



УДК 004.056

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ПРИ JPEG-СЖАТИИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ВСТРАИВАЕМЫХ В НЕПОДВИЖНЫЕ ИЗОБРАЖЕНИЯ

В.А. Батура^а^а Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

Адрес для переписки: Batu-vladimir@yandex.ru

Информация о статье

Поступила в редакцию 06.05.15, принята к печати 25.05.15

doi:10.17586/2226-1494-2015-15-4-708-715

Язык статьи – русский

Ссылка для цитирования: Батура В.А. Повышение устойчивости при JPEG-сжатии цифровых водяных знаков, встраиваемых в неподвижные изображения // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 4. С. 708–715.

Аннотация

Предмет исследования. Разработка и исследование способа повышения устойчивости при JPEG-сжатии цифровых водяных знаков, встраиваемых в неподвижные изображения. **Метод.** Представлен новый алгоритм цифрового маркирования неподвижных изображений, встраивающий цифровой водяной знак в неподвижное изображение при помощи модификации частотных коэффициентов дискретного преобразования Адамара. Выбор частотных коэффициентов для встраивания цифрового водяного знака основан на наличии резкого изменения их значений после модификации при максимальном сжатии JPEG. Выбор блоков пикселей для встраивания основан на показателе их энтропии. Новый алгоритм был подвергнут анализу устойчивости к компрессии изображения, зашумлению, фильтрации, изменению размера, цвета и эквализации гистограммы. Для сравнительного анализа был выбран алгоритм Elham, обладающий хорошей устойчивостью к JPEG-компрессии. В качестве объектов защиты было выбрано 9 полутоновых изображений. Незаметность вносимых в них искажений определялась на основе величины пикового отношения сигнала к шуму, величина которой должна быть не ниже 43 дБ для незаметности вносимых искажений. Стойкость встроенного водяного знака определялась коэффициентом корреляции Пирсона, величина которого для минимально допустимой устойчивости должно быть не ниже 0,5. Алгоритм вычислительного эксперимента: внедрение при помощи нового алгоритма и алгоритма Elham в каждое тестовое изображение водяного знака; внесение искажений в объект защиты; извлечение встроенной информации с ее последующим сравнением с оригиналом. Параметры алгоритмов были выбраны таким образом, чтобы обеспечить приблизительно одинаковый уровень вносимых в изображение искажений. **Основные результаты.** Представленный в статье метод предварительной обработки водяного знака способен существенно сократить объем информации, внедряемой в неподвижное изображение. В результате вычислительного эксперимента было установлено, что представленный алгоритм обладает повышенной устойчивостью к JPEG-сжатию, зашумлению, фильтрации Винера и изменению яркости. **Практическая значимость.** Представленный алгоритм может быть использован для защиты авторских прав на неподвижные изображения.

Ключевые слова

преобразование Адамара, цифровое маркирование, сжатие JPEG, цифровой водяной знак, стеганография.

Благодарности

Выражаю благодарность д.т.н., профессору кафедры вычислительной техники Университета ИТМО А.Ю. Тропченко за полезные рекомендации при проведении исследования.

INCREASE OF STABILITY AT JPEG COMPRESSION OF THE DIGITAL WATERMARKS EMBEDDED IN STILL IMAGES

V.A. Batura^а^а ITMO University, Saint Petersburg, 197101, Russian Federation

Corresponding author: Batu-vladimir@yandex.ru

Article info

Received 06.05.15, accepted 25.05.15

doi:10.17586/2226-1494-2015-15-4-708-715

Article in Russian

For citation: Batura V.A. Increase of stability at jpeg compression of the digital watermarks embedded in still images. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2015, vol.15, no. 4, pp. 708-715.**Abstract****Subject of Research.** The paper deals with creation and research of method for increasing stability at JPEG compressing of digital watermarks embedded in still images. **Method.** A new algorithm of digital watermarking for still images which

