

МОДИФИКАЦИЯ МЕТОДА КУТТЕРА-ДЖОРДАНА-БОССЕНА СКРЫТОГО ХРАНЕНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ ФОРМАТА JPEG

А.Е. Дизер

студент, e-mail: ahemoh@gmail.com

Е.С. Дизер

аспирант, e-mail: e.s.dizer@gmail.com

Т.М. Опарина

старший преподаватель, e-mail: oparina2007@yandex.ru

Омский государственный университет им. Ф.М. Достоевского

Аннотация. В данной статье представлена модификация метода Куттера-Джордана-Боссена, целью которой было повышение устойчивости стеганоконтейнеров к различным видам атак, увеличение количества скрываемой информации в графическом файле и корректность считывания скрытой информации.

Ключевые слова: стеганография, стеганоконтейнер, метод Куттера-Джордана-Боссена.

Введение

Стеганографическая система или стегосистема — совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. Обобщённая модель такой системы представлена (см. рис. 1).

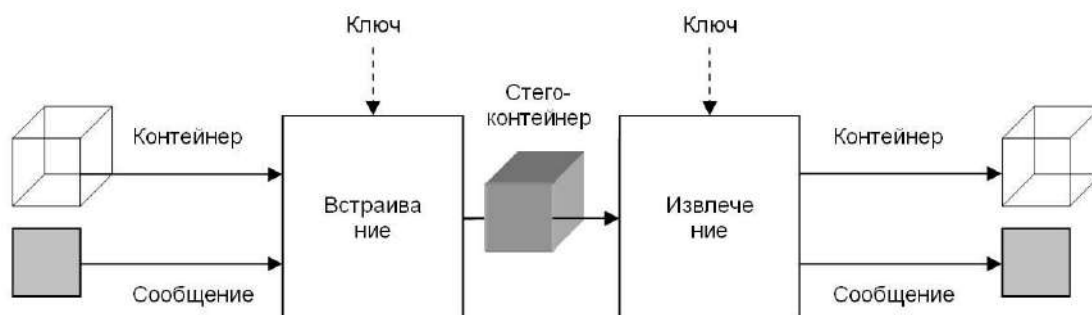


Рис. 1. Обобщенная модель стегосистемы

При построении стегосистемы должны учитываться следующие положения:

1. Противник имеет полное представление о стеганографической системе и деталях её реализации. Единственной информацией, которая остаётся неизвестной, является ключ, который позволяет установить факт наличия и получения скрытого сообщения.
2. Если противник каким-либо образом устанавливает факт наличия скрытого сообщения, то он не должен иметь возможность прочитать подобные сообщения из других данных до тех пор, пока ключ хранится в тайне.
3. Потенциальный противник должен быть лишён технических или каких-либо иных преимуществ в раскрытии содержимого тайных сообщений.

Далее будем использовать следующие понятия:

Контейнер — любая информация, которую можно использовать для сокрытия секретных сообщений. Пустой контейнер — контейнер без встроенного сообщения, а стегоконтейнер — со встроенной информацией.

Стеганографический канал или стегоканал — канал передачи скрытых сообщений.

Стегоключ — секретный ключ, который необходим для сокрытия секретного сообщения. Допускается использование нескольких стегоключей.

Согласно [1] все алгоритмы внедрения скрытой информации можно разделить на группы:

1. Алгоритмы, работающие с самим цифровым сигналом.
2. Алгоритмы, накладывающие скрытую информацию (изображения, звука, иногда текста) поверх оригинала.
3. Алгоритмы, связанные с особенностями форматов файлов.

Из группы методов сокрытия данных в графических файлах выберем и рассмотрим для реализации метод Куттера-Джордана-Боссена [4]. Для встраивания информации в контейнер используется одно из свойств зрительной системы человека, которое заключается в том, что восприимчивость человека к изменениям яркости синего цвета по сравнению с красным и зелёным — меньше всего, поэтому для встраивания скрытой информации методом Куттера-Джордана-Боссена используется синий цвет заданного контейнера-изображения.

Функции встраивания и извлечения в методе Куттера-Джордана-Боссена не симметричны. Следовательно, хотя правильное распознавание бита сообщения является высоковероятным, но не является стопроцентным, поэтому для уменьшения вероятности ошибок извлечения было предложено в процессе встраивания каждый бит повторять несколько раз (многократное встраивание). Следует отметить, что увеличение количества повторений существенно уменьшает вероятность возникновения ошибок при извлечении скрытого сообщения, но также это негативно отразится на вместимости стегоконтейнера.

