Виталий Г. Иваненко, Никита В. Ушаков
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

ЗАЩИТА ИЗОБРАЖЕНИЙ ФОРМАТА JPEG ПРИ ПОМОЩИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

DOI: http://dx.doi.org/10.26583/bit.2018.2.09

Аннотация. В связи с бурным развитием мультимедийных технологий встает вопрос защиты авторского права произведений в цифровом виде, особенно изображений. Преимущества упрощенной передачи фотографий по сети перечеркиваются их возможным воровством или неправомерным размещением на других сайтах. Следовательно, необходимо защищать информацию различными техническими средствами, одним из таких средств и являются цифровые водяные знаки. Рассматриваются существующие методы защиты изображений при помощи цифровых водяных знаков, отмечается их главные преимущества и недостатки. Проводится сравнительный анализ данных методов встраивания цифровых водяных знаков в изображения. По итогам анализа выбран наиболее эффективный метод – метод дифференциального встраивания энергии. Отмечается, что данный метод лучше всего использовать для обеспечения целостности и ЦВЗ и контейнера. Система встраивания ЦВЗ должна предотвращать попытки злоумышленников изменять ЦВЗ и исходные данные в контейнере. Приводятся требования к ЦВЗ, встраиваемому для защиты изображений. Описываются основные атаки на изображение в формате JPEG. Изучаются модификации алгоритмов сокрытия данных в JPEG. Проводится исследование алгоритма ДЭВ на устойчивость. Под показателем устойчивости понимается специальное значение, расчет которого приводится в работе. Изучаются недостатки алгоритма ДЭВ, а также приводятся способы их устранения. При исследовании изображение со встроенным в него ЦВЗ подвергалось таким атакам, как сжатие, фильтрация, масштабирование. Делается вывод, что метод ДЭВ применим для защиты авторского права на изображения, при помощи данного метода возможно легко выявить каналы утечки информации при передаче изображений.

Ключевые слова: цифровые водяные знаки, дифференциальное встраивание энергии, изображения, встраивание информации, модификация алгоритма.

Для цитирования. ИВАНЕНКО, Виталий Г.; УШАКОВ, Никита В.. ЗАЩИТА ИЗОБРАЖЕНИЙ ФОРМАТА JPEG ПРИ ПОМОЩИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ. Безопасность информационных технологий, [S.l.], n. 2, p. 106-113, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Дата доступа: 06 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.09.

Vitaliy G. Ivanenko, Nikita V. Ushakov
National Research Nuclear University “MEPhI”,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VGIvanenko@mephi.ru, http://orcid.org/0000-0003-0823-5501
e-mail: u.nick@inbox.ru, http://orcid.org/0000-0001-7347-239X

JPEG digital watermarking for copyright protection

DOI: http://dx.doi.org/10.26583/bit.2018.2.09

Abstract. With the rapid growth of the multimedia technology, copyright protection has become a very important issue, especially for images. The advantages of easy photo distribution are discarded by their possible theft and unauthorized usage on different websites. Therefore, there is

a need in securing information with technical methods, for example digital watermarks. This paper reviews digital watermark embedding methods for image copyright protection, advantages and disadvantages of digital watermark usage are produced. Different watermarking algorithms are analyzed. Based on analysis results most effective algorithm is chosen – differential energy watermarking. It is noticed that the method excels at providing image integrity. Digital watermark embedding system should prevent illegal access to the digital watermark and its container. Requirements for digital watermark are produced. Possible image attacks are reviewed. Modern modifications of embedding algorithms are studied. Robustness of the differential energy watermark is investigated. Robustness is a special value, which formulae is given further in the article. DEW method modification is proposed, it's advantages over original algorithm are described. Digital watermark serves as an additional layer of defense which is in most cases unknown to the violator. Scope of studied image attacks includes compression, filtration, scaling. In conclusion, it's possible to use DEW watermarking in copyright protection, violator can easily be detected if images with embedded information are exchanged.

Keywords: digital watermarks, differential energy watermarking, images, embedding information, algorithm modification.

