СПОСОБ ЗАЩИТЫ ДОКУМЕНТОВ НА ОСНОВЕ МОДЕЛИ ИЗОБРАЖЕНИЯ С ЦИФРОВОЙ ПАМЯТЬЮ

М. В. Харинов[1]

Санкт-Петербургский институт информатики и автоматизации РАН

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

[1]<khar@iias.spb.su>

УДК 621.391

Харинов М. В.. **Способ защиты документов на основе модели изображения с цифровой памятью** // Труды СПИИРАН. Вып. 7. — СПб.: Наука, 2008.

Аннотация. *В статье предлагается алгебраическое описание модели изображения, в которой его атрибутом считается «виртуальная» цифровая память, подобная памяти компьютера. В виртуальной памяти кодируется последовательность инвариантных представлений изображения при различном разрешении по яркости, вычисляемых независимо от сдвига, растяжения и других стандартных преобразований яркостной шкалы. Коды представления в виртуальной памяти разделяются на фиксированные, сохраняющие информацию 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. 10 назв.

UDC 621.391

Kharinov M. V. **Document protection technique based on a model of digital memory inherent in signal** // SPIIRAS Proceedings. Issue 7. — SPb.: Nauka, 2008.

Abstract. *In this paper, we develop an algebraic description for previously proposed model of image attributed with its own digital hardware–independent memory (named virtual memory) which is similar to a memory of computer. Virtual memory contains the sequence of invariant image representations for different intensity resolutions computed independently of shifting, stretching and other standard transformations of intensity scale. 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. 10 items.

1. Введение

В задаче стеганографической защиты документов требуется незаметно встроить в изображение (контейнер) максимальный объем произвольно заданных кодов сообщения так, чтобы его можно было восстановить по результирующему стегоизображению без использования каких-либо дополнительных сведений о контейнере или сообщении [1, 2].

Как известно, человек различает на цветовом изображении примерно 60 градаций яркости или несколько сотен цветовых оттенков, которые можно закодировать 10–16 битами [3]. Поскольку яркости пикселов кодируются в изображении 24 битами, объем скрытого сообщения может составлять не менее трети объема изображения, что превышает объем встраивания, обеспечиваемый современными методами стеганографии [1, 2, 4].

Большинство методов стеганографии, поддерживающих объем встраивания сообщения более 10%, опираются на LSB-метод, в котором младшие биты контейнера замещаются битами сообщения, а старшие биты составляют маскирующую картину в виде представления контейнера при уменьшенном разрешении по яркости [1].

Недостатком маскирующей картины является то, что она меняется при ли-

нейном преобразовании яркостей пикселов изображения. На первый взгляд, указанный недостаток нетрудно устранить за счет упаковки контейнера по яркости.[1] Но тогда картина оказывается зависимой от пикселов, встречающихся на изображении в единичном экземпляре. Как упаковка контейнера по яркости, так и учет встречаемости пикселов приводит к необходимости повторять вычисления для компенсации изменений числа градаций яркости и встречаемости пикселов при встраивании сообщения. При этом возникает проблема зацикливания алгоритма встраивания, которая усугубляется погрешностями расчетов в целых числах.

Перечисленные трудности удается преодолеть в модели изображения [5]. Модель обеспечивает повышение объема встраивания сообщения за счет вычисления независимых цветовых компонент маскирующей картины по алгоритму улучшения качества изображения посредством выравнивания гистограммы [6].

2. Особенности виртуальной памяти

В обсуждаемой модели изображение рассматривается как своеобразное устройство для передачи данных, которое независимо от цифровой или аналоговой формы представления обладает автономной «виртуальной» цифровой памятью, способной сохранять следы формирования и обработки изображения, искажений и шумов при передаче, или коды сообщения в определенных пределах трансформации изображения при затухании и дискретизации передаваемого сигнала.