1. Анализ существующих модификаций метода Куттера-Джордана-Боссена

В работах [2] и [3] были предложены модификации метода, которые направлены на преодоление проблем переполнения на этапе встраивания бита данных [2] и уменьшение вносимых в контейнер изменений [3]. Однако остаётся актуальным ряд недостатков, один из которых – это вероятностный характер чтения внедрённой информации из графического изображения. Это связано с тем, что встраивание бита данных происходит путём изменения синей составляющей цвета. При этом есть большая вероятность того, что изменённой яркости будет недостаточно для того, чтобы верно считать данный бит. Такая ситуация может возникнуть при встраивании бита «1» в тёмный пиксель на светлом фоне, либо встраивании «0» в светлый пиксель на тёмном фоне. При последующем чтении данного бита в большинстве случаев результат не будет корректным.

Если же попытаться изменить яркость синей составляющей настолько, чтобы при чтении результат был правильным, то это приведёт к сильному изменению цвета пикселя, и он будет выделяться на общем фоне (см. рис. 2).

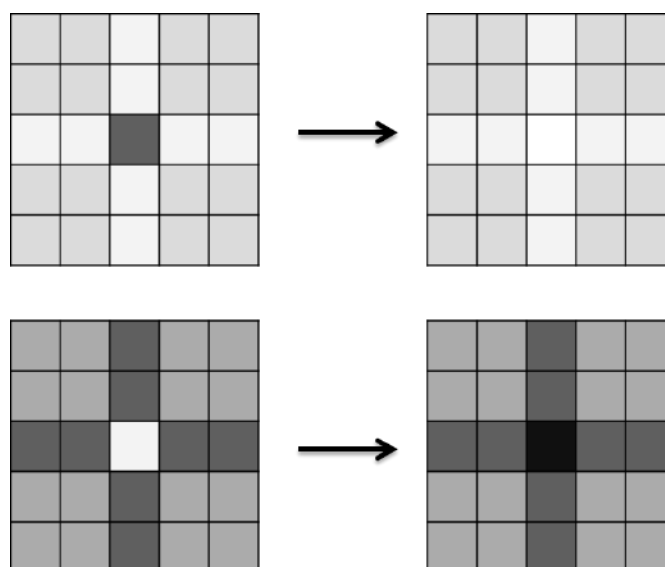
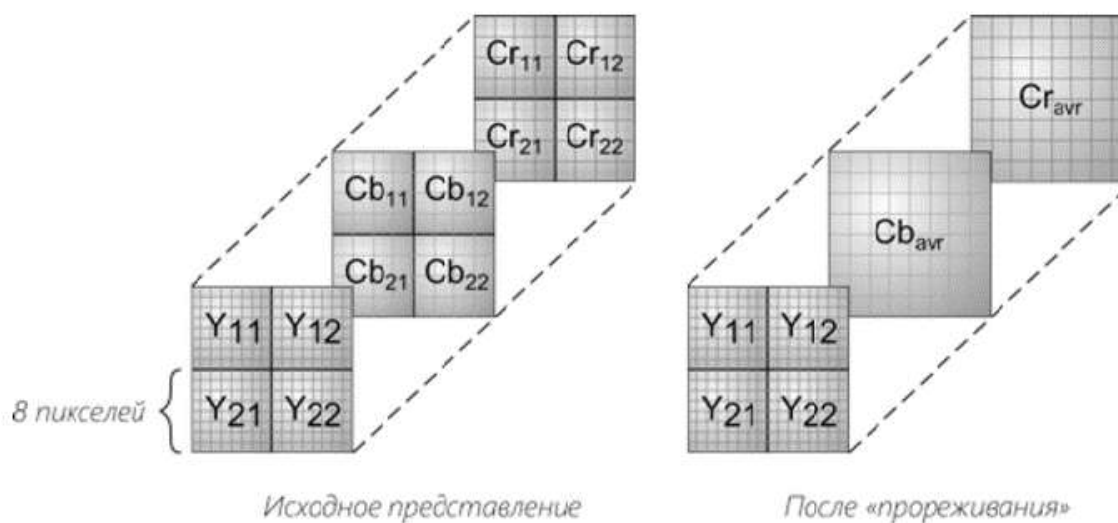


Рис. 2. Сильное изменение яркости пикселя с целью корректности считывания скрытой информации

Второй проблемой изменения только синей составляющей цвета является алгоритм сжатия JPEG (см. рис. 3). При преобразовании RGB \rightarrow YCbCr для каналов Cb и Cr, которые отвечают за цвет, может выполняться прореживание [5]. Например, каждому из 4 блоков яркостного канала Y ставятся в соответствие средние значения каналов Cb и Cr [6].