embeds digital watermark into a still image via modification of frequency coefficients for Hadamard discrete transformation is presented. The choice of frequency coefficients for embedding of a digital watermark is based on existence of sharp change of their values after modification at the maximum compression of JPEG. The choice of blocks of pixels for embedding is based on the value of their entropy. The new algorithm was subjected to the analysis of resistance to an image compression, noising, filtration, change of size, color and histogram equalization. Elham algorithm possessing a good resistance to JPEG compression was chosen for comparative analysis. Nine gray-scale images were selected as objects for protection. Obscurity of the distortions embedded in them was defined on the basis of the peak value of a signal to noise ratio which should be not lower than 43 dB for obscurity of the brought distortions. Resistibility of embedded watermark was determined by the Pearson correlation coefficient, which value should not be below 0.5 for the minimum allowed stability. The algorithm of computing experiment comprises: watermark embedding into each test image by the new algorithm and Elham algorithm; introducing distortions to the object of protection; extracting of embedded information with its subsequent comparison with the original. Parameters of the algorithms were chosen so as to provide approximately the same level of distortions introduced into the images. **Main Results.** The method of preliminary processing of digital watermark presented in the paper makes it possible to reduce significantly the volume of information embedded in the still image. The results of numerical experiment have shown that the proposed algorithm keeps higher resistance to JPEG compression, noising, Wiener filtering and brightness change. **Practical Relevance.** The proposed algorithm is applicable for copyright protection on the still images.

Keywords

Hadamard transformation, digital watermarking, JPEG compression, digital watermark, steganography.

Acknowledgements

The author expresses gratitude to A.Yu. Tropchenko, D.Sc., Professor of Chair of Computation Technologies, ITMO University, for useful recommendations when carrying out research.

Введение

Один из эффективных способов защиты авторских прав на неподвижные изображения – цифровое маркирование, которое является направлением стеганографии. Цифровое маркирование осуществляет внедрение цифрового водяного знака (ЦВЗ) в объект защиты (неподвижное изображение, видео-, аудио-информация и другая мультимедийная информация). ЦВЗ представляет собою невидимую человеческим глазом цифровую метку [1].

Существует большое количество вредоносных воздействий, связанных с обработкой неподвижного изображения и направленных на уничтожение встроенного ЦВЗ. Наиболее распространенной атакой является сжатие с потерями, способное уничтожить ЦВЗ без заметного искажения изображения. Сжатие с потерями реализуют, например, форматы JPEG и JPEG2000. Формат JPEG, широко распространенный в сети Интернет, обладает высокой эффективностью, следовательно, задача защиты ЦВЗ от компрессии JPEG является актуальной. Формат сжатия JPEG2000 обеспечивает более эффективное сжатие изображение, чем JPEG, однако на сегодняшний день он практически не используется в сети Интернет и большинством программного обеспечения для чтения графических файлов не поддерживается.

Среди алгоритмов цифрового маркирования наилучшую эффективность в противодействии атакам обработки изображения проявляют частотные алгоритмы цифрового маркирования. Такие алгоритмы осуществляют внедрение ЦВЗ в частотные коэффициенты дискретного косинусного преобразования (ДКП) [2, 3] и дискретного вейвлет-преобразования [4–6]. В последние годы в частотных алгоритмах цифрового маркирования применяется дискретное преобразование Адамара (ДПА) [7–14], которое для дополнительного уменьшения вычислительной сложности определяется строчно-столбцовым образом:

$$F_N = \frac{1}{N} A_N [X_N A_N], \quad (1)$$

где N – порядок матрицы Адамара; A_N – ядро преобразования Адамара, строки которого представлены последовательностью 1 и -1 ; X_N – матрица пикселей изображения; F_N – матрица частотных коэффициентов.

Матрица ядра ДПА обладает свойством симметричности, т.е.

$$A_N = A_N^T.$$

Чем больше количество перемен знака в строке ядра ДПА, тем больше частотность коэффициента. Ядро ДПА порядка $N = 2^n$, где n – целое положительное число, формируется при помощи операции кронекеровского умножения матриц:

$$A_{2N} = A_2 \otimes A_N = \begin{bmatrix} A_N & A_N \\ A_N & -A_N \end{bmatrix},$$

где $A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ представляет собой матрицу Адамара наименьшего порядка.

Использование данного преобразования обеспечивает схожую с ДКП устойчивость ЦВЗ к вредоносным воздействиям, в некоторых случаях даже превышая ее [15]. Кроме того, ДПА позволяет сильно уменьшить вычислительную сложность частотных алгоритмов цифрового маркирования и упростить их

аппаратную реализацию. Среди алгоритмов цифрового маркирования, основанных на ДПА [7–14], хорошей устойчивостью к JPEG-компрессии обладает алгоритм Elham [14], однако он не обеспечивает сильную устойчивость встраиваемой информации при сжатии JPEG высокого уровня. Целью работы являлась разработка алгоритма цифрового маркирования, обеспечивающего высокую устойчивость ЦВЗ к компрессии JPEG.