Виртуальная память вычисляется по изображению и состоит из запоминающих ячеек. Ячейки виртуальной памяти взаимно однозначно сопоставляются пикселам изображения и в свою очередь состоят из одинакового числа упорядоченных запоминающих элементов, различаемых по разряду. Подобно тому как биты в памяти компьютера составляют битовые плоскости, запоминающие элементы поразрядно объединяются в «каналы» виртуальной памяти.

Основной особенностью виртуальной памяти является то, что ее запоминающие элементы с учетом встречаемости пикселов разделяются на переменные (read-write), значения которых можно модифицировать подобно значениям битов в компьютере, и фиксированные (read-only), значения которых можно только читать. При этом фиксированные запоминающие элементы группируются в младших разрядах виртуальной памяти и в противоположность LSB-методу при использовании виртуальной памяти объем встраивания кодов сообщения падает с убыванием разряда.

Общий объем виртуальной памяти пропорционален числу разрядов, которое вычисляется по изображению и для большинства изображений превышает объем памяти, занимаемый изображением в компьютере, например вдвое. При этом бóльшую часть объема виртуальной памяти занимают фиксированные запоминающие элементы, тогда как переменные запоминающие элементы в пересчете на объем изображения занимают 70-90% и определяют суммарный объем, доступный для явного и неявного встраивания сообщения.

Полезной особенностью виртуальной памяти является то, что ее запоми-

[1] Упаковка по яркости сводится к нумерации по порядку встречающихся на изображении значений яркости и замещению полученными номерами исходных значений яркости пикселов изображения.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

нающими элементами служат не биты, как в современных компьютерах, а триты, как в ЭВМ Н. П. Брусенцова, которые по сравнению с битами принимают одно дополнительное значение [7]. В задаче стеганографии указанное дополнительное значение при считывании данных из виртуальной памяти интерпретируется как пропуск записи передаваемого бинарного сообщения, а при записи — как исключение записи бинарного сообщения в указанный трит виртуальной памяти посредством его преобразования в фиксированный. Таким образом, сообщение в целом также оказывается троичным, что обеспечивает управление распределением данных по пикселам и каналам виртуальной памяти.

Триты ячейки виртуальной памяти сопоставляются значению яркости пиксела, рассматриваемому в последовательности вложенных диапазонов яркости, которые вычисляются по изображению из условия максимально близкой встречаемости пикселов. Более подробно способ построения виртуальной памяти описан в одном из предыдущих выпусков сборника [5]. В настоящей статье он дополняется математическим описанием модели.

3. Алгебраическая схема

Пусть u — изображение; Hu — представление изображения в виртуальной памяти, получаемое преобразованием H по алгоритму из класса алгоритмов улучшения качества изображений [4, 6, 8]. Преобразование H отображает множество изображений во множество инвариантных представлений со сглаженными гистограммами, причем независимо от упаковки исходных изображений по яркости.

Преобразование H состоит в перераспределении встречающихся значений пикселов на шкале яркости так, чтобы при определенном арифметическом преобразовании A они объединялись между собой в установленном порядке, вычисляемом из условия равновероятной встречаемости пикселов изображения. При этом значения пикселов представления Hu формируются в «псевдотроичной» системе счисления, в которой преобразование A сводится к делению нечетных значений пикселов нацело пополам и удвоению четных значений, предварительно поделенных нацело на четыре [5, 8]. Итеративное применение преобразования A не выводит из множества инвариантных представлений Hu изображений u:

$$HA^nH = A^nH, \quad n = 0, 1, 2, \ldots,$$

и описывает сдвиг тритов в ячейках троичной виртуальной памяти, подобно тому как деление нацело пополам описывает сдвиг битов в ячейках двоичной памяти компьютера. Представления A^nHu изображения u при различных n записываются в том или ином числе разрядов виртуальной памяти и трактуются как инвариантные представления изображения при различном разрешении по яркости. Очередная плоскость тритов виртуальной памяти T_nu, состоящая из тритов одного разряда, вычисляется при последовательных значениях разрешения по яркости для каждой пары представлений изображения по разностной схеме, как в двоичной системе счисления:

$$T_nu = \left(A^n - 2A^{n+1}\right)Hu.$$

Пусть W — преобразование изображения u в изображение Wu со встро-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

