

Харинов М. В., Заболотский В. П.

СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ДОКУМЕНТОВ НА ОСНОВЕ МОДЕЛИ ЗАПОМИНАНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ

Аннотация. В статье описывается модель изображения, в которой его атрибутом считается «виртуальная» цифровая память, подобная памяти компьютера. Коды представления информации в виртуальной памяти разделяются на фиксированные, сохраняющие данные исходного изображения, и переменные коды «сообщения», которое записывается в виртуальную память для защиты изображения. На примере денежных знаков предлагается способ стеганографической защиты обычных и электронных документов. — Библ. 11 назв.

Ключевые слова: изображение, информация, кодирование, количество информации, стеганография, защита, цифровая память.

Abstract. In this paper, we describe a model of image attributed with its own digital hardware-independent memory (named virtual memory) which is similar to a memory of computer. The codes of image representation in virtual memory are divided into fixed and modifiable. The former store the information of source image and the latter contain the variable codes of the message embedded into the virtual memory to protect the image. By the example of banknotes the technique of steganography protection of usual and electronic documents is discussed. — Bibl. 11 items.

Keywords: image, information, encoding, information amount, steganography, protection, digital memory.

Введение

В современных задачах обработки сигналов (изображений) из заведомо не ограниченной предметной области возникает проблема уточнения понятия информации, а также её представления в виде конкретных кодов для унификации формального описания изображения при решении различных прикладных задач. В задачах распознавания, например, необходимо уметь вычислять общие признаки пикселей (элементарных клеток) изображения, дополняющие стандартную яркость. Формализация информации, содержащейся в каждом пикселе изображения, и описание ее количества, полезны для унификации обработки различного типа изображений, а также сигналов различной природы. Однако при этом возникает проблема логического и экспериментального обоснования решений.

Непосредственная практическая проверка варианта формализации понятия информации [1, 2] достигается в задаче обратимого встраивания максимального объема произвольных кодов информации одного сигнала (сообщения) в другой сигнал (контейнер) в условиях, когда при приеме контейнер сохраняется в упрощенном (сегментированном) виде, и оба сигнала считаются не известными. Интерпретация понятия информации строится в предполо-

жении, что сигнал (изображение) независимо от представления при обработке, или передаче обладает автономной цифровой памятью, названной «виртуальной». Виртуальная память хранит коды фиксированной информации контейнера и переменной информации сообщения независимо от предусмотренных преобразований сигнала, например, затухания в процессе передачи и может использоваться для хранения, передачи, а также обработки информации аналогично памяти компьютера или любого другого устройства. В настоящей статье предлагается простейший вариант модели изображения с виртуальной памятью, и на доступном примере обсуждается ее применение для защиты документов.

Особенности виртуальной памяти

Виртуальная память определяется как формальная матрица ячеек с кодами информации, которые вычисляются по изображению с сохранением порядка яркостей и определяют количество информации в пикселях изображения. Каждому пикселу изображения сопоставляется ячейка виртуальной памяти. Подобно ячейкам компьютерной памяти, виртуальные ячейки содержат одинаковое число разрядов. Однако число разрядов виртуальной памяти зависит от изображения и, вообще говоря, превышает число разрядов в исходном компьютерном представлении, например, вдвое. Подобно тому, как биты памяти компьютера объединяются в битовые плоскости, запоминающие элементы поразрядно составляют «каналы» виртуальной памяти.

Основной особенностью виртуальной памяти является то, что ее запоминающие элементы разделяются на переменные (read-write), значения которых можно модифицировать подобно значениям битов в компьютере, и фиксированные (read-only), значения которых можно только читать. Разделение запоминающих элементов виртуальной памяти на переменные и фиксированные выполняется так, что позволяет при адаптивной обработке записать в переменные запоминающие элементы произвольное сообщение и восстановить контейнер в упрощенном (сегментированном) виде за счет сохранения фиксированных запоминающих элементов.

В отличие от ячеек памяти компьютера ячейки виртуальной памяти состоят не из битов, а из тритов, принимающих три значения (0 и ± 1). Триты с нулевыми значениями относятся к фиксированным. Для переменных тритов определяется две операции — изменение значения трита на противоположное и преобразование переменного трита в фиксированный. Модификация переменных тритов поддерживает запись в виртуальную память заданного троичного сообщения из 0 и ± 1 , нулевые триты которого при чтении информации обозначают неопределенное значение, сопоставляемое фиксированным тритам виртуальной памяти, а при записи трактуются как пропуск встраивания сообщения, кодируемый преобразованием переменных тритов в фиксированные. Число фиксированных, в частности, нулевых тритов

возрастает с убыванием разряда виртуальной памяти, и для встраивания сообщения максимального объема эффективно использовать старшие разряды виртуальной памяти. Как показывает эксперимент, при встраивании сообщения в виртуальную память с пропуском нескольких старших разрядов допустимо считать, что фиксированные триты содержат явную, а переменные триты — неявную информацию изображения.

