

# Стеганографическое преобразование цветного изображения в полутоновое для распределения цифровых фотографий

В.Н. Горбачев, И. К. Метёлев, Е.М. Кайнарова, Е.С. Яковлева

Северо-Западный институт печати

Санкт-Петербургского государственного университета технологии и дизайна, Санкт-Петербург, Россия.

{Елена Кайнарова} helenkainarova@gmail.com

## Аннотация

Для процесса преобразования цветного изображения в полутоновое и обратно рассмотрена стеганографическая система с секретным ключом. Для встраивания использованы битовые плоскости яркостной компоненты модели YUV и оригинальный алгоритм блочного кодирования, который позволяет скрывать информацию в старших битовых плоскостях. С помощью предложенной системы обсуждается задача о распределении цифровых изображений, когда пользователь может предварительно ознакомиться с интересующим его изображением. Представлен протокол, который позволяет исключить незаконное копирование цветного оригинала.

**Keywords:** *стеганография, преобразование цветного изображения в полутоновое*

## 1. ВВЕДЕНИЕ

Современная стеганография, которая занимается встраиванием цифровых данных одного объекта в цифровые данные другого, имеет широкое применение для защиты медианформации в частности для охраны авторского права. Однако, методы стеганографии позволяют решать ряд других задач, в число которых входит преобразование цветного изображения в полутоновое и обратно, известное как Color to Gray and Back Reversible Transformation (CGRT). Идея заключается в том, чтобы информацию о цвете исходного изображения с помощью стеганографии встроить в его полутоновую версию, а потом, например, после печати извлечь из черно-белого оттиска цвет и восстановить оригинал.

В литературе указывают следующие примеры применений такого преобразования.

Считают, что оно может быть полезным для офисов, где цветные документы появляются редко, поэтому для печати используется централизованный мощный черно-белый принтер [1]. Другим примером служит система резервного копирования Hardcopy Image Backup Copy для хранения аналоговых копий, сделанных с документов и цветных фотографий [2]. Известно, что при длительном хранении, 30-50 лет, происходит изменение цвета вплоть до полной его потери. Поэтому система создает копию со встроенной информацией, которая позволяет восстановить исходный цвет изображения.

Особенность CGRT можно пояснить следующим образом. Для заданного RGB изображения в качестве его полутоновой версии может служить яркостная компонента из модели YCbCr, что соответствует телевизионному стандарту NTSC (National Television Standards Committee). При этом для обычного представления цветной пиксел с энтропией 24 бита

заменяется на полутоновый с энтропией 8 бит. Энтропия не сохраняется, поэтому преобразование необратимо как с физической, так и математической точек зрения. Решение дает стеганография, ее методы позволяют встроить информацию о цвете в полутоновую версию, из которой потом восстанавливается цветное изображение. Строго говоря, такое преобразование также необратимо, однако оригинал и восстановленное изображение оказываются визуально неразличимы, поэтому говорят, что преобразование обратимо.

Для встраивания цвета в полутоновое изображение могут использоваться стандартные стеганографические методы, такие как дискретное вейвлет-преобразование [3]. Можно использовать особенности процесса печати, встраивая информацию через алгоритмы растривания [4] путем модулирования параметров оттиска.

Цель настоящей работы рассмотреть схему встраивания цвета с секретным ключом.

Ключ в соответствии с принципом Керхгоффса обеспечивает теоретическую секретность системы и вместе с тем позволяет передать изображение пользователю, которому оно предназначено.

В стеганографии роль ключа часто играет позиция пиксела, в которую встраивается информация, если пиксел выбирается случайно [5]. Вместо этого мы выбрали случайную матрицу. Она используется вместе с нашим алгоритмом блочного кодирования [6]. Этот алгоритм основан на условии сохранения яркости блока, в который встраивается бит сообщения, что увеличивает объем скрываемой информации.