Новый алгоритм цифрового маркирования

Новый алгоритм цифрового маркирования встраивает монохромный черно-белый водяной знак в коэффициенты ДПА полутонового изображения. Алгоритм состоит из нескольких этапов, каждый из которых представлен ниже. Предварительно рассмотрим правило выбора частотных коэффициентов ДПА для встраивания битов ЦВЗ.

Правило выбора частотных коэффициентов. При изменении некоторых частотных составляющих ДПА их значение при коэффициенте качества сжатия JPEG $Q = 0$ резко отклоняется от значения при том же коэффициенте качества без предварительной модификации (рис. 1).

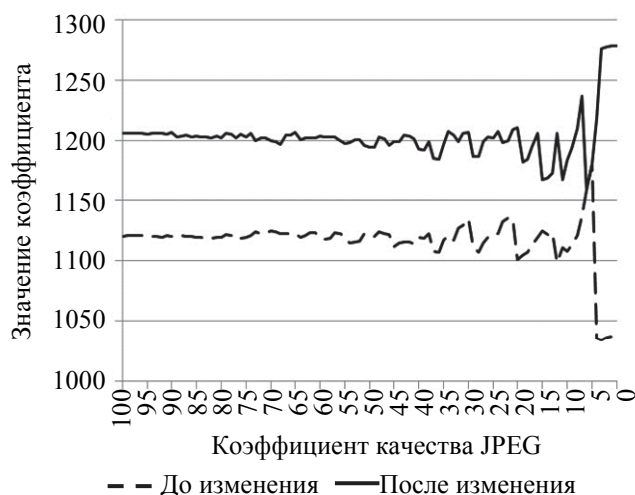


Рис. 1. Изменение коэффициентов дискретного преобразования Адамара до и после модификации в процессе компрессии JPEG

Такие изменения коэффициентов связаны с особенностями JPEG-сжатия. В процессе сжатия JPEG основная потеря информации происходит на стадии квантования, при которой частотные составляющие ДКП изменяются по формуле

$$c' = \text{round}(c / q) \times q,$$

где round — оператор округления, c — частотная составляющая ДКП до квантования, а c' — после квантования, q — значение элемента таблицы квантования.

При $Q = 0$ все элементы наиболее распространенной таблицы равны 255. Если остаток от деления $c/255$ больше или равен 0,5, то наблюдается резкое изменение конечного состояния частотной составляющей ДКП. При этом наиболее близкий к ней по частоте коэффициент ДПА также изменит свое конечное состояние (рис. 1).

Предсказать величину коэффициента ДКП, зная значение ДПА, не представляется возможным. Исходя из этого, для выбора коэффициента ДПА необходима проверка значения коэффициента ДКП при $Q = 0$. ДКП определяется по следующей формуле:

$$D(u, v) = \frac{c(u, v)}{4} \times \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \times \cos\left(\frac{2x+1}{16} \times u \times \pi\right) \times \cos\left(\frac{2y+1}{16} \times v \times \pi\right),$$

где $c(u, v)$ — нормирующий множитель, равный $1/\sqrt{2}$ при $u=0$ или $v=0$ и единице для остальных значений индексов.

Использование подобных коэффициентов ДПА (рис. 1) позволит сильно повысить устойчивость ЦВЗ к JPEG-сжатию. Встраивание ЦВЗ предпочтительно осуществлять в низкочастотные коэффициенты ДПА, изменение которых вызывает менее заметные искажения. Выбранные для данного алгоритма коэффициенты ДПА имеют следующие координаты (y, x) в блоках размером 8×8 по мере увеличения частотности: 1,5; 5,1; 1,7; 5,5; 7,1; 3,1; 7,5; 5,7; 1,3; 1,4; 5,3; 7,7; 3,5; 4,1. Им соответствуют коэффициенты ДКП с координатами (y, x) : 1,2; 2,1; 3,1; 2,2; 1,3; 1,4; 2,3; 3,2; 4,1; 5,1; 4,2; 3,3; 2,4; 1,5.

Сокращение числа бит встраиваемой информации. Сокращение числа бит встраиваемой информации — первый этап работы нового алгоритма, представлен на рис. 2.