енными кодами установленного сообщения. При этом коды сообщения встраиваются в изображение u, а извлекаются из инвариантного представления HWu и преобразование W определяется в рамках условия, что в различных комбинациях с преобразованием H оно порождает отображение множества изображений u на множество инвариантных представлений HWu изображений со встроенным сообщением. Указанное условие выполняется благодаря поддерживаемым в модели виртуальной памяти алгебраическим соотношениям:

$$H^2 = H, \quad W^2 = W,$$

$$HWH = WHW = HW,$$

которые иллюстрируются рис. 1.

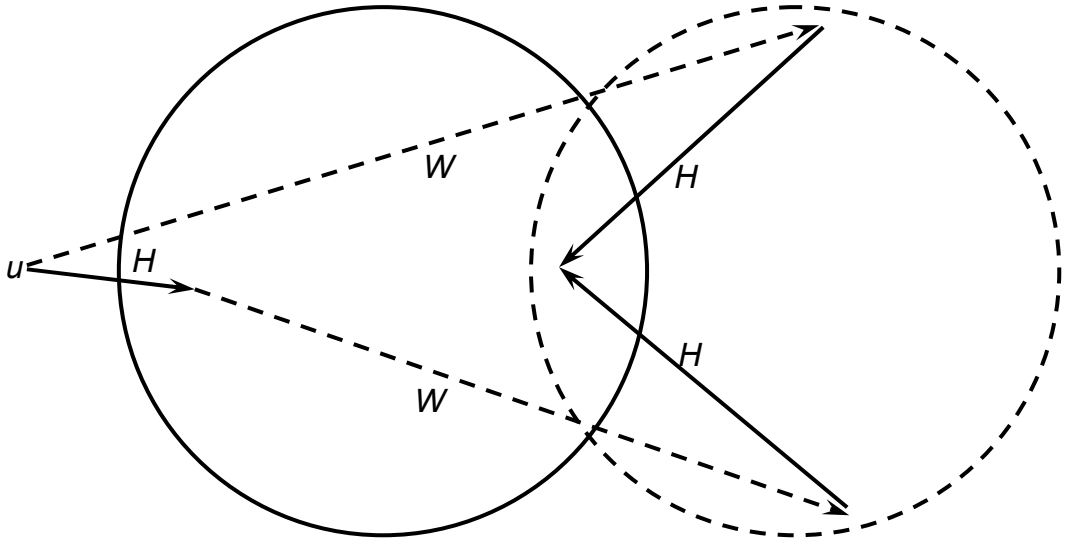

Рис. 1. Алгебраическая схема получения инвариантного представления изображения со встроенным сообщением.

На рис. 1 сплошными линиями обозначены преобразование H и множество инвариантных представлений изображений, пунктиром — преобразование W и множество изображений со встроенным сообщением. Пересечение кругов обозначает множество инвариантных представлений изображений со встроенным сообщением.

Как показано на рис. 1, H не выводит из множества изображений с рассматриваемым сообщением и коммутирует с преобразованием HW. Сообщение встраивается в доступный объем виртуальной памяти двумя различными способами, которые приводят к одному и тому же инвариантному представлению HWu изображения со встроенным сообщением. При этом если изображения, совпадающие при упаковке по яркости, считать изоморфными по яркостному порядку, то исходное изображение с точностью до изоморфизма « ~ » совпадает со своим инвариантным представлением, а все три представления изображения со встроенным сообщением оказываются изоморфными друг другу:

$$u \sim Hu, \quad WHu \sim HWu \sim Wu.$$

Выписанные отношения изоморфизма выполняются благодаря аналогии алгебраических свойств упаковки по яркости N и преобразования H:

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

$$N^2 = N, \quad H^2 = H,$$

$$NH = N, \quad HN = H,$$

которые порождают одно и то же разбиение множества изображений u, v на классы изоморфных элементов:

$$Nu = Nv \quad \Leftrightarrow \quad u \sim v \quad \Leftrightarrow \quad Hu = Hv.$$

4. Применение для защиты документов

Приведенная алгебраическая схема описывает преобразование кодированных в изображении данных, которые, согласно обсуждаемой модели, содержатся в приписанной изображению цифровой виртуальной памяти. В терминологии стеганографии виртуальная память порождается контейнером, а контейнер, в частности электронный документ, уподобляется документу, записанному на физическом носителе данных. В случае обычных документов, например денежных купюр, физический носитель изображения сам по себе является источником данных. 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, поясняемое рис.2.

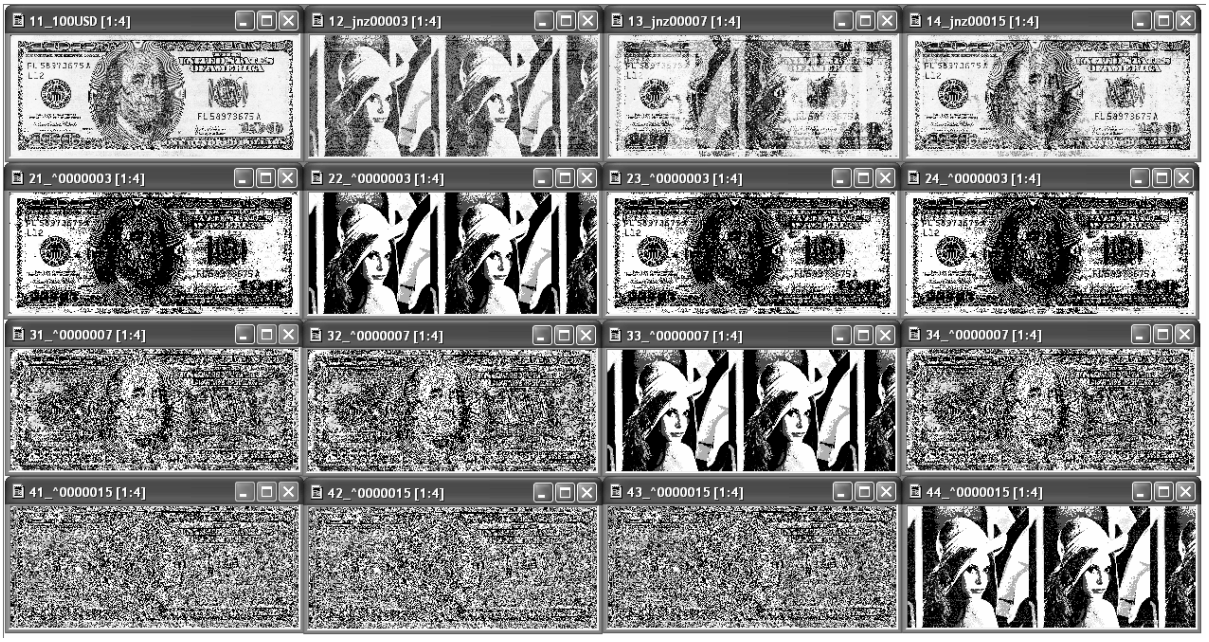

Рис.2. Запись сообщения в последовательные каналы виртуальной памяти.

Рис.2 иллюстрирует эффект встраивания сообщения (стандартное изображение «Лена» в двухградационном представлении) в последовательные каналы (разряды) виртуальной памяти цветовых компонентов контейнера в виде денежной купюры. В левом столбце изображений сверху показан исходный контейнер, а под ним — представления изображения в трех старших каналах виртуальной памяти. В следующем столбце контейнер и представления изображения показаны в преобразованном виде — после встраивания сообщения в самый старший канал виртуальной памяти. Остальные столбцы иллюстрируют

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

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 изображения при многоканальном встраивании сообщения.