For citation. IVANENKO, Vitaliy G.; USHAKOV, Nikita V.. JPEG digital watermarking for copyright protection. IT Security (Russia), [S.l.], n. 2, p. 106-113, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1117>. Date accessed: 06 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.09.

Введение

На сегодняшний день широко распространена передача изображений через интернет. В связи с легкостью копирования изображений число нарушений авторских прав на такие работы неумолимо растет путем их размещения на торрентах и других пиратских сайтах. Таким образом, проблема защиты авторских прав на изображения является актуальной. Одним из основных технических средств защиты информации при её передаче в сети интернет является встраивание в защищаемый объект невидимых меток – цифровых водяных знаков (ЦВЗ) [1].

Одним из наиболее популярных форматов сжатия изображений является JPEG (Joint Photographic Experts Group). Данный алгоритм работает с областями 8x8 пикселей, на которых происходит плавное изменение яркости и цвета. Поэтому, если разложить матрицу данной области при помощи дискретного косинусного преобразования, то только первые коэффициенты будут значимыми. Это значит, по алгоритму JPEG изображение сжимается за счет плавности изменения цветов. В алгоритме используется дискретное косинусное преобразование(ДКП) для разложения, а также преобразования матриц коэффициентов 8x8 пикселей, в результате получается новая матрица коэффициентов. Также, применяется обратное преобразования для возвращения к исходному изображению. ДКП необходимо для разложения изображения по амплитудам частот, после дискретного косинусного преобразования получается матрица, большинство коэффициентов которой (кроме первых) близки к нулю. Следовательно, можно использовать квантование коэффициентов для их аппроксимации, при этом практически не теряя качество изображения [2].

В работе рассматриваются и анализируются наиболее распространённые алгоритмы внедрения ЦВЗ в формат изображений JPEG.

1 Алгоритм Куттера-Джордана-Боссена

Алгоритм Куттера-Джордана-Боссена (далее Kutter) является одним из наиболее эффективных методов встраивания информации в изображения [1].

Этот алгоритм впервые опубликован в 1998 году, однако и сейчас проводятся исследования данного алгоритма. Например, в исследованиях [2] предлагается

модифицировать алгоритм вводом дополнительных правил для устранения проблем извлечения данных. В работе [3] предлагается уменьшение изменения, которые ЦВЗ вносит в контейнер, что повышает надежность метода защиты. Также, предлагается модификация алгоритма на основе трёх составляющих цвета для повышения устойчивости алгоритма к различным видам атак, а также увеличения объема скрываемой информации в работе [4].

Суть алгоритма заключается в изменения яркости синей компоненты цветовой гаммы. Сокрытие информации основывается на наименьшей чувствительности человеческого зрения к синему цвету. Встраивание происходит по следующему принципу. Пусть z_i- — встраиваемый бит; *K — {R, G, B, P}* — контейнер; *p(x, y)* — текущая позиция (текущий пиксель) в координатной сетке контейнера.

В соответствии со спецификацией алгоритма JPEG яркость определяется следующей формулой:

$$l(p) = 0.299r(p) + 0.587g(p) + 0.114b(p). \quad (1)$$

Внедрение ЦВЗ осуществляется по формуле

$$\tilde{b}(p) = \begin{cases} b(p) - ql(p), \text{если } z_i = 0 \\ b(p) + ql(p), \text{если } z_i = 1 \end{cases}, \quad (2)$$

где q — параметр, определяющий энергию встраиваемого сигнала. Его величина прямо пропорциональна устойчивости и обратно пропорциональна скрытности вложения. Под устойчивостью понимается сохранение исходного ЦВЗ после различных воздействий на контейнер.

Обнаружение ЦВЗ выполняется на основании предсказания значения текущего пикселя на основании значений его соседей в пределах “пиксельного креста” размером 7x7 пикселей [2].