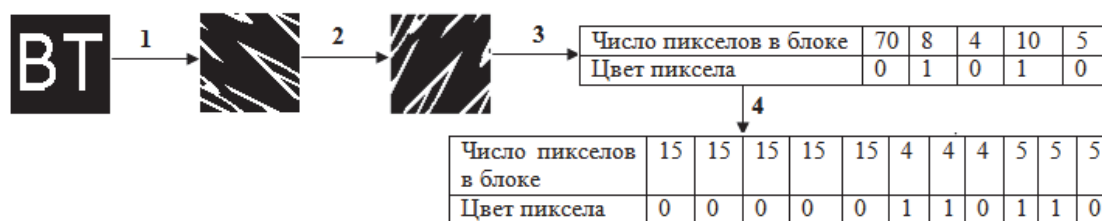


Рис. 2. Сокращение встраиваемой информации цифрового водяного знака

Процесс сокращения встраиваемой информации состоит из следующих этапов.

1. По представленной ниже формуле ЦВЗ подвергается однократному преобразованию Арнольда, представляющую собой обратимую хаотическую карту:

$$\begin{bmatrix} y' \\ x' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} y \\ x \end{bmatrix} \pmod N,$$

где N – сторона квадратного ЦВЗ; (y, x) – исходные координаты пиксела ЦВЗ; (y', x') – координаты пиксела ЦВЗ после преобразования.

2. Полученное на первом этапе изображение поворачивается на 90° вправо и подвергается зигзаг-сканированию, начиная с верхнего левого угла. За счет использования на первом этапе преобразования Арнольда образуются последовательности с большим количеством подряд идущих 0 или 1.
3. Формируется промежуточная таблица дескрипторов, содержащая число пикселей каждого блока и маркер (бит), обозначающий цвет каждого блока.
4. Выполняется дополнительная декомпозиция вектора битов (цветов пикселей), которая осуществляется по формулам, представленным в табл. 1.

L/n	$n \geq 0,39 \times x$	$0,16 \times x \leq n \leq 0,39 \times x$	$n < 0,16 \times x$
L_0	$round(0,39 \times x)$	$ceil(count/4) - 1$	n
L_1		$round(0,125 \times x)$	

Таблица 1. Формулы дополнительной декомпозиции ЦВЗ

где x – ширина ЦВЗ; n – число бит в векторе бит; L_0 – длина блока декомпозиции вектора «0» бит; L_1 – длина блока декомпозиции вектора «1» бит; $ceil$ – округление в большую сторону; $round$ – округление в меньшую сторону.

В результате встраиванию подлежит строка маркеров, указывающих цвет блока пикселей. У пользователя в качестве одного из элементов ключа остается только структура ЦВЗ (количество блоков каждого цвета).

Внедрение цифрового водяного знака

Встраивание вектора-строки маркеров ЦВЗ осуществляется в два этапа.

Встраивание «1». Для каждой «1» в строке маркеров, полученных на этапе предварительной обработки ЦВЗ, процесс встраивания осуществляется по следующему алгоритму.

1. Разбиение контейнера на неперекрывающиеся блоки размером 8×8 ;
2. Поиск блоков 8×8 , энтропия (E) которых больше заданного первого порога E_1 . Энтропия определяется по формуле [7]

$$E = \sum_{i=1}^n p_i \exp(1 - p_i),$$

где p_i – вероятность возникновения соответствующего уровня яркости i в блоке изображения. Вероятность p находится в интервале $[0; 1]$. Сумма вероятностей всех типов яркостей блока равна 1. Определить вероятность p появления уровня яркости i можно, основываясь на значении гистограммы частот появления пикселей с соответствующей яркостью i [16].

3. Получение частотных коэффициентов ДПА выбранного блока пикселей по формуле (1).
4. Поиск в полученной матрице частотного коэффициента по представленному ранее правилу поиска.
5. Встраивание «1» в выбранный коэффициент ДПА по формуле

$$c'_i = c_i + sign \times \alpha,$$

где $sign$ – знак сложения или вычитания коэффициента усиления α с частотным коэффициентом c_i ; c'_i – модифицированный коэффициент ДПА.

6. Сохранение в ключевой матрице M местоположения блоков и модифицируемых коэффициентов.