Модификация тритов виртуальной памяти отображается соответствующими преобразованиями яркостей пикселей изображения.

Модель виртуальной памяти

Для построения виртуальной памяти шкала яркости итеративно разбивается на диапазоны так, чтобы в каждый диапазон очередного разбиения попадало приблизительно равное число пикселей. При этом, если рассматривать яркость данного пикселя, то на каждом шаге к ней приближается одна из границ диапазона, который содержит эту яркость. При каждом разбиении шкалы яркости на диапазоны вычисляются триты очередного разряда виртуальной памяти. Если яркость данного пикселя изображения при разделении рассматриваемого диапазона оказывается в числе больших яркостей, то соответствующему триту виртуальной памяти приписывается положительное значение, если оказывается в числе меньших, то отрицательное. Для единственной яркости вырожденного (неделимого) диапазона значение трита виртуальной памяти полагается нулевым. Для изменения значения трита на противоположное яркость пикселя замещается яркостью из альтернативного диапазона.

К фиксированным относят триты, которые сопоставляются пикселям с граничными яркостями, а остальные триты считаются переменными. Для фиксирования («прошивания») значения трита в данном разряде виртуальной памяти яркость пикселя замещается одной из граничных яркостей соответствующего диапазона.

Количество информации, содержащейся в данном пикселе изображения, определяется числом переменных тритов, т.е. объемом сообщения, которое можно записать в ячейку виртуальной памяти данного пикселя изображения. Количество информации для изображения в целом получается суммированием оценок, полученных для пикселей. При преобразовании переменных тритов в фиксированные количество информации в ячейках виртуальной памяти падает, а на изображении уменьшается число пикселей различной яркости.

Запись кодов информации в переменные триты виртуальной памяти осуществляется последовательно — от старших каналов к младшим. Запись сообщения в очередной канал виртуальной памяти не влияет на информацию в предыдущих каналах, но изменяет используемое разбиение шкалы яркости и нарушает информацию в последующих каналах. Поэтому формирование требуемого сообщения в каждом канале сопровождается восстановлением кодов информации в последующих каналах, и для заполнения переменных тритов виртуальной

памяти желаемыми значениями запись сообщения в очередной канал с восстановлением информации в последующих каналах повторяется до достижения точного предела, когда изображение и виртуальная память не перестают меняться.

В задачах стеганографии и других, связанных с учетом неформализованного зрительного восприятия, прозрачность модели и алгоритмов ее программной реализации необходима для достижения опытным путем требуемого эффекта сокрытия или, наоборот, проявления сообщения. При этом объем сообщения достигает 70% от объема контейнера, а при условии неявного встраивания составляет 30-50%.

Обоснование модели

Для экспериментального обоснования модели виртуальной памяти полезно сопоставить классические оценки количества информации с оценкой количества информации согласно модели, которая, в отличие от классических оценок получается целочисленной (см. рис. 1).