Оценка получается по следующей формуле:

$$\tilde{b}'(p) = \frac{1}{4c}\left(-2b'(p) + \sum_{i=-c}^{+c} b'(x+i, y) + \sum_{j=-c}^{+c} b'(x, y+j)\right), \quad (3)$$

где c - число пикселей сверху (снизу, слева и справа) от текущего пикселя. Если секретный бит встраивается r раз, то его значение находиться по формуле

$$\delta = -\frac{1}{r}\sum_{i=1}^{r} \tilde{b}_i{}'(p) - b_i(p). \quad (4)$$

При этом, нельзя гарантировать верное определение значения секретного бита, поскольку функция верификации не является обратной к функции внедрения.

Данный алгоритм может также использоваться для защиты видеозаписей при их распространении [5].

2 Метод замены наименее значащего бита(LSB)

Алгоритм встраивания LSB является самым популярным из-за его простоты.

Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ — это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения [6].

Популярность данного метода обусловлена его простотой и тем, что он позволяет

скрывать в относительно небольших файлах значительные объемы информации. Метод зачастую работает с растровыми изображениями, представленными в формате без компрессии, например, GIF и BMP. Метод НЗБ имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей [7].

Основной его недостаток — высокая чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто дополнительно применяют помехоустойчивое кодирование [8].

Для повышения устойчивости метода, а также более эффективного скрытия информации возможно использование данного метода совместно с криптографией [9].

3 Алгоритм ДЭВ

В основе рассматриваемого ниже метода лежит дифференциальное встраивание энергии (ДЭВ), под энергией при этом понимаются значение коэффициентов ДКП рассматриваемой области изображения, формула её расчета приводится чуть ниже.

Описанный в данной работе метод ДЭВ встраивает цифровой водяной знак, состоящий из l бит b_j $(j = 0, 1, 2, \ldots, l-1)$ в изображение. Каждый бит цифрового водяного знака внедряется в определенную область изображения, которая состоит из n блоков коэффициентов дискретного косинусного преобразования размера 8*8 [10].

В выбранную область изображения осуществляется встраивание бита ЦВЗ за счет модификации разности энергий D между высокочастотными (ВЧ) коэффициентами дискретного косинусного преобразования верхней и нижней части области. Подмножество ВЧ коэффициентов обозначается S(c). Если встраивается 0, то ВЧ коэффициенты нижней части области приравниваются к нулю, если 1, то верхней. ЦВЗ встраивается лишь за счет удаления определенных коэффициентов.

Для вычисления энергии субобласти A используется следующая формула:

$$E_{\mathrm{A}}(c, n, Q) = \sum_{d=0}^{n/2} \sum_{i \in S(c)} ([\theta_{i,d}]_{\mathrm{Q}})^2, \tag{5}$$

где $\theta_{i,d}$ - коэффициент ДКП с индексом i из d-го блока коэффициентов ДКП субобласти A; $[]_{\mathrm{Q}}$ — означает, что энергия вычисляется у квантованных коэффициентов. Вычислении энергии субобласти B осуществляется таким же образом.

Подмножество S(c) определяется на основе выбранного порога

$$\boldsymbol{S(c) = \{h \in 1, 63\} | (h \geq c)\}.}$$

Порог c показывает количество коэффициентов ДКП, которые не будут использоваться при встраивании, его необходимо выбрать при встраивании [11].

4 Сравнительные характеристики алгоритмов

В зависимости от решаемой задачи, используются различные алгоритмы. Если необходима проверка целостности файла-изображения, целесообразно использовать алгоритм, внедряющий хрупкий ЦВЗ, если необходимо передать секретное сообщение в файле-контейнере нужны уже другие характеристики для ЦВЗ, если необходимо подтверждение авторских прав на изображение, необходим выбор алгоритма, осуществляющий внедрение робастного ЦВЗ, устойчивого к атакам на контейнер и т д [12].

Для непосредственного выбора после описания характеристик, приведенных в таблице 1, даётся краткое заключение по каждому из алгоритмов.