Встраивание «0» считается условным – этапы внедрения идентичны алгоритму для «1», но само встраивание не осуществляется. При поиске пригодных для встраивания блоков используется порог энтропии E_0 , а не E_1 .

В результате внедрения формируется ключевая матрица M , содержащая дескрипторы i , где $i = 1, 2, 3, \dots$. Дескрипторы в таблице расположены в порядке следования цветковых маркеров, полученных в результате предварительной обработки ЦВЗ. Каждый дескриптор имеет следующие характеристики: $M(1,i)$ и $M(2,i)$ – координаты (y, x) верхнего левого пиксела блока изображения размером 8×8 ; $M(3,i)$ и $M(4,i)$ – координаты (y_c, x_c) частотного коэффициента ДПА; $M(5,i)$ – знак внедрения $sign$; $M(6,i)$ – количество пикселей внедряемого цвета.

Извлечение цифрового водяного знака

Извлечение ЦВЗ осуществляется с использованием исходного изображения и ключевой матрицы M . Биты ЦВЗ извлекаются по следующим формулам:

$$\begin{aligned} &\text{если } M(5, i) = -1 \\ &w_i = \begin{cases} 1, &\text{если } c'_i < (c_i[M(3,i), M(4,i)] - 50), \\ 0, &\text{если } c'_i \geq (c_i[M(3,i), M(4,i)] - 50), \end{cases} \\ &\text{если } M(5, i) = 1 \\ &w_i = \begin{cases} 1, &\text{если } c'_i > (c_i[M(3,i), M(4,i)] + 50), \\ 0, &\text{если } c'_i \leq (c_i[M(3,i), M(4,i)] + 50), \end{cases} \end{aligned}$$

где w_i – извлеченный бит ЦВЗ; c_i – исходный частотный коэффициент ДПА; c'_i – модифицированный коэффициент ДПА. Характеристики дескрипторов представлены ранее.

На основе извлеченной строки бит и количества пикселей для каждого бита формируется строка пикселей ЦВЗ. Из строки пикселей при помощи зигзаг-алгоритма формируется изображение, которое подвергается повороту на 90° влево. Затем осуществляется обратное преобразование Арнольда:

$$\begin{bmatrix} y \\ x \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \times \begin{bmatrix} y' \\ x' \end{bmatrix} \bmod N,$$

где N – сторона квадратного ЦВЗ; (y, x) – исходные координаты пиксела ЦВЗ; (y', x') – координаты пиксела извлеченного ЦВЗ.

Анализ предложенного алгоритма

Разработанный алгоритм был подвергнут проверке на незаметность вносимых искажений, а также устойчивость встраиваемого ЦВЗ к наиболее распространенным вредоносным воздействиям: компрессии изображения (JPEG, JPEG2000), зашумлению, фильтрации, изменению размера, яркости и эквализации гистограммы. Дополнительно проверке на наличие ложного срабатывания был подвергнут предложенный метод сокращения бит встраиваемой информации ЦВЗ.

Для сравнения с предложенным алгоритмом был использован алгоритм Elham [14], обладающий хорошей устойчивостью к компрессии JPEG. Для объективности сравнения параметры алгоритмов подбирались таким образом, чтобы встраивание ЦВЗ обеспечивало приблизительно одинаковый уровень искажения контейнера. Порог энтропии для каждого изображения подбирался максимально возможным для лучшей незаметности вносимых искажений.

В качестве контейнеров использовались 9 изображений размером 512×512 , отличающихся друг от друга гладкостью текстур и уровнем яркости. Используемый в ходе эксперимента ЦВЗ представляет собой монохромное черно-белое изображение размером 64×64 пиксела (рис. 3).



Рис. 3. Используемый цифровой водяной знак

В качестве меры незаметности внедренного ЦВЗ выбран наиболее распространенный показатель – пиковое отношение сигнала к шуму ($PSNR$), измеряемый в децибелах (дБ) и определяемый по формуле

$$PSNR = 10 \lg \frac{255^2 \times M \times N}{\sum_{x,y} (f(x,y) - \hat{f}(x,y))^2},$$

где $f(x, y)$ – контейнер; $\hat{f}(x, y)$ – стеганоконтейнер; x, y – координаты пикселей изображения; M и N – высота и ширина изображения. Искажения считаются незаметными, если $PSNR \geq 43$ дБ.

