H_\mu \ : \ \begin{matrix} H_{Mrsn}u\{x\} \equiv Hu\{x\} \\ H_{\frac{\mu\text{-}1}{2}}u\{x\} = AH_\mu u\{x\} \end{matrix} \quad \mu = 3,7,...,Mrsn \ ,$$

где $Mrsn$ — число градаций формальной амплитудной шкалы представления Hu, выражаемое некоторым числом Мерсенна [8]; μ — число градаций шкалы представления $H_\mu u$, которое вычисляется итеративным делением числа $Mrsn$ нацело пополам; A — арифметическое преобразование, которое определяется выполнением расчетов в псевдотроичной системе счисления [9] и сводится к делению нечетных яркостей текущего представления нацело на 2, а четных — к удвоению амплитудных значений, предварительно поделенных нацело на 4.

Для краткости условимся называть инвариантные идемпотентные гомоморфные представления $H_\mu u$ *гистограммными образами*, в частности, представление Hu именовать *изоморфным* гистограммным образом.

При обратимом встраивании сообщения гистограммный образ используется для разделения пикселов изображения на не модифицируемые при встраивании сообщения пикселы видимого (вычисляемого) контекста сигнала (контейнера или стего-изображения) и варьируемые пикселы, в которых кодируются биты сообщения посредством зеркального отражения яркостных значений относительно оси диапазона допустимой модификации яркости. Пределы допустимой яркостной модификации вычисляются для каждой амплитудной *градации* (множества одинаковых амплитудных значений) гистограммного образа как

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

точная нижняя и точная верхняя границы яркостей пикселов изображения, яркости которых преобразуются в рассматриваемое амплитудное значение гистограммного образа.

7. Запоминание иерархии разбиений дискретной последовательности

Построение изоморфного гистограммного образа изображения (а вместе с ним и всей иерархии гистограммных образов) выполняется в алгоритме итеративного разбиения последовательных значений шкалы яркости с запоминанием получаемой иерархии разбиений в псевдотроичной системе счисления.

Рис. 4 поясняет запоминание иерархии разбиений на примере разделения строк одномерных таблиц из единственной строки ячеек посредством итеративного разделения каждой строки на две части равной длины, либо на три части с выделением центральной ячейки при невозможности симметричного разделения строки ячеек пополам:

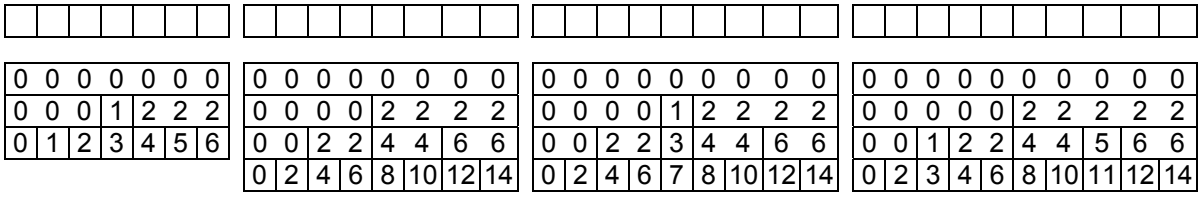

Рис. 4. Запоминание иерархии разбиений на примере формальных таблиц из единственной строки. Вверху — рассматриваемые одномерные таблицы. Внизу под ними — последовательные результаты кодирования иерархии разбиений в псевдотроичной системе счисления.

Обсуждаемый рисунок следует трактовать как абстрактную схему вычислений изоморфного гистограммного образа. Построение изоморфного гистограммного образа выполняется по гистограмме яркости. В роли последовательностей ячеек рассматриваются яркостные значения горизонтальной оси гистограммы, обозначающие упорядоченные множества одинаковых пикселов изображения, количество которых откладывается по вертикальной оси. Вместо метрической длины строки ячеек при построении изоморфного гистограммного образа используется количество пикселов слева и справа от рассматриваемого яркостного значения. В результате вычислений получаются амплитудные значения изоморфного гистограммного образа, которые сопоставляются каждому встречающемуся на изображении значению яркости и записываются вместо пикселов этой яркости в процессе преобразования H изображения u в изоморфный гистограммный образ Hu.