Таблица 1. Алгоритмы сокрытия данных в JPEG

Название метода	Принцип работы	Преимущества	Недостатки
Kutter	Изменение яркости синей компоненты цветовой гаммы.	Устойчивость к сжатию, обрезке, изменения контрастности и фильтрации	Только для изображений с глубиной цвета 24 бита
LSB	Замена последнего бита	Невидимость ЦВЗ, высокая регулируемая пропускная способность	Уязвимость ко всем видам атак на контейнер[13]
ДЭВ	Модификация энергетической разности между коэффициентами блоков пикселей	Сложность удаления ЦВЗ, устойчивость к большинству виду атак	Низкая скорость встраивания ЦВЗ

Технология определения устойчивости того или иного алгоритма или стеганосистемы состоим из четырех шагов [14]:

1. Скрываемая информация внедряется в контейнер
2. Контейнер подвергается внешнему воздействию или атаке
3. Скрытая информация извлекается из контейнера
4. Извлеченная информация сравнивается с оригинальной и определяется степень их соответствия

Таблица 2. Устойчивость алгоритмов внедрения ЦВЗ в JPEG

Алгоритм	Сжатие	Масштабирование	Поворот	Обрезка
Kutter	+	–	–	+
LSB	–	–	–	–
ДЭВ	+	–	+	+

Наиболее перспективным для изображений формата JPEG является метод ДЭВ, так как он устойчив ко многим видам воздействий на контейнер. Кроме того, ЦВЗ, встроенный данным методом, невидим для человеческого глаза. Поэтому алгоритм ДЭВ был модифицирован и изучен более подробно.

5 Исследование алгоритма ДЭВ

Основные проблемы алгоритма ДЭВ:

– Высокочастотные коэффициенты ДКП легко отбрасываются фильтрами, в связи с чем алгоритм ДЭВ, использующий для внедрения ЦВЗ высокочастотные коэффициенты будет уязвим к этому воздействию на контейнер

– Алгоритм ДЭВ не учитывает, какое влияние на исходное изображение оказывает отбрасывание коэффициентов ДКП

Для решения этих проблемы предлагаются следующие модификации:

1. Алгоритм учитывает только низкочастотные АС коэффициенты ДКП и внедряет цифровой водяной знак в соответствии с предложенными масками яркости и контраста.

2. Алгоритм модифицирует коэффициенты ДКП только в соответствии с заранее рассчитываемом значении JND [15], что исключает вероятность искажения изображения из-за слишком высокой разности энергий D.

Также, было проведено исследование на устойчивость модифицированного алгоритма в соответствии с шагами, приведенными ранее. Оценку устойчивости проводилась при помощи коэффициента ошибочных бит BER (Bit Error Rate). Формула вычисления данного коэффициента имеет следующий вид:

$$\boldsymbol{BER}(\boldsymbol{S},\boldsymbol{S'}) = \frac{\sum \boldsymbol{p_i}}{\boldsymbol{N}}, \quad (6)$$

$$\text{где } p_i = \begin{cases} 1, & \text{если } s_j \neq s_j^m \\ 0, & \text{если } s_j = s_j^m. \end{cases}$$

s_j – j-й бит оригинала встраиваемой строки, S_j^m – бит извлеченной строки, N-общее количество бит цифрового водяного знака.

Если коэффициент BER=0, то внедряемая и извлеченная информация полностью идентичны. При BER=1 каждый бит извлеченного не соответствует оригинальному. Таким образом, при BER>0.5 ЦВЗ можно считать извлеченным полностью некорректно. Ошибки по большей части возникают на темных изображениях, где AC-коэффициентов (все коэффициенты, кроме первых, которые называются DC-коэффициентами) очень мало, или они вообще отсутствуют. Таким образом, на черном экране процент ошибок будет равен 50%, так как он высчитывается без исходной информации.

Таблица 3. Свойства изображений

	Разрешение (пиксели)
Изображение 1	1920*1200
Изображение 2	810*1080

Начнем с сжатия JPEG с потерями. Для проверки устойчивости к сжатию JPEG изображение-контейнер подвергалось сжатию JPEG во всем диапазоне значения коэффициента качества JPEG. Как можно увидеть из таблицы, оригинальный алгоритм не обладает достаточной устойчивостью к такого рода внешним воздействиям.