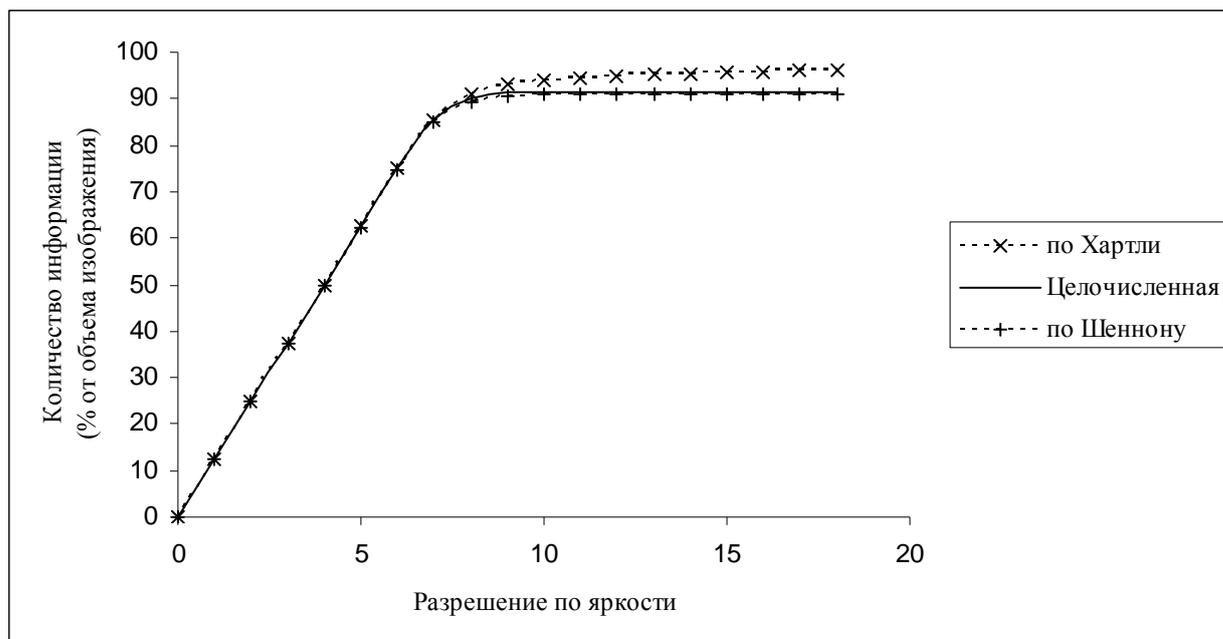


Рис. 1. Оценки количества информации.

Рис. 1 демонстрирует целочисленную оценку количества информации, которая получена для некоторого изображения и рассматривается в зависимости от разрешения по яркости (числа рассматриваемых старших разрядов виртуальной памяти) и сравнивается с классическими оценками по Р. В. Хартли [3] и К. Э. Шеннону [4]. Значения целочисленной оценки, выделенные сплошной линией, оказываются в границах классических оценок, выделенных пунктиром. При низком разрешении по яркости целочисленная оценка количества информации совпадает с оценкой по Р.В.Хартли и описывает однородную картину распределения количества информации по пикселям изображения. С ростом разрешения проявляется заметное различие между оценками по Р. В. Хартли и К. Э. Шеннону, тогда как цело-

численная оценка приближается к шенноновской и совпадает с ней в пределах 0.5-1%. При этом среднее значение целочисленного количества информации, в расчете на пиксел изображения, описывается в виде:

$$\log_2 m \geq \frac{1}{N} \sum_{i=1}^N q_i \geq \frac{1}{N} \sum_{i=1}^N \log_2 \left(\frac{N}{n_i} \right),$$

где q_i — целочисленное количество информации в i -м пикселе, N — число пикселей в представлении изображения, m — число встречающихся градаций яркости, n_i — встречаемость пиксела, т. е. число пикселей в изображении, совпадающих с i -м пикселем по яркости.

Таким образом, модель виртуальной памяти обеспечивает оценку количества информации, которая согласуется с классическими оценками, и в дополнение к известным способам целочисленной интерпретации количества информации [5] позволяет предложить новый способ выражения количества информации в целых числах.

Применение для защиты документов

Согласно обсуждаемой модели информация изображения независимо от его исходного представления (в памяти компьютера, на бумаге и пр.) содержится в самостоятельной цифровой памяти. Цифровая виртуальная память порождается некоторым контейнером, а контейнер, в частности электронный документ, уподобляется документу, записанному на физическом носителе информации. В случае обычных документов, например, денежных купюр, физический носитель изображения сам по себе является источником информации. В этом случае для предотвращения подделки необходимо защитить не только цифровое изображение как электронный документ, но и бумажный носитель, на котором оно печатается.

Для сформулированных задач модель сигнала с виртуальной памятью позволяет построить наглядное решение (см. рис. 2).

Рис. 2 иллюстрирует эффект встраивания сообщения (стандартного изображения «Лена» в двухградационном представлении) в последовательные каналы (разряды) виртуальной памяти контейнера в виде денежной купюры. В левом столбце изображений сверху показан исходный контейнер, а под ним — представления информации трех старших каналов виртуальной памяти. В следующем столбце контейнер и представления информации показаны в преобразованном виде — после встраивания сообщения в самый старший канал виртуальной памяти. Остальные столбцы иллюстрируют преобразование контейнера при встраивании сообщения в последующие каналы виртуальной памяти. Следует обратить внимание, что запись сообщения в старший канал виртуальной памяти вызывает сопутствующие искажения контейнера в младших каналах, которые подавляются процедурой восстановления в них прежней информации, что позволяет избежать накопления искажений при многоканальном встраивании сообщения.