8. Идемпотентное встраивание сообщения

При встраивании и извлечении кодов сообщения посредством многоканальной троичной памяти используется три системы счисления. Каналы троичной памяти рассчитываются в троичной системе счисления и образуются тритами одинаковых разрядов, сопоставляемыми «коридорам» допустимого варьирования значений яркостей. Построение троичной памяти выполняется посредством изоморфного гистограммного образа Hu, который вычисляется в псевдотроичной системе счисления [9]. Разделение тритов на активные и неак-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

тивные поддерживается в двоичной системе счисления *структурным* представлением троичной памяти, установленные и неустановленные биты которого помечают, соответственно, активные и неактивные триты троичной памяти.

Поскольку в описанной схеме модификация изображения при встраивании сообщения, вообще говоря, влияет на структурное представление троичной памяти, встраивание сообщения выполняется итеративно и повторяется достаточное число раз до полной стабилизации стего-изображения. Экономичное по времени *идемпотентное* встраивание сообщения в изображение выполняется за единственную итерацию и достигается, если формировать троичную память с *непрерывной структурой*, т.е. с отсутствием чередования активных и неактивных тритов и значениями структурного представления кратными числам Мерсенна. Для формирования непрерывной структуры троичной памяти (от старших разрядов к младшим) при вычислении в данной ячейке троичной памяти первого неактивного трита относят к неактивным также и остальные триты младших разрядов ячейки.

Результаты расчетов объема встраивания при формировании многоканальной троичной памяти с учетом и без учета требования непрерывности структуры приведены в табл. 2 для *однородного* сообщения, порождаемого исходной последовательностью кодов из одинаковых битов.

Таблица 2

Экспериментальные данные по встраиванию однородного сообщения в стандартное изображение «Лена» (объем 64 Кб)

	Троичная память с чередованием активных и неактивных тритов			Троичная памятьс непрерывной структурой		
μ	*Ch*	Max число активных тритов на пиксел t_{max}	Объем встраивания *I* (байт)	*Ch*	Max число активных тритов на пиксел t_{max}	Объем встраивания *I* (байт)
1	9	4	24682	9	4	21612
3	10	3	19233	12	3	14566
7	9	3	17767	11	3	16031
15	8	3	13897	10	3	13078
31	8	3	10390	10	3	10124
63	8	3	5348	9	2	5218
127	8	3	1333	8	3	1298
255	8	2	200	8	2	193
511	8	2	66	8	2	64
1023	7	2	21	6	1	19
2047	6	2	13	5	2	12
4095	5	2	4	5	2	4
8191	3	1	2	3	1	2
16383	2	0	0	2	0	0

где: μ — максимальное число диапазонов начального разбиения шкалы яркости изображения; *Ch* — число каналов.

В табл. 2 показаны характеристики многоканальной троичной памяти в зависимости от разбиения рабочего диапазона яркости на несколько *самостоятельных* начальных диапазонов, которые строятся посредством гистограммного образа в μ градациях амплитуды и обрабатываются независимо друг от друга. Под $I\{x\}$ понимается число активных тритов, сопоставляемых в координате x пикселу изображения. Тогда оценки объема встраивания I и максимального

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

числа активных тритов $t_{\max}$ многоканальной троичной памяти выражаются соотношениями:

$$t_{\max} = \max_{x} I\{x\}$$
$$I = \sum_{x} I\{x\} \text{ (бит)}$$

Согласно таблице объем встраивания I оценивается в 20–30%. Число каналов Ch может превышать разрядность (число бит) яркостей исходного изображения, которая в рассматриваемом случае равна 8. В общем случае число активных тритов в ячейке многоканальной троичной памяти также может превышать разрядность исходного яркостного представления изображения.