Применение нашей схемы мы рассмотрели на примере распределения цифровых изображений из банка цветных фотографий. Задача заключается в том, чтобы пользователь предварительно ознакомился с интересующим его изображением перед тем как его приобрести. Задача является актуальной, поскольку сейчас спрос на высококачественные цифровые изображения, в частности на базы с экспертными оценками, растет. Предложенное решение основано на компромиссе, который достигается, если использовать идею  $\beta$ -версии. Вместо того чтобы предоставить пользователю полноценное цветное изображение, он получает полутоновую версию со встроенным цветом. Мы описали протокол, который с помощью распределения секретного ключа, позволяет законному пользователю восстановить из  $\beta$ -версии исходное цветное изображение.

Применение преобразования цветного изображения в полутоновое и обратно для этой задачи авторам неизвестно.

## 2. ПРЕОБРАЗОВАНИЕ ЦВЕТНОГО ИЗОБРАЖЕНИЯ В ПОЛУТОНОВОЕ

Задача Color to Gray and Back Reversible Transformation является интересным примером применения стеганографических методов для приложений. Мы кратко поясним ее на основе результатов [1], где использовано дискретное вейвлет-преобразование.

Исходное цветное изображение представлено в модели YCbCr, яркостная компонента которой Y играет роль контейнера для встраивания цвета, информация о котором представлена в хроматических компонентах Cb и Cr. Дискретное вейвлет-преобразование яркостной компоненты DWT(Y) состоит из четырех блоков коэффициентов, каждый из которых имеет размер равный четверти исходного изображения. Два блока заменяются на одну четверть коэффициентов из хроматических компонент Cb и Cr.

Получается новый вейвлет-образ яркостной компоненты Y', от которого вычисляется обратное вейвлет-преобразование IDWT(Y')=Yc. В результате получается полутоновая версия исходного цветного изображения, это Yc, в которую встроены цвет. Восстановление цветного изображения осуществляется в обратном порядке. Поскольку встроено только 1/4 всей информации о цвете, восстановленное изображение не равно исходному, однако они визуально неразличимы равно как и полутоновые компоненты Y и Yc.

Мы использовали стеганографическую систему с секретным ключом. В ней сообщение M встраивается в контейнер C с помощью секретного ключа K. Заполненный контейнер S называют стегоконтейнером.

Если E и D алгоритмы встраивания и детектирования, то стеганографическая система описывается соотношениями [7]

$$E: C \otimes M \otimes K \rightarrow S, \\ D: C \otimes S \otimes K \rightarrow M.$$

Два основных свойства стеганографической системы это неразличимость пустого и заполненного контейнера,  $C \approx S$  и секретность, которая обеспечивается ключом.

В нашей схеме цветное RGB изображение преобразовывается в модель YUV с яркостной компонентой Y и хроматическими компонентами X=U,V, из которых с помощью секретного ключа строились сообщения

$$M = (K + X) \bmod(255), \quad (1)$$

где K случайная матрица, размеры которой равны размеру исходного изображения. Далее M встраивается в яркостную компоненту Y, которая играет роль контейнера.

## 3. БЛОЧНОЕ ВСТРАИВАНИЕ С СОХРАНЕНИЕМ ЯРКОСТИ

Алгоритм блочного встраивания [6] использует битовые плоскости яркостной компоненты. Он работает следующим образом. Каждая битовая плоскость  $Y_V, V=1, \dots, 8$ , где младшая -  $Y_1$ , разделяется на непересекающиеся блоки  $Y_{V_a}$  размера  $h \times h$ . В каждом блоке определяется бит четности побочной диагонали

$$d_a = \bigoplus_{x \in Y_{V_a}} y[x, h - x]$$

Встраивание бита сообщения m в блок  $Y_{V_a}$  осуществляется по правилу

$$E: Y_{V_a} \rightarrow S_{V_a} = \begin{cases} Y_{V_a}, & \text{if } d_a \oplus m = 0, \\ ZY_{V_a}, & \text{if } d_a \oplus m = 1. \end{cases}$$

Здесь оператор Z осуществляет либо изменение бита в побочной диагонали, либо ищет блок  $S_{V_a}$  с яркостью равной или близкой к яркости  $Y_{V_a}$ . В результате яркость блока сохраняется максимальным образом.