Для определения устойчивости внедренного ЦВЗ был использован коэффициент корреляции Пирсона, определяемый по формуле

$$k = \frac{\sum_c \sum_r (A(c, r) - A_m) \times (B(c, r) - B_m)}{\sqrt{\sum_c \sum_r ((A(c, r) - A_m)^2) \times \left(\sum_c \sum_r (B(c, r) - B_m)^2 \right)}}$$

где c, r – координаты пикселя изображения; $A(c, r)$ – исходный водяной знак; $B(c, r)$ – извлеченный водяной знак; A_m, B_m – среднее арифметическое пикселей исходного и извлеченного ЦВЗ.

Коэффициент корреляции Пирсона принимает значения от -1 до 1 . Значению $k=1$ соответствует полная идентичность встроенного и извлеченного ЦВЗ. Как правило, ЦВЗ считается устойчивым к вредоносному воздействию, если $k \geq 0,5$. В противном случае встроенная информация считается уничтоженной.

В процессе вычислительного эксперимента в каждый контейнер при помощи нового алгоритма и алгоритма Elham осуществляется встраивание ЦВЗ. Полученное изображение (стеганоконтейнер) подвергается вредоносному воздействию. Затем из поврежденного стеганоконтейнера извлекается ЦВЗ с последующим измерением коэффициента корреляции между исходным и извлеченным ЦВЗ. Значения корреляции для каждой атаки, полученные при использовании 9 тестовых изображений, усредняются.

Способ уменьшения количества бит встраиваемого ЦВЗ был проверен на ложное срабатывание (проявление ЦВЗ при подстановке случайной последовательности маркеров). Для исходного ЦВЗ (рис. 3) размером 64×64 , 54×54 , 44×44 , 34×34 и 24×24 пикселя было сгенерировано 10^5 случайных последовательностей бит. Ложное срабатывание считалось произошедшим, если коэффициент корреляции Пирсона между исходным изображением и полученным в результате ложной подстановки маркеров – не менее $0,5$. Значения $0,2 \leq k < 0,5$ считались нежелательными.

Результаты эксперимента

Применение предварительной обработки ЦВЗ перед встраиванием позволило для использованного водяного знака (рис. 3) сократить объем встраиваемых бит на 88% по сравнению с аналогичным методом без предварительного сокращения встраиваемой информации. Для текущего ЦВЗ разных размеров (указанных ранее) на 10^5 случайных последовательностей бит коэффициент корреляции не превышал $0,5$. Следовательно, ложного срабатывания стеганодетектора не наблюдалось. Для ЦВЗ размером 64×64 вероятность появления нежелательной корреляции составляет $0,001\%$ на 10^5 случайных последовательностей бит. При уменьшении размера встраиваемого ЦВЗ до 24×24 вероятность нежелательного исхода возрастает до $1,275\%$ на 10^5 случайных последовательностей бит. Таким образом, использование структуры ЦВЗ в качестве части ключа не является для стеганодетектора информацией, способной привести к ложному срабатыванию.

Среднее значение $PSNR$ для 9 тестовых полутоновых изображений составляет $43,2218$ дБ, что показывает малую заметность вносимых искажений. Алгоритм Elham демонстрирует схожее значение $PSNR$, равное $43,2104$ дБ.

Разработанный алгоритм обеспечивает более высокую, чем у алгоритма Elham, устойчивость ЦВЗ к компрессии JPEG (рис. 4, а). Устойчивость наблюдалась для 99% диапазона значений коэффициента качества Q . Резкое падение устойчивости для значений Q , находящихся в диапазоне от 6 до 3, связано с особенностью поведения коэффициентов ДПА при сжатии JPEG (рис. 1). По сравнению с алгоритмом Elham наблюдается улучшение устойчивости ЦВЗ к компрессии JPEG2000 (рис. 4, б) вплоть до уровня сжатия 1:67.