На верхних изображениях со встроенным сообщением можно рассмотреть как контейнер, так и сообщение, причем визуальное комбинирование сигналов сочетается с возможностью их автоматического разделения. Характерно, что на обсуждаемых изображениях наблюдается преимущественно информация, содержащаяся в паре старших каналов виртуальной памяти. Информация, содержащаяся в последующем каналах, оказывается менее заметной, что в сочетании с возможностью пропуска записи сообщения упрощает встраивание в них стеганографических сообщений, обеспечивает повышение объема неявного сообщения до 30–50% и оказывается более продуктивным, чем стандартное условие встраивания сообщения в несколько младших разрядов памяти компьютера в LSB-методе.

Для индивидуальной защиты каждой купюры без создания специальной базы данных имеет смысл использовать бумажный носитель с выраженной случайной структурой (волокнами, 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 воспроизведения встраивания 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 данных в некоторый секретный контейнер в виде псевдослучайной картины или любого другого заданного изображения с достаточной емкостью виртуальной памяти, то контейнер может служить требуемым ключом, поскольку в кодированном виде он частично сохраняется в результирующем изображении.

5. Заключение

Помимо задач стеганографии модель может применяться в редакторах изображений (Photoshop и др.), а также в программах создания изображений (CorelDraw и др.), в которых для изображений, заданных в обычном матричном формате, можно реализовать режим послойной генерации объектов, разделяя объекты в каналах виртуальной памяти.

С теоретической точки зрения модель интересно применить для уточнения понятия информации изображения в рамках структурного подхода [9, 10]. В указанном подходе в качестве информационных элементов (носителей единиц информации) можно рассматривать триты виртуальной памяти, что планируется выполнить в перспективе продолжения работ.

Литература

1. *Грибунин В .Г., Оков И. Н., Туринцев И. В*. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.
2. *Оков И. Н.* Аутентификация речевых сообщений и изображений в каналах связи / Под ред. В.Ф. Комаровича. СПб.: Изд-во Политехнич. ун-та, 2006. 392 с.
3. *Александров В. В., Горский Н. Д.* ЭВМ видит мир. Л.: Машиностроение, 1990. 140 с.
4. *Харинов М. В.* Адаптивное встраивание водяных знаков по нескольким каналам, патент РФ № 2329522, заявители: СПИИРАН–«Самсунг Электроникс Ко., Лтд.» // Официальный Бюллетень Патентного ведомства Российской Федерации № 20 от 20.07.2008. 41 с.
5. *Харинов М. В*. Модель цифрового изображения с виртуальной памятью на основе псевдотроичной системы счисления // Труды СПИИРАН (к 30–летию СПИИРАН) / Под ред. чл.–кор. РАН Р. М. Юсупова. СПб: Наука, 2007. Вып. 4. С. 126–135.
6. *Прэтт У.* Цифровая обработка изображений. Том 1–2. М.: Мир, 1982. 1200 с.
7. *Брусенцов Н. П.* Вычислительная машина "Сетунь" Московского государственного университета // Новые разработки в области вычислительной математики и вычислительной техники. Киев, 1960. С. 226–234.
8. *Харинов М. В.* Запоминание и адаптивная обработка информации цифровых изображений / Под ред. Р. М. Юсупова. СПб.: Изд-во С.–Петерб. ун-та, 2006. 138 с.
9. *Темников Ф. Е*. Информатика // Известия вузов. Электромеханика. 1963. № 11. С. 1277.
10. *Юсупов Р. М.* Теоретические основы прикладной кибернетики. Вып. 1. Элементы теории информации. Л: Типография ВИКА им. А. Ф. Можайского, 1973. 110 с.