Таблица 4. Устойчивость к сжатию

Коэффициент качества JPEG(%)	100	90	80	70	60	50	40	30	20
Изображение 1(BER)	0.03	0.06	0.0.8	0.13	0.29	0.34	0.41	0.47	0.49
Изображение 2(BER)	0.04	0.07	0.0.7	0.15	0.31	0.37	0.39	0.40	0.47

Фильтрация является одним из наиболее вероятных внешних воздействий на контейнер с внедренным ЦВЗ, для исследования были выбраны 4 вида фильтров: низкочастотный фильтр, высокочастотный фильтр, усредняющий фильтр и контрастные фильтры, с размеров окна 3x3. Результаты приведены в таблице 4.

Таблица 5. Устойчивость к фильтрации

Фильтры	Низкочастотный	Высокочастотный	Усредняющий	Контрастный
Изображение 1(BER)	0.05	0.48	0.20	0
Изображение 2(BER)	0.04	0.46	0.22	0

В ходе эксперимента изображение восстанавливалось в оригинальный размер после масштабирования и потом производилось извлечение, результаты приведены в таблице 6.

Таблица 6. Устойчивость к масштабированию

Масштабирование(% от исходного изображения)	95	90	85	80
Изображение 1(BER)	0.34	0.41	0.47	0.49
Изображение 2(BER)	0.37	0.39	0.40	0.47

Из таблицы видно, что данный метод особенно уязвим к масштабированию даже после модификаций.

Заключение

На основании изложенного можно заключить, что метод ДЭВ применим для защиты авторского права на изображения, он обладает значительными преимуществами по сравнению с алгоритмами LSB и Куттера. Алгоритм LSB, не смотря на современные модификации обладает чрезвычайно низкой устойчивостью к атакам на контейнер, в связи с чем ЦВЗ, встроенный этим методом будет легко удален при передаче изображения по сети. при помощи данного метода возможно легко вычислить канал утечки информации. Проблемой же алгоритма Куттера является функция извлечения ЦВЗ – она не обратна функции встраивания, в связи с чем возникает проблема точного восстановления встроенного цифрового водяного знака. Алгоритм ДЭВ не обладает подобными недостатками, следовательно, он лучше обеспечивает защиту авторского права на изображения.

СПИСОК ЛИТЕРАТУРЫ:

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография: Стратегия развития информационного общества в РФ. М.: Солон-Пресс, 2009. - 265 с. - ISBN: 5-98003-011-5. С. 215–220.
2. А.Е. Дизер, Е.С. Дизер, Т.М. Опарина Модификация метода Куттера-Джордана-Боссена скрытого хранения информации в изображениях формата JPEG. Математические структуры и моделирование 2016. №3(39). С. 177-183.
3. Фомин Д.В. Модификация метода скрытия информации Куттера-Джордана-Боссена. Вестник Амурского государственного университета, 2014. Выпуск 65, Серия: естественные и экономические науки. С. 58-62.
4. Защелкин К.В. Усовершенствование метода скрытия данных Куттера-Джордана-Боссена. МНПК «Современные информационные и электронные технологи». 2013. с. 214-216.
5. Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganograhpic algorithm in video sequences. Young Researchers in Electrical and Electronic Engineering (ElConRus), 2017 IEEE Conference of Russian.
6. Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding. Proc. SPIE. — 1995. — Vol. 2420. — P.40.
7. Евсютин О.О. Модификация стеганографического метода LSB, основанная на использовании блочных клеточных автоматов. Информатика и системы управления, 2014, №1(39), с.15-22.
8. Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, №4, 2016, p.126-132.
9. Joshi K. Yadav R. A new LSB-S image steganography method blend with cryptography for secret communication. Third International Conference on Image Information Processing (ICIIP), 2015, p. 86-90.
10. Иваненко В.Г., Ушаков Н.В. Встраивание цифровых водяных знаков в видеозаписи. Безопасность информационных технологий — 2016. — №4. — с.21-24.
11. Ivanenko V. Ushakov N. Copyright protection for video content based on digital watermarking. BICA 2017: Biologically Inspired Cognitive Architectures (BICA) for Young Scientists p. 329-334.
12. Иваненко В.Г., Ушаков Н.В. Цифровые знаки в электронном документообороте. Безопасность информационных технологий — 2017. — №3. — с.37-42.
13. S.Tabasu Kannan, S.Azhagu Senthil A Frame work for various watermarking algorithms. Asian Journal of Computer Science and Technology ISSN 2249-0701 Vol.4, №1, 2015, p.21-28.