9. Инвариантное итеративное встраивание сообщения. Пример

Для инвариантного встраивания сообщения в изображение последнее в процессе итеративной поразрядной записи компонент сообщения замещается своим гомоморфным, в частности, — изоморфным образом. При этом, даже при непрерывной структуре троичной памяти, идемпотентность встраивания, вообще говоря, утрачивается, но его итеративное повторение обеспечивает сходимость результата к требуемому стего-изображению. Необходимым условием построения стего-изображения в сходящемся алгоритме преобразования является упаковка по яркости гомоморфного гистограммного образа, которым замещается изображение перед встраиванием очередных кодов сообщения.

Рис. 5–6 иллюстрируют инвариантное встраивание сообщения из наложенных друг на друга цифр в упакованные по яркости гистограммные образы стандартного изображения «Лена» размером 256×256 пикселов при непрерывной многоканальной троичной памяти.

Рис.5 иллюстрирует исходную последовательность кодов сообщения, в качестве которого взят ряд рисованных цифр и прочих символов размером по 51×82 пикселов каждое, упакованных с наложением друг на друга в битовых плоскостях полутонового изображения. За счет периодического повторения картины сообщения по координатам и, при необходимости, по яркостным каналам коды сообщения геометрически повторяются в границах изображения до заполнения объема многоканальной троичной памяти.

Рис. 5. Исходные коды сообщения в виде полутонового изображения (слева) и в виде последовательности составляющих изображение битовых плоскостей (справа).

На рис 6 показаны результаты для начальных значений параметра $\mu_1 = 15, 31, 63$, совпадающего с числом градаций яркостной шкалы гистограммного образа, которым замещается изображение, и параметра $\mu = 1, 3, 7$, ограничивающего число независимых яркостных диапазонов, на которые формально разделяется рабочий диапазон яркости.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

