Список используемых источников

1. Korzhik V., Morales Luna G., Loban K. Stegosystem Based on Noisy Channels // International Journal of Computer Science and Applications. 2011. Vol. 8 №. 1. P. 1–13.

2. Коржик В. И., Небаева К. А., Алексеевс М. Использование модели канала с шумом для построения стегосистемы // Телекоммуникации. 2013. S 7. С. 33–36.

3. Коржик В. И., Небаева К. А., Алексеевс М., Стегосистема для каналов с шумом при использовании «слепого» декодера // Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании». 20–24 февраля 2012: материалы конф., СПб., 2012. С. 238–240.

4. Небаева К. А. Стегосистемы на основе каналов с шумом при использовании слепого декодера // В мире научных открытий. 2013. № 10.1 (46). С. 118–132.

5. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом : дис. … канд. техн. наук: 05.12.13 / Небаева Ксения Андреевна. СПб., 2014. 176 с.

6. Герлинг Е. Ю. Исследование и разработка методов обнаружения стеговложений в неподвижных изображениях : дис. … канд. техн. наук: 05.12.13 / Герлинг Екатерина Юрьевна. СПб., 2014. 211 с.

ИСПОЛЬЗОВАНИЕ МЕТОДА 3-БИТНОГО КВАНТОВАНИЯ ДЛЯ АЛГОРИТМА СЕЛЕКТИВНОЙ АУТЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ, УСТОЙЧИВОГО К JPEG СЖАТИЮ

А.Г. Жувикин, В.И. Коржик

Преимуществом использования цифровых водяных знаков является то, что они не требуют использования дополнительного объёма памяти для хранения метаданных. Однако, применение JPEG сжатия, как наиболее распространённого метода уменьшения размера изображений, приводит к нарушению целостности при использовании точной аутентификации. В данной работе предложен улучшенный метод селективной аутентификации изображений, устойчивый к JPEG сжатию, основанный на применении центральных конечных разностей и алгоритма 3-битного квантования вектора свойств. Экспериментальные результаты показали высокую устойчивость к JPEG сжатию с параметром качества $Q \geq 8$, высокую вероятность обнаружения искажений небольших искажений изображений, показатели $PSNR \geq 40$ дБ после погружения цифровых водяных знаков и низкую вычислительную сложность алгоритма по сравнению с предыдущим методам.

Ключевые слова: цифровые изображения; селективная аутентификация; JPEG; 3-битное квантование; вейвлет-преобразование Хаара; центральные конечные разности

THE USAGE OF 3-BIT QUANTIZATION METHOD FOR SELECTIVE IMAGE AUTHENTICATION ALGORITHM ROBUST TO JPEG COMPRESSION

Zhuvikin A., Korzhik V.

The advantage of watermarking usage is it does not require to store of metadata in extra memory space. However, JPEG algorithm, being a common method for image compression, leads to break-in of strict image authentication. An improved algorithm of selective image authentication tolerant to JPEG compression is presented. Proposed method is based on central finite differences

and 3-bit quantization of the feature vector. The experimental results show that algorithm has strong resistance to JPEG compression with quality factor Q ≥ 8, the high probability of malicious tampering detection and low order of calculation complexity comparing with the previous presented. A visual quality (PSNR) of the watermarked image is higher than 40 dB.

Keywords: digital images, selective authentication, JPEG, 3-bit quantization, discrete wavelet transform.

Введение

В будущем сохранение целостности изображений будет оставаться актуальной задачей. Методы аутентификации изображений с использованием цифровых водяных знаков (ЦВЗ) не требуют использования дополнительного объёма памяти, а погружают аутентификатор непосредственно в само изображение. Они имеют широкие возможности для практического применения в таких сферах как: медицина, охрана правопорядка, военные и коммерческие сферы. В литературе представлены различные алгоритмы точных и селективных методов аутентификации изображений. Ограниченность применения точной аутентификации [1] заключается в том, что после изменения даже одного бита изображение будет считаться поддельным. Для того чтобы изображение можно было подвергать естественным преобразованиям, таким как JPEG-сжатие, но при этом обнаруживались искажения содержания изображений, были разработаны алгоритмы селективной аутентификации [2, 3, 4, 5]. В данной работе представлен улучшенная версия алгоритма [6]. Для формирования аутентификатора используются центральные конечные разности (ЦКР) [7] и 3-битное квантование [8], а для погружения применен метод с использованием 3-уровнего дискретного вейвлет-преобразования (ДВП) [9].