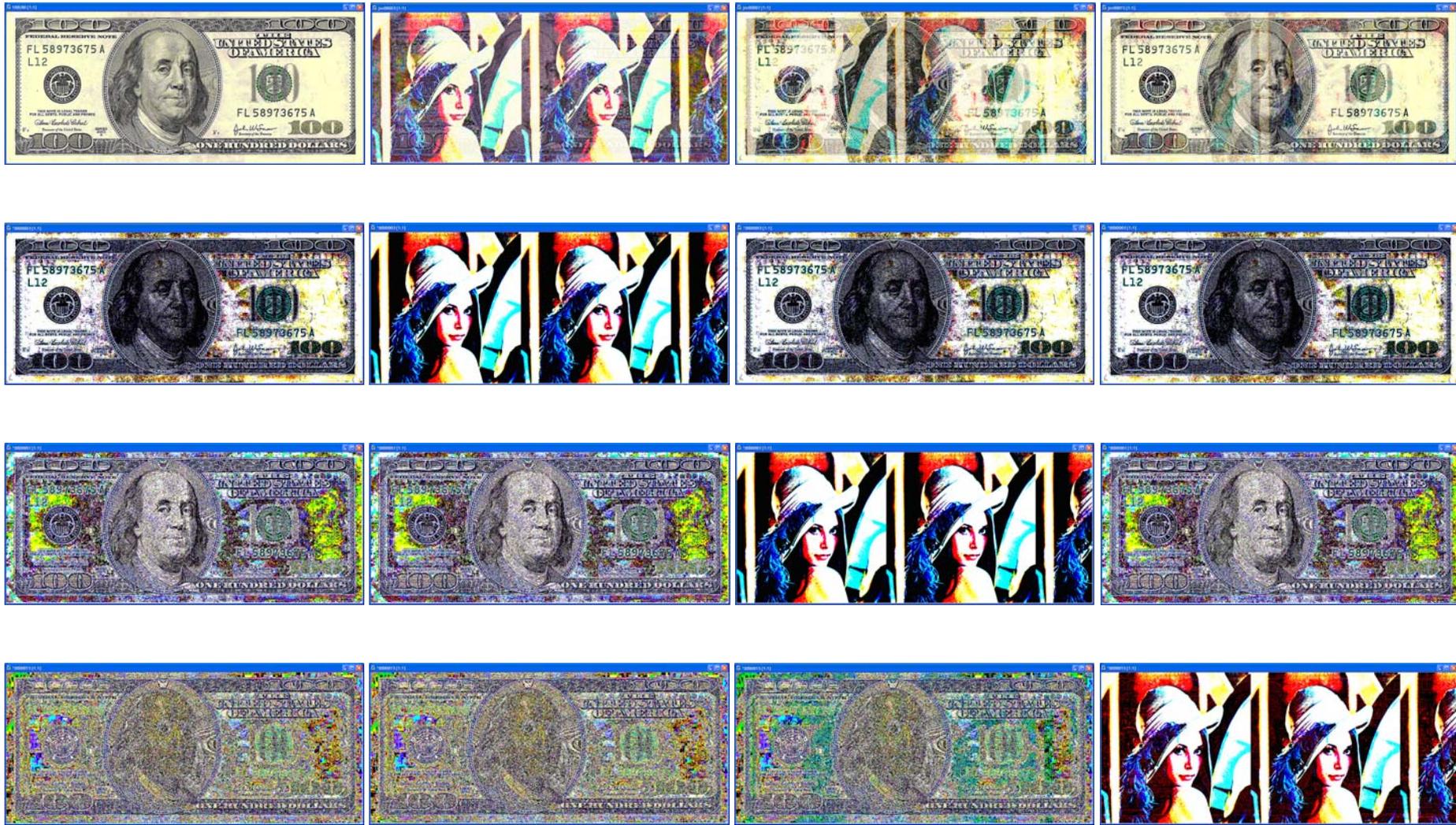


Рис. 2. Запись сообщения в последовательные каналы виртуальной памяти.