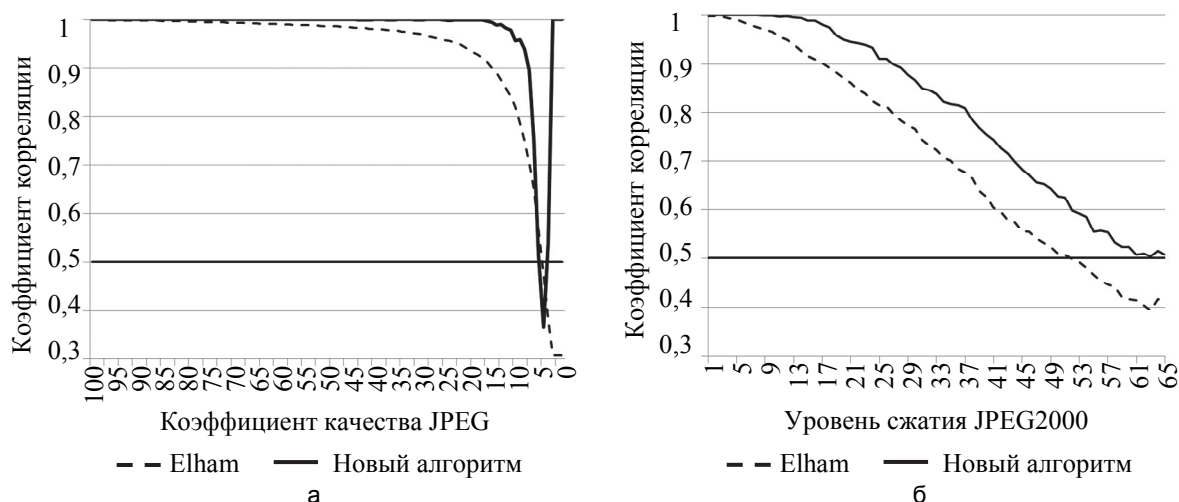


Рис. 4. Устойчивость внедренного цифрового водяного знака к компрессии JPEG (а) и JPEG2000 (б)

Результаты сравнительного анализа устойчивости нового алгоритма и алгоритма Elham к другим атакам приведены в табл. 2.

Тип атаки	Параметр атаки	Новый алгоритм (Корреляция)	Elham [11] (Корреляция)
Шум Гаусса	Дисперсия 0,01	0,8887	0,7157
	Дисперсия 0,02	0,7082	0,5857
	Дисперсия 0,03	0,5909	0,5065
	Дисперсия 0,04	0,5126	0,4506
Шум «Соль и перец»	Дисперсия 0,02	0,9452	0,7983
	Дисперсия 0,06	0,7308	0,5872
	Дисперсия 0,08	0,6358	0,5217
	Дисперсия 0,1	0,5627	0,4671
Среднечастотная фильтрация	Окно 2×2	0,6124	0,5999
	Окно 3×3	0,8651	0,8495
	Окно 4×4	0,3979	0,4519
Фильтрация Винера	Окно 2×2	0,9937	0,8994
	Окно 3×3	0,9676	0,9420
	Окно 8×8	0,5416	0,4267
Изменение яркости	0,8	0,9218	0,6699
	1,2	0,9978	0,8106
	1,4	0,9020	0,6423
	1,6	0,5731	0,5293
Изменение размера	50%	0,9296	0,9396
	35%	0,5920	0,6414
Эквализация гистограммы	–	0,5488	0,5518

Таблица 2. Сравнение стойкости нового алгоритма с алгоритмом Elham

Новый алгоритм обладает увеличенной устойчивостью к зашумлению Гаусса и шуму «Соль и перец». Однако стойкость разработанного алгоритма к шуму Гаусса нуждается в дополнительном улучшении до дисперсии 0,07, при которой изображение окончательно теряет свою коммерческую ценность. Существенно улучшено противодействие ЦВЗ фильтрации Винера до окна фильтрации размером 8×8, а также изменению яркости изображения в диапазоне от 75% до 160%. Стойкость нового алгоритма по отношению к среднечастотной фильтрации, изменению размера изображения и эквализации его гистограммы аналогична алгоритму Elham.

Заключение

Представленный в работе алгоритм обеспечивает улучшенную и практически полную устойчивость цифрового водяного знака к JPEG-сжатию. Используемый в новом алгоритме процесс предварительной обработки водяного знака позволяет существенно сократить объем встраиваемой информации. Стратегия выбора частотных коэффициентов дискретного преобразования Адамара, помимо противодействия компрессии, увеличивает устойчивость алгоритма к зашумлению, фильтрации Винера и изменению яркости изображения. Выбор блоков на основе значения энтропии яркости пикселей увеличивает незаметность искажений изображения, позволяя использовать высокие коэффициенты усиления встраиваемой информации. Дальнейшие исследования будут направлены на изучение возможностей данного алгоритма в области маркирования цветных изображений, а также влияния декомпозиции контейнера на блоки разного размера и на стойкость встраиваемого цифрового водяного знака.