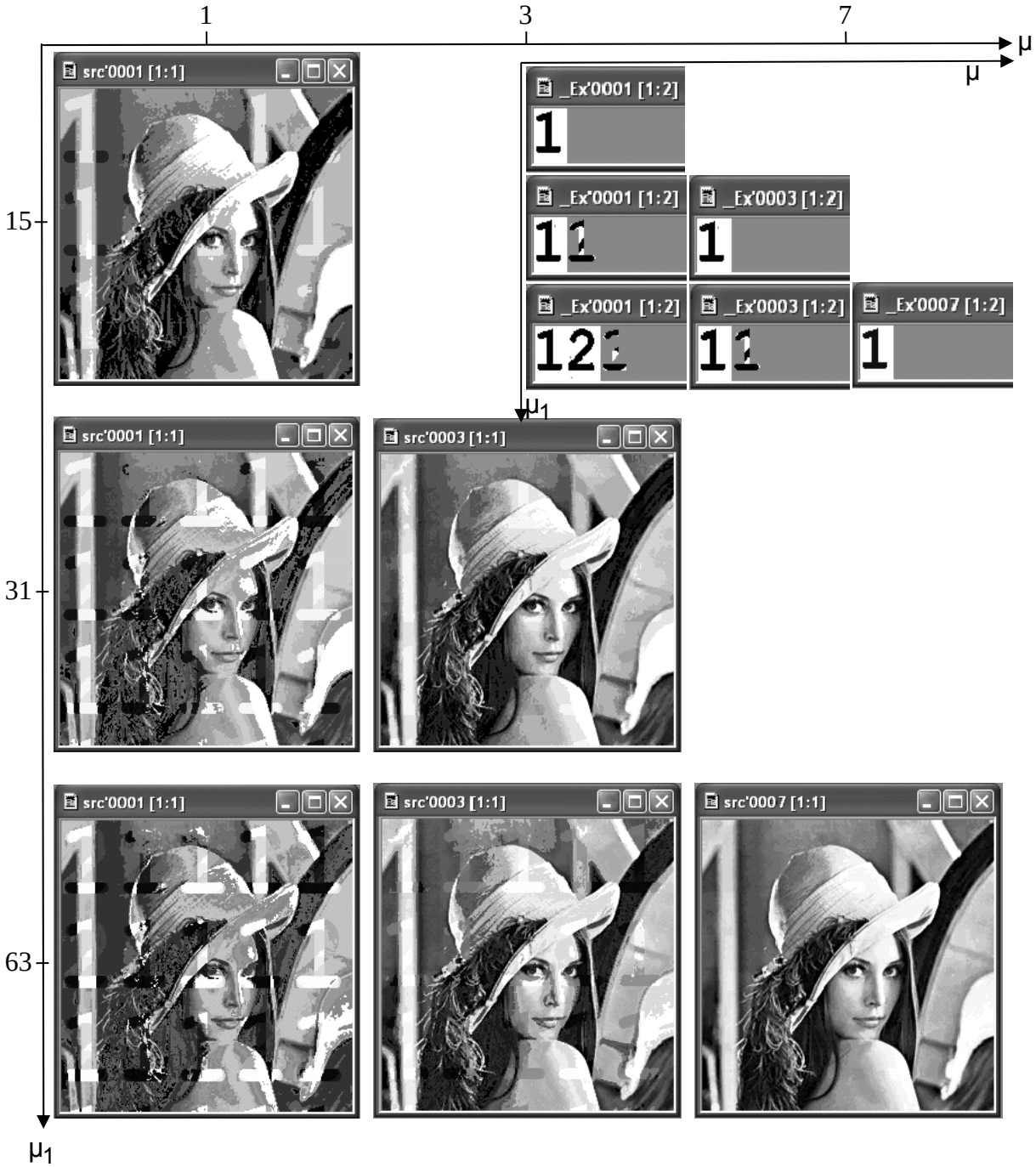

Рис. 6. Многоканальное инвариантное встраивание сообщения в троичную память с одновременным снижением числа градаций яркости стего-изображения. На осях отложены значения параметров $\mu_1 = 15, 31, 63$ (сверху вниз) и $\mu = 1, 3, 7$ (слева направо). Стего-изображения упорядочены в треугольную таблицу слева. В правом верхнем углу показана таблица соответствующих сообщений. Изображения эквидистантно нормированы по яркости на рабочий диапазон.

Рис. 6 содержит две треугольные таблицы, составленные из изображений. Первая таблица (слева) составлена из стего-изображений, а вторая (в правом верхнем углу) — из встроенных сообщений, компонентами которых являются рисунки цифр, встроенных в различные каналы.

Крайнее верхнее стего-изображение, полученное при параметре $\mu_1 = 15$, имеет 8 градаций яркости, остальные в том же столбце — 14 и 20 градаций (при параметрах $\mu_1 = 31$ и $\mu_1 = 63$, соответственно). При переходе от представ-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ления к представлению вдоль главной диагонали число градаций в стего-изображении приблизительно удваивается.

Ограниченное число градаций в стего-изображениях позволяет убедиться в сохранении сообщения при стандартных яркостных преобразованиях (упаковке, растяжении и пр.) посредством системного редактора.

Характерно, что при переходе от представления к представлению вдоль нисходящей (главной) диагонали и согласованном изменении обсуждаемых параметров, содержащиеся в различных каналах компоненты сообщения, а также само сообщение практически не меняются. Однако при этом с увеличением параметров μ и μ_1 видимые компоненты сообщения «теряются» в маскирующей картине, что полезно для управления встраиванием заданного сообщения. Оптимальное сокрытие сообщения достигается в граничном случае, когда сообщение фактически встраивается в самый младший канал.

В случае изображений с достаточно большим числом каналов троичной памяти ее младший канал удобно использовать для информации, сопровождающей факт сокрытия сообщения, например, в задачах контроля утечки информации, в том числе, скрытой в других каналах троичной памяти.