Приведем пример работы оператора. Z для  $h=2$

$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \rightarrow Y_{V_a} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

$$S_{V_a} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Здесь сообщение представлено  $2 \times 2$  матрицей M. Каждый бит сообщения встраивается в один из четырех блоков  $Y_{V_a}$ . Стегоизображение  $S_{V_a}$  состоит из четырех блоков. Видно, что только один из блоков, правый верхний, изменил яркость (сумму элементов) на 1.

Алгоритм детектирования не использует исходного контейнера, такое детектирование называют слепым. Встроенное сообщение M извлекается из блока стегоизображения  $S_{V_a}$  с помощью вычисленного бита четности побочной диагонали. Его четность 0 или 1 равна значению бита сообщения. Затем, используя секретный ключ, находят хроматические компоненты  $X=U,V$

$$X = (M - K + 255) \bmod(255).$$

Условие сохранения яркости позволяет увеличить объем встраиваемой информации. Так, оказывается возможным использовать больше битовых плоскостей, начиная от младшей  $V=1$  вплоть до  $V=5,6$ , при этом сообщение не будет «просвечивать» [6]. Чем больше встроено информации о цвете в полутоновый контейнер, тем меньше будет отличаться от оригинала восстановленное изображение.

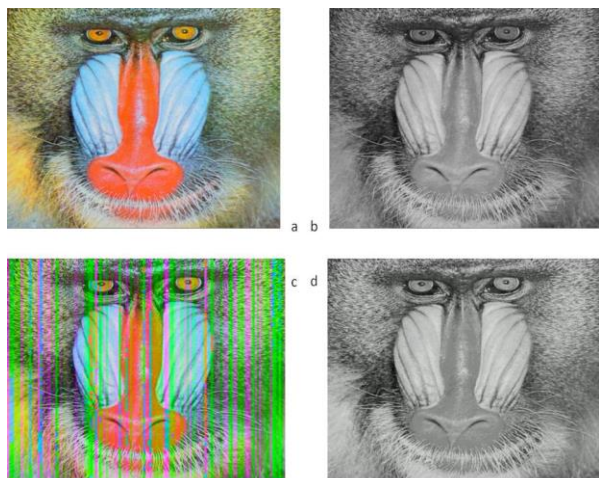
## 4. ЭКСПЕРИМЕНТ

Исходное RGB-изображение, рис.1-а, преобразовывалось в модель YUV. Компонента Y, в которую будет встраиваться цвет, приведена на рис.2-б. Число бит  $H_Y$ , которые можно зарезервировать в Y, определяется числом взятых битовых плоскостей T, числом пикселей n и величиной блока h, который используется алгоритмом встраивания:  $H_Y = nT/h^2$ . Ясно, что весь объем цветовой информации не встроить.

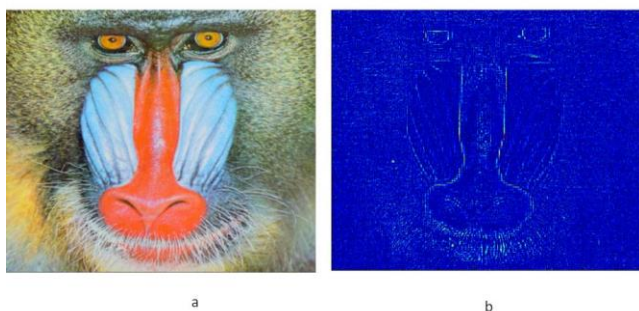
Поэтому разрешение хроматических компонент  $X=U,V$  уменьшалось путем усреднения по окрестности  $a \times a$ . В телевизионном стандарте передачи данных  $a=2$ , это называют 4:1:1. Мы использовали случай  $a=4$ . В результате объем цветовой информации  $H_C$  будет равен 1/8 от Y или  $H_C = (1/8)nk$ , где k битовая глубина канала Y,U и V. Обычное значение  $k=8$ . При  $h=2$  найдем, что  $H_Y = (T/4)H_C$ . Это означает, что при  $T=4$  мы встроим всю информацию о цвете  $H_C$ . Наш метод кодирования максимальным образом сохраняет яркость блоков. Поэтому при использовании не одной, а четырех битовых плоскости сокрытая в Y информация не «просвечивает». На рис.1-д показана яркостная компонента, в четыре битовых плоскости которой  $V=1,2,3,4$  встроены цвет.