На верхних изображениях со встроенным сообщением, можно рассмотреть как контейнер, так и сообщение, причем визуальное комбинирование сигналов сочетается с возможностью их автоматического разделения, что для современной обработки изображений представляет самостоятельный интерес. Характерно, что на обсуждаемых изображениях наблюдается преимущественно информация, содержащаяся в паре старших каналов виртуальной памяти. Информация, содержащаяся в последующих каналах, оказывается менее заметной, что в сочетании с возможностью пропуска записи сообщения упрощает встраивание в них стеганографических сообщений, и для повышения объема неявного сообщения оказывается более продуктивным, чем стандартное условие встраивания сообщения в несколько младших разрядов памяти компьютера [6].

Для индивидуальной защиты каждой купюры без создания специальной базы данных имеет смысл использовать бумажный носитель с выраженной случайной структурой (волоконнами, включениями и пр.), которые просматриваются на глаз или легко детектируются стандартными средствами. Тогда для исключения подделки посредством тиражирования купюры достаточно в качестве сообщения при печати отображать в изображении картину структуры физического носителя данных, например, в виде «теней» упомянутых волокон или включений, чтобы «привязать» изображение к конкретному физическому носителю.

Для обнаружения подделки документов посредством полной имитации процесса их изготовления со встраиванием образа физического носителя в виртуальную память изображения достаточно при генерации изображения, предназначенного для печати, использовать некоторый секретный ключ, без которого невозможно в точности воспроизвести изображение, вычисляемое для данного физического носителя. Если генерацию изображения осуществлять посредством встраивания сообщений в некоторый исходный контейнер в виде псевдослучайной картины или любого другого заданного изображения с достаточной емкостью виртуальной памяти, то контейнер может служить требуемым ключом, поскольку в упрощенном виде сохраняется в результирующем изображении.

Заключение

В работе мы на практическом примере обосновываем общедоступное понимание информации как последовательности символов, кодов, «следов» или иных «отпечатков», которые можно записать на бумаге, в памяти компьютера или ином физическом носителе информации, а также в виртуальной памяти изображения. Интерпретацию понятия информации строится в рамках комбинаторного подхода А. Н. Колмогорова, который подчеркивал, что понятие информации не обязательно связывать с понятием вероятности [7]. Количество информации оценивается в соответствии со структурным подходом к информации Ф. Е. Темникова [8, 9], в котором оно сводится к подсчету структурных элементов сигнала.

Идея «сконструировать» троичную виртуальную память из компонент изображения неожиданна. Однако то, что для обработки цифровой информации эффективно использовать именно троичную память, благодаря Н. П. Брусенцову известно почти полвека [10, 11]. Возможно, модель сигнала с троичной памятью окажется полезной для более полного раскрытия преимуществ известных решений.

Литература

1. **Kharinov M.V.** Algebraic Description of Data Embedding Basing on Idempotent Image Transformations // *Pattern Recognition and Image Analysis* / Vol. 19. No 3, 2009. — pp. 491-496.
2. **Kharinov M.V.** Invariant Representation of Information and Information Quantity in Image-Processing Tasks // *Pattern Recognition and Image Analysis* / Vol. 18. No 4, 2008. — pp. 643-648.
3. **Hartley R.V.L.** Transmission of information // *Bell System Technical Journal*. Vol. 7, No 3, 1928. — pp. 535-563.
4. **Shannon C.E.** A mathematical theory of communication // *Bell System Technical Journal*, Vol. 27. July and October, 1948. — pp. 379–423 and 623–656.
5. **Юсупов Р.М.** Теоретические основы прикладной кибернетики. Выпуск 1. Элементы теории информации. Л.: типография ВИКА им. А. Ф.Можайского, 1973. — 110 с.
6. **Грибунин В.Г., Оков И.Н., Туринцев И. В.** Цифровая стеганография. М.: Солон-Пресс, 2002. — 272 с.
7. **Колмогоров А.Н.** Три подхода к определению понятия «Количество информации» // *Проблемы передачи информации*. 1965. Вып. 1. Т. 1. — С. 3 – 8.
8. **Темников Ф. Е.** Информатика // *Известия вузов. Электромеханика*. 1963. № 11. — С. 1277.
9. **Темников Ф. Е., Афонин В. А., Дмитриев В. И.** Теоретические основы информационной техники. М.: Энергия, 1979. — 512 с.
10. **Брусенцов Н. П.** Вычислительная машина "Сетунь" Московского государственного университета. В кн.: Новые разработки в области вычислительной математики и вычислительной техники. Киев, 1960. — С. 226-234.
11. **Брусенцов Н. П.** Реставрация логики. М.: Новое тысячелетие, 2005. — 165 с.