В первом разделе описаны ЦКР и алгоритм 3-битного квантования. Во втором разделе приведены результаты экспериментов и оптимизации параметров предложенного метода селективной аутентификации.

1. Свойства ЦКР и применение 3-битного квантования вектора свойств

ЦКР первого порядка любой функции I : $\{0, 1, \ldots, n_x\} \times \{0, 1, \ldots, n_y\} \to \mathbf{Z}^+$ определены как [7]:

$$\delta_x(x,y) = \frac{1}{2}\big(I(x+1,y) - I(x-1,x)\big),$$
$$\delta_y(x,y) = \frac{1}{2}\big(I(x,y+1) - I(x,x-1)\big).$$

Для уменьшения влияния шума в ЦКР после JPEG-сжатия предлагается использовать свёртку яркостей отсчётов изображения с 2-ух мерным фильтром Гаусса, который имеет следующую импульсную характеристику

$$h(i,j) = \begin{cases} \dfrac{1}{2\pi\sigma^2}\exp\left(\dfrac{\left(i-\frac{n}{2}\right)^2 + \left(j-\frac{n}{2}\right)^2}{2\sigma^2}\right), & \text{если } 1 \le i \text{ и } j \le n, \\ 0, & \text{иначе,} \end{cases}$$

где σ^2 – характеризует параметр фильтрации, а n – размер окна ядра Гаусса. После 2-ух мерной свёртки $h**I$ получаем:

$$\tilde{I}(x,y) = \sum_{i=0}^{n_x-1}\sum_{j=0}^{n_y-1} h(i,j)I(x-i,y-j).$$

Пусть, элементы $\delta(x, y)$ матрицы свойств **D** изображения определены как:

$$\tilde{\delta}(x,y) = \sqrt{\tilde{\delta}_x{}^2(x,y) + \tilde{\delta}_y{}^2(x,y)},$$

тогда применяя операцию уменьшающей передискретизации, можем уменьшить размер матрицы **D** до требуемого размера:

$$d(k,m) = \frac{1}{st}\sum\{\tilde{\delta}(i,j) \mid s(m-1) < i \le sm \text{ и } t(k-1) < j \le tk\},$$

где s и t – целочисленные параметры для вертикальной и горизонтальной составляющих соответственно. Для простоты, в дальнейшем будем представлять матрицу **D** как одномерный вектор свойств $d(i)$ длины $(n_x n_y)/st$.

3-битное квантование вектора свойств d выполняется по правилам [8]:

$$(p_{1i}, p_{2i}) = [d_\Delta(i) \bmod 4]_2, \quad p_{3i} = \begin{cases} 1, & d(i) \in [a_i, b_i) \\ 0, & d(i) \in [a_i, b_{i+1}) \end{cases}, \quad \acute{d}_\Delta(i) = \left\lfloor \frac{d(i)}{\Delta} \right\rfloor,$$

где $a_i = \Delta d_\Delta(i)$, $b_i = \Delta(d_\Delta(i)+1/2)$ и $[\cdot]_2$ – аргумент в двоичном представлении, p_{1i}, p_{2i}, p_{3i} – 3 бита i-ого элемента вектора возмущений p.

После этого вектор свойств d может быть хеширован и использован для формирования цифровой подписи (ЦП). Если после JPEG-сжатия элементы вектора свойств изменились не более чем на один уровень квантования [8], то его можно восстановить по следующему алгоритму:

$$\acute{d}(i) = \begin{cases} \acute{d}(i) + \Delta, & \alpha_i = 0 \text{ и } \tilde{p}_{3i} = 0, \\ \acute{d}(i) + \Delta, & \alpha_i = 0 \text{ и } \tilde{p}_{3i} = 1 \text{ и } \acute{p}_{3i} = 1, \\ \acute{d}(i) - \Delta, & \alpha_i = 1 \text{ и } \tilde{p}_{3i} = 1, \\ \acute{d}(i) - \Delta, & \alpha_i = 1 \text{ и } \tilde{p}_{3i} = 0 \text{ и } \acute{p}_{3i} = 0, \\ \acute{d}(i), & \text{иначе}, \end{cases}$$

$$\alpha_i = \begin{cases} 0, & [\acute{p}_{1i}\acute{p}_{2i}]_{10} = ([\tilde{p}_{1i}\tilde{p}_{2i}]_{10} - 1) \bmod 4, \\ 1, & [\acute{p}_{1i}\acute{p}_{2i}]_{10} = ([\tilde{p}_{1i}\tilde{p}_{2i}]_{10} + 1) \bmod 4, \\ 2, & \text{иначе}. \end{cases}$$