10. Сравнение с известными решениями

Относительно низкий объем встраивания кодов сообщения, который характерен для современных решений в области стеганографии, связан, прежде всего, с противоречивостью условий решения задачи, справедливо отмечаемой в [6]. По нашему мнению, основным источником противоречий является неточная формализация условия незаметного встраивания сообщения, которое отождествляется с метрической близостью контейнера и стего-изображения. Условие метрической близости стего-изображения и контейнера препятствует оптимизации сокрытия сообщений, поскольку:

- логически не согласуется с предположением о контейнере, который не доступен на приемном конце;
- ограничивает возможный объем сообщения;
- препятствует встраиванию сообщения одновременно с упрощением стего-изображения за счет сокращения числа градаций яркости (сопутствующее изменение гистограммы влечет большое поточечное среднеквадратичное отклонение);
- ограничивает возможности инвариантного встраивания сообщения независимо от предусмотренных преобразований;
- препятствует робастному встраиванию сообщения с периодическими повторениями по координатам и вложенным диапазонам допустимого варьирования яркости.

где, в отличие от *инвариантности* (сохранения в точном смысле), под *робастностью* (устойчивостью к возможным случайным или преднамеренным помехам при передаче) понимается неполное, неточное сохранение сообщения, которое исследуется на примерах заранее известных искажений в виде линейных преобразований, JPEG-компрессии, добавления шумов и пр.

Другим типичным постановочным недостатком современных решений, выполняющих встраивание сообщения по результатам анализа контейнера [7], является несовпадение результатов анализа для контейнера и стего-изображения, которое компенсируется указанием сведений о размещении ко-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

дов сообщения в стего-изображении независимо от маскирующего контекста передаваемого сигнала. При этом в [5] прямое или косвенное (алгоритмическое) указание списка координат встроенных кодов сообщения предлагается считать в стеганографии атрибутивным аналогом криптографического ключа, что, например, ограничивает возможности использования стеганографии для независимой передачи ключевой криптографической информации.

Вышеуказанные недостатки преодолеваются в предложенном подходе, в котором решение строится на низком уровне запоминания и извлечения произвольных бинарных кодов и, в зависимости условий применения, трактуется как встраивание стеганографического сообщения относительно большого объема, или произвольного водяного знака.

Упрощенная блок-схема обратимого встраивания в нашем подходе приведена на рис. 7.

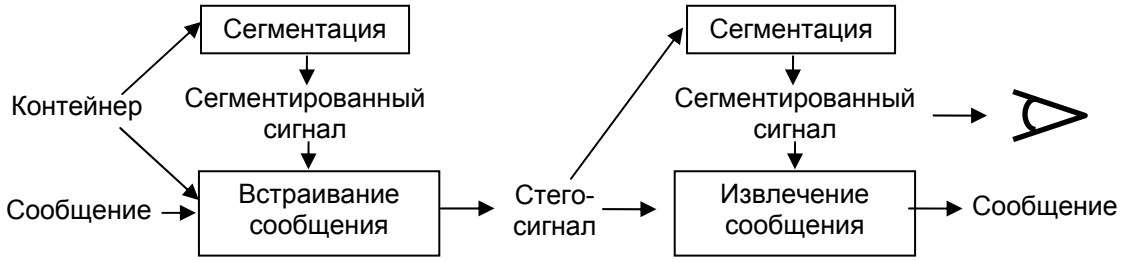

Рис. 7. Блок-схема встраивания и извлечения сообщения в предложенном решении.

Сохранение маскирующего контекста контейнера при встраивании сообщения достигается в буквальном смысле его инвариантности относительно внедрения кодов сообщения, при котором контейнер сохраняется в упрощенном (сегментированном) виде. Тот же сегментированный контейнер используется вместо сопутствующих сведений о размещении встроенных кодов.