References

- Gribunin V.G., Okov I.N., Turintsev V.I. *Tsifrovaya Steganografiya* [Digital Steganography]. Moscow, SOLON-Press Publ., 2002, 272 p.
- Wu X., Sun W. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing Journal*, 2013, vol. 67, no. 2, pp. 1170–1182. doi: 10.1016/j.asoc.2012.09.028
- Patra J.C., Phua J.E., Borland C. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digital Signal Processing: A Review Journal*, 2010, vol. 20, no. 6, pp. 1597–1611. doi: 10.1016/j.dsp.2010.03.010
- Bhatnagar G., Jonathan Wu Q.M. A new logo watermarking based on redundant fractional wavelet transform. *Mathematical and Computer Modelling*, 2013, vol. 58, no. 1–2, pp. 204–218. doi: 10.1016/j.mcm.2012.06.002
- Bhatnagar G., Jonathan Wu Q.M., Raman B. A new robust adjustable logo watermarking scheme. *Computers and Security*, 2012, vol. 31, no. 1, pp. 40–58. doi: 10.1016/j.cose.2011.11.003

6. Maheswari S., Rameshwaran K. Robust blind complex double Haar wavelet transform based watermarking algorithm for digital images. *IACSIT International Journal of Engineering and Technology*, 2011, vol. 3, no. 6, pp. 638–645.
7. Maity S.P., Kundu M.K. DHT domain digital watermarking with low loss in image informations. *AEU – International Journal of Electronics and Communications*, 2010, vol. 64, no. 3, pp. 243–257. doi: 10.1016/j.aeue.2008.10.004
8. Maity S.P., Kundu M.K. Perceptually adaptive spread transform image watermarking scheme using Hadamard transform. *Information Sciences*, 2011, vol. 181, no. 3, pp. 450–465. doi: 10.1016/j.ins.2010.09.029
9. Saryazdi S., Nezamabadi-pour H. A blind digital watermark in Hadamard domain. *International Journal of Computer, Information, Systems and Control Engineering*, 2007, vol. 1, no. 3, pp. 784–787.
10. Bhatnagar G., Raman B. Robust watermarking in multiresolution Walsh-Hadamard transform. *2009 IEEE International Advance Computing Conference, IACC 2009*. Patiala, India, 2009, art. 4809134, pp. 894–899. doi: 10.1109/IADCC.2009.4809134
11. Sarker I.H., Iqbal S. Content-based image retrieval using Haar wavelet transform and color moment. *Smart Computing Review*, 2013, vol. 3, no. 3, pp. 155–165.
12. Ho A.T.S., Shen J., Tan S.H. A character-embedded watermarking algorithm using the fast Hadamard transform for satellite images. *Proceedings of SPIE – The International Society for Optical Engineering*, 2002, vol. 4793, pp. 156–167. doi: 10.1117/12.451249
13. Latif A., Rashidi F. A watermarking scheme based on the parametric slant-hadamard transform. *Journal of Information Hiding and Multimedia Signal Processing*, 2011, vol. 2, no. 4, pp. 377–386.
14. Shabanali Fami E., Samavi S., Rezaee Kaviani H., Molaei Radani Z. Adaptive watermarking in Hadamard transform coefficients of textured image blocks. *Proc. 16th International Symposium on Artificial Intelligence and Signal Processing, AISP 2012*. Shiraz, Iran, 2012, vol. 181, pp. 503–507. doi: 10.1109/AISP.2012.6313799
15. Батура В.А., Трощенко А.Ю. Сравнительный анализ эффективности использования ортогональных преобразований в частных алгоритмах маркировки цифровых изображений [Comparative analysis of application efficiency of orthogonal transformations in frequency algorithms for digital image watermarking]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 6 (94), pp. 106–112.
16. Явна Д.В., Бабенко В.В. Психологически обоснованный метод оценки количества информации в изображении [Psychophysiologicaly motivated method for estimating the amount of information in an image]. *Inzhenernyi Vestnik Dona*, 2014, vol. 31, no. 4–1, p. 116.

Батура Владимир Александрович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Batu-vladimir@yandex.ru

Vladimir A. Batura – Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, Batu-vladimir@yandex.ru