где $[\cdot]_{10}$ – аргумент в десятеричном представлении, $\tilde{p}_{1i}$, $\tilde{p}_{2i}$, $\tilde{p}_{3i}$ – 3 бита i-ого элемента $\tilde{p}_i$ вектора возмущений $\tilde{p}$, который был извлечён как ЦВЗ, а $\tilde{p}_{1i}$, $\tilde{p}_{2i}$, $\tilde{p}_{3i}$ – биты вектора возмущений $\acute{p}$ рассчитанного по искажённой версии изображения I, $d(i)$ – i-ый элемент вектора свойств, рассчитанный по искажённому изображению перед восстановлением квантованного вектора свойств.

2. Экспериментальные результаты и оптимизация параметров

В качестве алгоритма погружения и извлечения был использован метод на основе трёхуровневого дискретного вейвлет-преобразования (ДВП) с погружением ЦВЗ в области коэффициентов LH3 и HL3 [6]. Алгоритм погружения имеет высокую устойчивость к JPEG-сжатию с параметрами качества $Q \geq 6$ [6]. На рисунке 1 приведена главная схема предлагаемого алгоритма селективной аутентификации с соответствующими обозначениями.

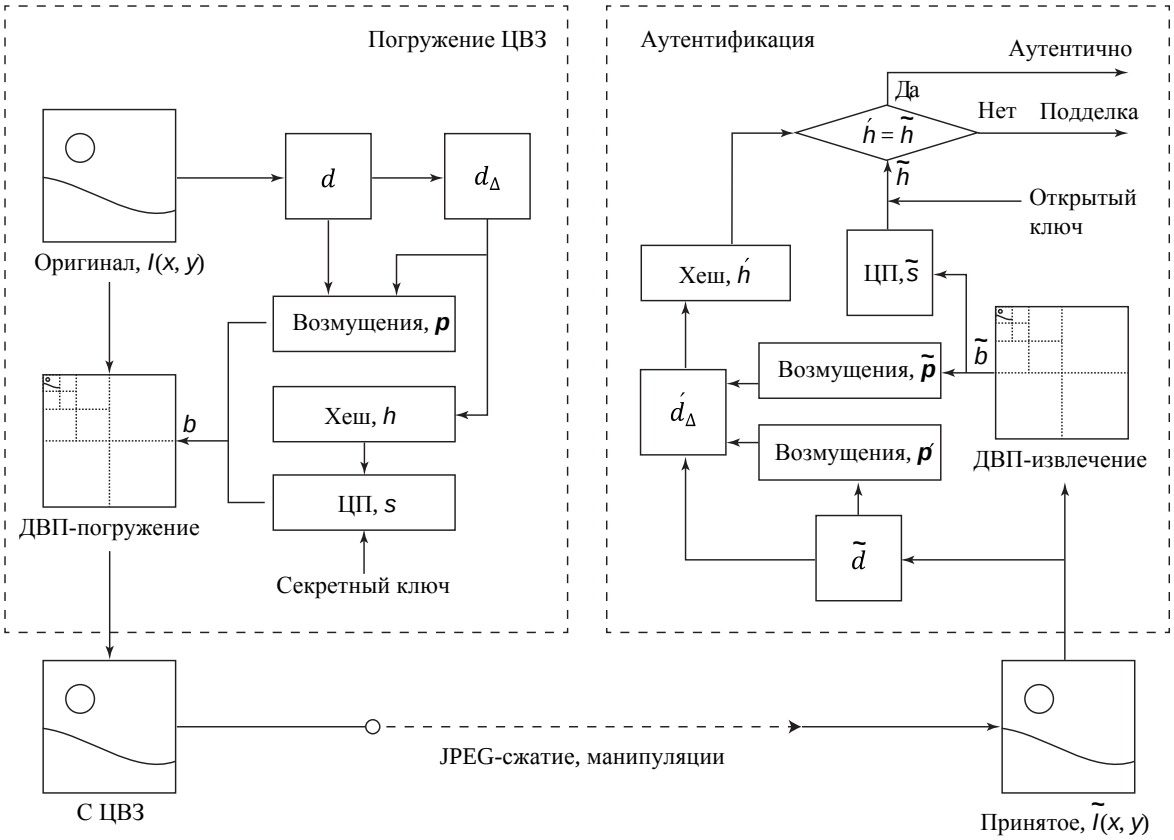

Рис. 1. Главная схема предлагаемого алгоритма селективной аутентификации с соответствующими обозначениями