Чтобы восстановить исходное цветное изображение нужен ключ. Если ключ неизвестен, то подобрать его практически

невозможно. Формально здесь возникает задача перебора  $2^{nk}$  полутоновых матриц, что с вычислительной точки зрения является сложной задачей класса NP. На рис.1-с приведен пример восстановленного изображения, когда некоторые биты в ключе специально изменены, «испорченный ключ». Однако, если взять исконный ключ, то восстановленное изображений, рис.2-а, визуально не отличить от исходного. Вместе с тем, различие есть. На рис.2-б приведена разность между синими компонентами.

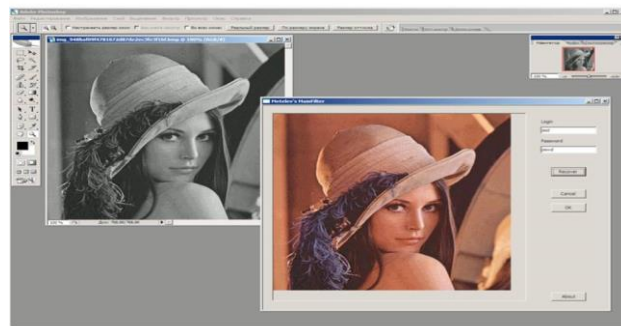


**Рис. 1:** Встраивание цвета в полутоновое изображение. а) исходное цветное изображение; б) яркостная компонента модели YUV, в которую встраивается цвет; в) восстановленное цветное изображение с неполноценным ключом; д) яркостная компонента со встроенным цветом.



**Рис. 2:** Восстановление цветного изображения из полутонового. а) восстановленное изображение; б) разность между синими каналами исходного и восстановленного изображения.

Работа рассмотренной схемы встраивания цвета реализована в полнофункциональной информационной системе, включающую в себя клиентскую часть, интегрированную в пакет *Adobe Photoshop*, рис.3, и серверную часть, сочетающую в себе веб-сервер и сервер приложений.



**Рис. 3:** Интерфейс в Adobe Photoshop.

## 5. ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ ЦВЕТНЫХ ИЗОБРАЖЕНИЙ

Приведенная схема встраивания цвета с секретным ключом дает решение задачи о распределении цветных изображений, которые собраны в фотобанке. Задачу можно сформулировать следующим образом. У Алисы есть цветное изображение *A*, которое она хочет продать. Боб желает приобрести его, но предварительно он хочет ознакомиться с ним, получив его в свое распоряжение. Однако Алиса ему не доверяет.

Решение основано на следующем компромиссе. В целях осторожности Алиса передает Бобу вместо цветного изображения *A* полутоновое *B*, в яркостной компоненте которого встроена информация о цвете. После того, как Боб сообщил о своем намерении приобрести интересующее его изображение, Алиса высылает ему секретный ключ и Боб извлекает из *B* цветное изображение.

Компромисс использует идею версии, он заключается в том, что Алиса сохраняет свои авторские права, будучи защищена секретным ключом, а Боб получает возможность детально ознакомиться, однако, с полутоновым изображением.

Разумеется, эту задачу можно решить иначе. Пусть у Алисы есть два отдельных изображения, цветное *A* и его полутоновая версия *B<sub>0</sub>*, которые оба должны быть отправлены через канал получателю.

Это простое решение, но в нем есть недостаток, который заключается в том, что злоумышленник сразу может получить цветное изображение *A* при атаке на канал. В первом случае эта возможность исключена, поскольку по каналу цветное изображение в явном виде не передается, а для передачи секретного ключа Алиса может использовать стандартные протоколы криптографии.

## 6. ВЫВОДЫ

Методы стеганографии позволяют решать задачи, которые не сводятся только к защите медиаинформации и охране авторского права. В области обработки изображений хорошо известны необратимые преобразования цветного изображения в полутоновое. Однако такое свойство как обратимость может быть рассмотрено с точки зрения зрительного восприятия, когда исходное цветное изображение и изображение, восстановленное из его полутоновой версии, оказываются неразличимы. Для этого случая в литературе используется специальный термин Color to Gray and Back Reversible Transformation.