Рис. 3. Преобразование RGB \rightarrow YCbCr

2. Модификация метода Куттера-Джордана-Боссена на основе трёх составляющих цвета

Для того чтобы внедрённая информация была более устойчива к JPEG сжатию, а также сами изменения оставались менее заметными для восприятия, в данной работе предлагается использовать все три составляющие цвета, которые образуют Y:

$$Y_{x,y}^* = 0,299R_{x,y}^* + 0,587G_{x,y}^* + 0,114B_{x,y}^*.$$

Обратимся к первому требованию к стеганосистеме, описанному выше: изменения должны быть не заметны при визуальном контроле. Существует эмпирический закон Вебера-Фехнера, который позволяет определить степень заметности изменения яркости для человеческого глаза:

$$p = \ln \frac{Y + \varepsilon}{Y},$$

где p — контрастность, Y — яркость пикселя, ε — величина изменения яркости. В соответствии с законом Вебера-Фехнера, пороговая контрастность — это постоянная величина, которая равна 0,02–0,05 в зависимости от условий наблюдения. Пороговая контрастность при изменении яркости на $\varepsilon = 1$ и $\varepsilon = 2$ каждого канала пикселя в отдельности и яркости всего пикселя в целом показана на (см. рис. 4).

В модификации метода пиксель изменяется таким образом, чтобы его яркость отличалась от средней яркости его фона в пределах этого закона. От-



Рис. 4. Зависимость изменения видимости от приращения яркости

дельно стоит рассмотреть случай, когда пиксель сильно контрастирует со своим фоном, к примеру, в области контуров. То есть разница между яркостью изменённого пикселя и его фона превышает некоторое значение Δ :

$$|Y - Y_{cp}| > \Delta.$$

Модификация яркости такого пикселя приводит к сильной его заметности, следовательно, такие области необходимо пропускать. Второе требование к стеганосистеме — это устойчивость к искажениям. Алгоритм JPEG использует сжатие с потерями. Даже если оригинальное изображение без изменений сохранить алгоритмом JPEG, произойдёт потеря информации в виде незначительного изменения оттенка пикселей. Чтобы избежать потери скрытых битов, в модификации метода Куттера-Джордана-Боссена яркость изменённого пикселя должна отличаться от фона не менее чем на некоторую величину δ . Таким образом, яркость изменённого пикселя должна удовлетворять условию:

$$\begin{cases} |Y - Y_{cp}| > \Delta, \\ \left| k * \ln \frac{Y + \varepsilon}{Y_{cp}} \right| < p. \end{cases}$$

В связи с этим необходимо дополнить данные условия проверкой (см. рис. 5):

Если яркость изменённого пикселя $\Delta + \delta < |Y - Y_{cp}| < \Delta + 2\delta$, то данный пиксель лежит в пограничной области между контрастным и подходящим для встраивания, поэтому яркость данного пикселя необходимо изменить так, чтобы она удовлетворяла условию $|Y - Y_{cp}| > \Delta + 2\delta$ и данный пиксель однозначно