Во-первых, необходимо исследовать чувствительность предлагаемого алгоритма к JPEG-сжатию. Для эксперимента было взято 50 различных цифровых изображений размерами 512×512, имеющие различный контент и текстуры. Области ДВП LH3 и HL3 содержат по $2\times(2^6)^2 = 2^{13} = 8192$ коэффициента, каждый из которых позволяет погрузить один бит [6].

Длина вектора свойств d была выбрана равной $2^{10} = 1024$, соответствующая размерам $2^5\times2^5 = 32\times32$ матрицы **D**. Для этого необходимо выбрать параметры $s = t = 2^4 = 16$. Таким образом, вектор возмущений p имеет длину $3\times2^{10} = 3072$ бита. В качестве алгоритма хеш-функции был выбран SHA-2 [1], а ЦП-алгоритм основанный на криптосистеме РША [1] с длиной модуля равной 1024. Общий размер погружаемых данных равен 3072 + 1024 = 4096 бит. После вы-

бора параметров было произведено исследование эффективности системы селективной аутентификации.

На рисунке 2 отображена зависимость показателя TPR (*True Positive Rate*) от параметра JPEG-сжатия Q и интервала квантования Δ элементов вектора свойств d. Как видно, метод является устойчивым к JPEG-сжатию с параметрами качества $Q \geq 8$ при значениях $\Delta \geq 7{,}5\times10^{-3}$.

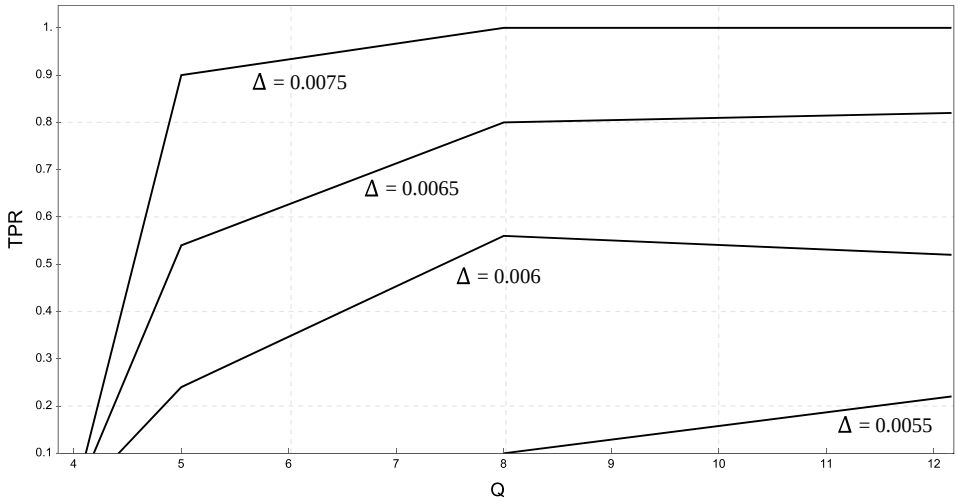

Рис. 2. Зависимость показателя TPR (True Positive Rate) от параметра JPEG-сжатия Q и интервала квантования Δ элементов вектора свойств d

Для исследования способности системы обнаруживать преднамеренные искажения был поставлен следующий эксперимент. Были взяты псевдослучайные квадратные области размерами $\alpha_0\times\alpha_0$, в которых были выбраны случайные значения яркостей пикселей. Для каждого изображения было искажено 50 таких областей. На рисунке 3 приведена зависимость показателя TNR (*True Negative Rate*) от размера области искажений α_0 и интервала квантования Δ элементов вектора свойств d. Из графика видно, что алгоритм обнаруживает искажения размерами $\alpha_0 \geq 10$ при значениях $\Delta \leq 10^{-2}$.