Чтобы восстановить цветное изображение из полутонового, в последнем должна быть информация о цвете, которая встраивается и извлекается методами современной стеганографии.

В нашей работе рассмотрен вариант стеганографической системы с секретным ключом. Наш алгоритм блочного кодирования позволяет увеличить объем встраиваемой информации, путем использования старших битовых плоскостей вплоть до 4-5 включительно без заметного визуального искажения.

Схемы с Color to Gray and Back Reversible Transformation в литературе традиционно включают процесс печати, когда цветное изображение восстанавливается из полутонового оттиска. Однако, процесс печати очень сильно усложняет задачу извлечения встроеной информации.

Вместо этого мы рассмотрели применение для случая распределения цифровых изображений, которые собраны в фотобанке. Задача заключается в том, чтобы пользователь мог предварительно ознакомиться с интересующей его картинкой перед тем как ее купить. Предложенное решение построено на идее  $\beta$ -версии, когда пользователю вместо полноценного цветного изображения предоставляется его полутоновая версия. Полутоновая версия содержит информацию о цвете, который можно извлечь, однако, лишь при наличии секретного ключа. Мы привели протокол, который позволяет исключить незаконное копирование исходного цветного изображения.

## 7. REFERENCES

- [1] Braun K. and de Queiroz R.L. Color to Gray and Back: Color Embedding Into Textured Gray Images. Proc. IS&T/SID 13th Color Imaging Conference, pp.120-124, 2005.
- [2] Hoarau E., Tastl I., Moroney N.A. Hardcopy Backup and Reconstruction System for Digital Images. Proc.of 2009 ICIP, Cairo, Egypt Nov., 2009.
- [3] de Queiroz R. L., Braun K. M. Color to Gray and Black: Color Embedding Into Texture Gray Image. ISEE Translation on Image Processing, V. 15, No. 6, JUNE 2006, p. 1464-1470.  
Ko K.-W., Kwon O.-S., Son C.-H., Kwon E.-Y., and Ha Y.-H. Color Embedding and Recovery Based on Wavelet Packet Transform / Journal of Imaging Science and Technology. — 2008. — vol. 52.— pp. 010501-1–010501-10.
- [4] Oztan B., Sharma G. Multiplexed Clustered-dot halftone watermarks using bi-directional phase modulation and detection. Proceedings of 2010 IEEE 17th International Conference on Image Processing, Hong Kong, September 26-29, 2010.  
Ulichney R., Tastl I., Hoarau E. Analog Image Backup with Steganographic Halftones, Color Imaging XVI: Displaying, Processing, Hardcopy, and Applications, IS&T/SPIE Electronic Imaging Symposium, San Francisco Airport, CA, 7866-53, January 23-27, 2011.
- [5] Nohara F., Horiuchi T., Tominaga S. An Accurate Algorithm For Color to Gray and back / ICIP. — 2009. — pp. 485-488.
- [6] В.Н. Горбачев, Е.М. Кайнарова, И.К. Метелев. Один алгоритм блочного встраивания цифрового водяного знака в наименее значащие биты на основе условия равенства яркости. /Известия высших учебных

заведений. Проблемы полиграфии и издательского дела. М: МГУП, 2010, №2, с. 60 – 70.

Cox I.J., Miller M.L., Bloom J.F., Fridrich J., Kaler T. Digital Watermarking and Steganography', ELSEVIER, Morgan Kaufmann Publishers, 2008.

Fridrich J. Steganography in Digital Media. Principles, Algorithms, and Application, Cambridge University Press, New York, 2010.

## Авторы

Валерий Николаевич Горбачев, преподаватель Северо-Западного института печати СПб государственного университета технологии и дизайна (СЗИП СПб ГУТД).

Иван Кириллович Метелев, аспирант СЗИП СПб ГУТД, [ivan.metelev@yandex.ru](mailto:ivan.metelev@yandex.ru).

Елена Михайловна Кайнарова, преподаватель СЗИП СПб ГУТД, [helenkainarova@gmail.com](mailto:helenkainarova@gmail.com).

Елена Сергеевна Яковлева, преподаватель СЗИП СПб ГУТД, [2305lena@mail.ru](mailto:2305lena@mail.ru).