В результате сегментации по алгоритмам улучшения качества изображения [10] контейнер необратимым образом, но без существенного ущерба для зрительного восприятия преобразуется в упрощенное представление изображения — сегментированный сигнал (контейнер или стего-изображение) с ограниченным числом градаций, который задается вычисляемым множеством яркостей неизменных пикселов и сохраняется при встраивании сообщения. Не меняющиеся при встраивании пикселы являются экстремальными в определенным образом вычисленных диапазонах яркости и задают начало отсчета, а также пределы изменения остальных, модифицируемых пикселов промежуточной яркости, изменением которых кодируется сообщение. Таким образом, сегментированный контейнер, равно как и сегментированное стего-изображение, служат неизменным началом отсчета модификации яркостных значений, используемым для кодирования сообщения.

Робастность сообщения в точном смысле его сохранения при предусмотренных линейных и нелинейных *изоморфных* преобразованиях стего-изображения (упаковки, растяжения, эквидистантной нормировки по яркости и пр.) обеспечивается за счет предварительного преобразования контейнера при встраивании сообщения, а при извлечении сообщения — стего-изображения, в инвариантное гомоморфное идемпотентное представление. Робастность, устойчивость сообщения к не предусмотренным искажениям стего-изображения обеспечивается за счет геометрического повторения кодов сообщения в грани-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

цах контейнера и во вложенных диапазонах допустимого варьирования яркости, а также за счет кодирования сообщения относительно большими яркостными перепадами.

11. Заключение

Задачу стеганографии часто характеризуют как задачу сокрытия факта встраивания сообщения в сигнале-контейнере. В нашем понимании она формулируется как задача обратимого встраивания сообщения без разрушения контейнера и формализуется, как описано выше. Следует отметить, что в работе рассмотрены только принципиальные моменты решения задачи стеганографии, которые позволяют преодолеть типичные недостатки современных методов использования скрытых коммуникаций. Для практического развития прикладного программного обеспечения и технологии решения стеганографических задач в рамках предложенного решения необходимо предусмотреть способы параметризации алгоритмов встраивания в зависимости от выбираемого пользователем «ключа», а также способы управления локальным встраиванием кодов сообщения по указанию пользователя, которые возможно разработать для заинтересованных сторон.

С научной точки зрения более интересным продолжением исследований представляется развитие методов анализа и обработки изображений в терминах чтения, преобразования и записи в троичную многоканальную память содержащейся в них природной, шумовой и пр. информации. Указанное направление планируется развивать в приложении к изображениям, а также к аудиосигналам в процессе продолжения работ.

Литература

1. *Брусенцов Н. П.* Вычислительная машина «Сетунь» Московского государственного университета // Новые разработки в области вычислительной математики и вычислительной техники. Киев, 1960. С. 226–234.
2. *Брусенцов Н. П.* Реставрация логики. М.: Новое тысячелетие, 2005. 165 с.
3. *Колмогоров А. Н., Кондратов А. М*. Ритмика поэм Маяковского // Вопросы языкознания. 1962. № 3. С. 62–74.
4. *Колмогоров А. Н.* Три подхода к определению понятия «Количество информации» // Проблемы передачи информации. 1965. Вып. 1, том 1. С. 3–8.
5. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 258 с.
6. *Chen B., Wornell G. W.* Quantization index modulation: A class of provably good methods of digital watermarking and information embedding // IEEE Transactions on Information Theory, May 2001. Vol. 47. P. 1423–1443.
7. *Hirohisa H.* A data embedding method using BPCS principle with new complexity measures // Proc. of Pacific Rim Workshop on Digital Steganography, 2002. P. 30–47.
8. *Кнут Д. Е.* Искусство программирования для ЭВМ. Получисленные алгоритмы. М.: Мир, 1977. т. 2. 724 с.
9. *Харинов М. В., Горохов В. Л.* Псевдотроичная система счисления и анализ изображений // Известия вузов России. Радиоэлектроника. СПб., 2003. Вып. 2. С. 49–53.
10. *Прэтт У*. Цифровая обработка изображений: В 2-х кн. М.: Мир, 1982. 714 с.