14. Abdullah Bamatraf, Rosziati Ibrahim, Mohd.Najib B. Mohd Salleh Digital watermaking algorithm using LSB. International Conference on Computer Application and Industrial Electronics (ICCAIE 2010), 2010, p.155-159.
15. Yaqing Niu, Matthew Kyan, Lin Ma, Azzedine Beghdadi, Sridhar Krishnan Visual salience's modulatory effect on just noticeable distortion profile and it's application in image watermarking. Signal Processing: Image Communication 28 (2013), p.917-928.

REFERENCES:

[1] Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography: Salon-Press Information society development strategy in Russia, 2009. (in Russian).
[2] A.E. Dizer, E.S. Dizer, T.M. Oparina Modification of The cutter-Jordan-Bossen method of hidden information storage in JPEG images. Mathematical structures and modeling 2016. №3(39). p. 177-183. (in Russian).
[3] Fomin D.V. Modification of method of concealment of information of Kutter-Jordan-Bossen. Bulletin of the Amur state University, 2014. Issue 65, Series: natural and economic Sciences. P. 58-62. (in Russian).
[4] Zashelkin K.V. Improved method of hiding data Cutter-Jordan-Bossen. International scientific-practical conference "Modern information and electronic technology». 2013. p. 214-216. (in Russian).
[5] Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganograhpic algorithm in video sequences. Young Researchers in Electrical and Electronic Engineering (ElConRus), 2017 IEEE Conference of Russian.
[6] Bender W., Gruhl D., Morimoto N. Techniques for Data Hiding [Текст]. Proc. SPIE. — 1995. — Vol. 2420. — P.40.
[7] Evsyutin O.O. Modification of the steganographic method LSB, based on the use of block cellular automata. Informatics and control systems, 2014, №1(39), p.15-22 (in Russian).
[8] Tavoli R. Bakhsi Maryam Salehian F. A new method for text hiding in the image by using LSB. (IJACSA) Internation Journal of Advanced Computer Sceince and Apllications, vol.7, №4, 2016, p.126-132.
[9] Joshi K. Yadav R. A new LSB-S image steganography method blend with cryptography for secret communication. Third International Conference on Image Information Processing (ICIIP), 2015, p. 86-90.
[10] Ivanenko V.G., Ushakov N.V. Embedding digital watermarks in video recording. Information technology security, 2016, №4, p. 21-24 (in Russian).
[11] Ivanenko V. Ushakov N. Copyright protection for video content based on digital watermarking. BICA 2017: Biologically Inspired Cognitive Architectures (BICA) for Young Scientists p. 329-334.
[12] Ivanenko V.G., Ushakov N.V. Digital watermarks in electronic document circulation. Bezopasnost' informacionnyh tekhnologij, 2017, №3, p. 37-42 (in Russian).
[13] S.Tabasu Kannan, S.Azhagu Senthil A Frame work for various watermarking algorithms. Asian Journal of Computer Science and Technology ISSN 2249-0701 Vol.4, №1, 2015, p.21-28.
[14] Abdullah Bamatraf, Rosziati Ibrahim, Mohd.Najib B. Mohd Salleh Digital watermaking algorithm using LSB. International Conference on Computer Application and Industrial Electronics (ICCAIE 2010), 2010, p.155-159.
[15] Yaqing Niu, Matthew Kyan, Lin Ma, Azzedine Beghdadi, Sridhar Krishnan Visual salience's modulatory effect on just noticeable distortion profile and it's application in image watermarking. Signal Processing: Image Communication 28 (2013), p.917-928.

Поступила в редакцию – 21 февраля 2018 г. Окончательный вариант –03 мая 2018 г.
Received – February 21, 2018. The final version – May 03, 2018.