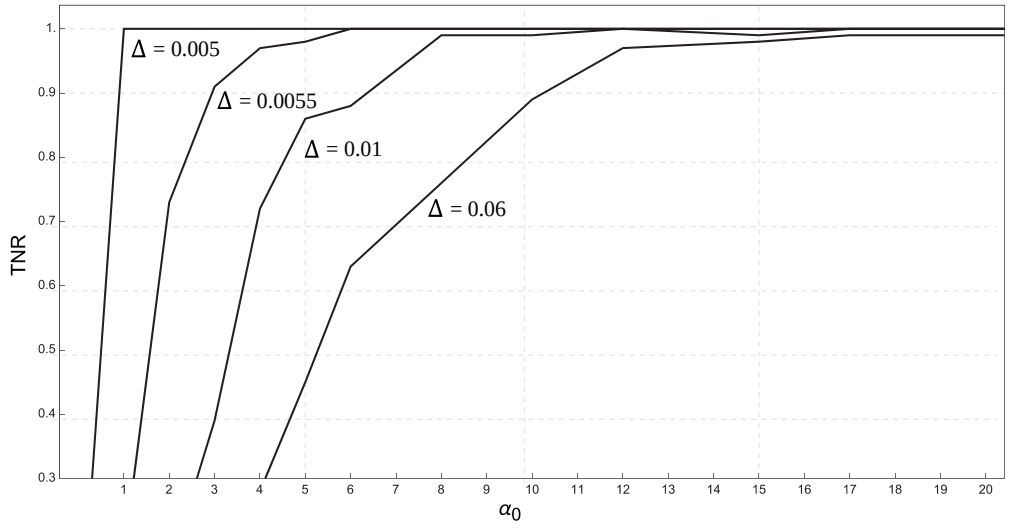

Рис. 3. Зависимость показателя TNR (True Negative Rate) от размера области искажений α_0 и интервала квантования Δ элементов вектора свойств d

Заключение

В данной работе представлен алгоритм селективной аутентификации, использующий ЦКР и 3-битное квантование. Главной идеей в решении задачи описания содержания изображения является применение ЦКР и формирование на их основе вектора свойств изображения, который после применения 3-битного квантования позволяет сформировать компактный аутентификатор. Благодаря применению алгоритма 3-битного квантования и оптимизации его параметров, изначальные уровни квантования вектора свойств полностью восстанавливаются после применения JPEG-сжатия.

В качестве алгоритма погружения был использован метод на основе трёхуровневого ДВП, использующий области коэффициентов HL3 и LH3. Экспериментальные исследования показали эффективность предлагаемого алгоритма. Метод является устойчивым к JPEG-сжатию с параметрами качества $Q \geq 8$, а изображения после погружения ЦВЗ имеют высокие показатели визуального качества PSNR ≥ 40 дБ.

Главными преимуществами данного метода являются его способность обнаруживать преднамеренные искажения размерами $\alpha_0 \geq 10$ и относительно низкая вычислительная сложность.

Устойчивость алгоритма погружения и извлечения ЦВЗ к другим преобразованиям, таким как, изменение яркости, контрастности и размера является открытой проблемой.

Список используемых источников

1. Menezes A. A. J., Van Oorschot P., and Vanstone, S. Handbook of Applied Crytography // Discrete Mathematics and Its Applications Series. Crc Press. 1997.

2. Lee M. H., Korzhik V. I., Morales-Luna G., Lusse S., and Kurbatov E. Image authentication based on modular embedding. IEICE Transactions 89-D. 2006. N 4. PP. 1498–1506.

3. Goljan M., Fridrich J. J., and Du R. Distortion-free data embedding for images / In Proceedings of the 4th International Workshop on Information Hiding. IHW '01. Springer-Verlag, London, UK. 2001. PP. 27–41.

4. Fridrich J., Goljan M., and Du R. Invertible authentication watermark for JPEG images / In ITCC (2004-01-26). IEEE Computer Society. PP. 223–227.

5. Ni Z., Shi Y., Ansari N., and Su W. Reversible data hiding / IEEE Trans. Circuits Syst. Video Techn. 2006. 16, 3. PP. 354–362.

6. Korzhik V., Zhuvikin A., and Morales-Luna G. Selective image authentication tolerant to JPEG compression / In 6th IISA 2015. IEEE, 06–08.

7. Eberly D. Derivative approximation by finite differences. Tech. rep. 2008.

8. Zivic N. Robust Image Authentication in the Presence of Noise. Springer International Publishing, 2015. 187 p.

9. Porwik P. and Lisowska A. The Haar wavelet transform in digital image processing: its status and achievements // Int. Journal Machine Graphics & Vision. 2004. V. 13. N 1. PP. 79–98.