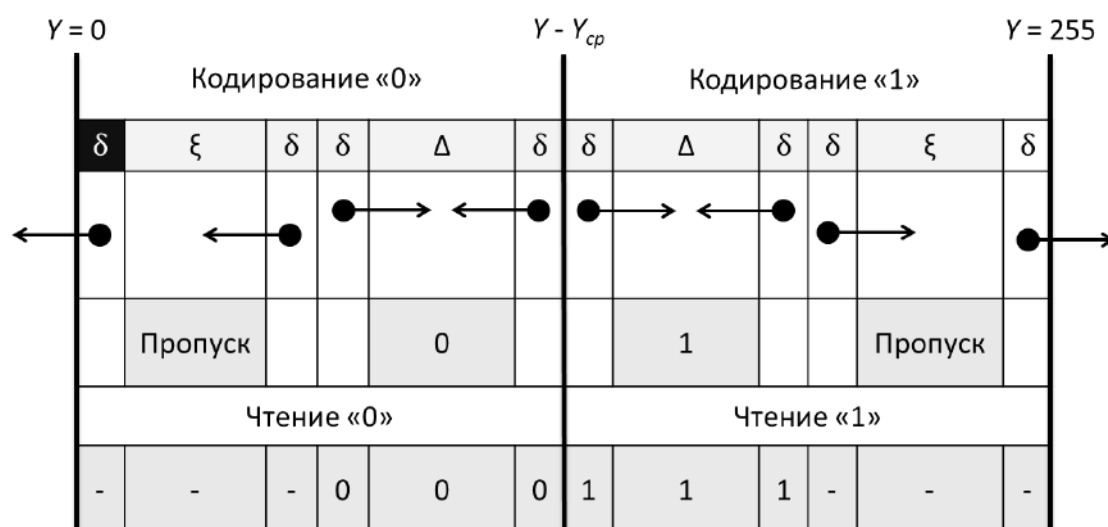


Рис. 5. Кодирование и чтение бита информации

трактовался как слишком контрастный.

При приближении яркости пикселя к границам чёрного ($Y = 0$) и белого ($Y = 255$) цвета значение яркости данного пикселя явно устанавливается как 0 или 255 соответственно. Это позволяет устранить возможные погрешности при работе алгоритма. Таким образом, значение разницы между яркостью пикселя и фона будет лежать либо в области Δ и означать успешную запись бита, либо в области ξ и означать, что данный пиксель не подходит для записи информации. При чтении область контрастных пикселей расширяется и задаётся как $|Y - Y_{cp}| > \Delta + 2\delta$, аналогично область информационных пикселей расширяется до $|Y - Y_{cp}| < \Delta + 2\delta$, что позволяет учитывать возможное изменение яркости при работе алгоритма сжатия JPEG.

Заключение

В отличие от оригинального метода, данная модификация позволяет достичь практически стопроцентной корректности считывания всех битов за счёт использования всех трёх составляющих его цвета, а также исключения из расчётов пикселей, имеющих большую разность яркости по сравнению с окрестностью. К тому же модификация позволяет расширить размер стеганоконтейнера за счёт уменьшения избыточности вносимой информации и увеличить стойкость к JPEG сжатию. Помимо этого модифицируемый алгоритм сохраняет преимущества оригинального метода Куттера-Джордана-Боссена, а именно повышенная устойчивость к различным видам атак, таким как удаление информации из наименее значимых битов, зашумление и кадрирование, а также сохраняет высокую устойчивость к частотному детектированию.

ЛИТЕРАТУРА

1. Васина Т.С. Обзор современных алгоритмов стеганографии // Наука и образование, 2012. № 4. URL: <http://technomag.bmstu.ru/doc/370605.html> (дата обращения: 20.09.2015).
2. Защелкин К.В. Усовершенствование метода скрытия данных Куттера-Джордана-Боссена // МНПК «Современные информационные и электронные технологии», 2013. С. 214–216.
3. Фомин Д.В. Модификация метода скрытия информации Куттера-Джордана-Боссена // Вестник Амурского государственного университета, 2014. Вып. 65 : Сер. Естеств. и экон. науки. С. 58–62.
4. Kutter M., Jordan F., Bossen F. Digital Signature of color image using amplitude modulation // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. P. 518–526.
5. Digital compression and coding of continuous-tone still images. Requirements and guidelines // ITU-T Recommendation T. 81, 1992. 28 p.
6. Douglas A. Kerr. Chrominance Subsampling in Digital Images. 2012. Issue 3. URL: <http://dougkerr.net/Pumpkin/articles/Subsampling.pdf> (дата обращения 10.10.2015).

**THE MODIFICATION OF THE KUTTER-JORDAN-BOSSSEN METHOD
OF THE LATENT INFORMATION STORAGE IN JPEG IMAGES****Alexander Dieser**Student, e-mail: ahemoh@gmail.com**Katherina Dieser**Postgraduate Student, e-mail: e.s.dizer@gmail.com**T.M. Oparina**Senior Tutor, e-mail: oparina2007@yandex.ru

Dostoevsky Omsk State University

Abstract. This article presents a modification of the Kutter-Jordan-Bossen method aimed at improving the sustainability of stego files to different types of attacks, an increased amount of hidden information in graphics file and the correct reading of the hidden information.

Keywords: steganography, stego file, Kutter-Jordan-Bossen method.